On the Effectiveness of Hardware Trojan Horse Detection via Side-Channel Analysis

Sophie Dupuis, Giorgio Di Natale, Marie-Lise Flottes, Bruno Rouzeyre

On the effectiveness of Hardware Trojan Horses Detection via Side-Channel Analysis

Sophie Dupuis*, Giorgio Di Natale, Marie-Lise Flottes, Bruno Rouzeyre
LIRMM – UM2/CNRS
161 rue Ada, 34095, Montpellier cedex 5, France
Email: {firstname.lastname}@lirmm.fr

Abstract—**Hardware TrojanHorses (HTHs) are malicious and stealthy alterations of integrated circuits introduced at design or fabrication steps in order to modify the circuit's intended behavior when deployed in the field. Due to HTHs stealth and diversity(intended alteration, implementation, triggering conditions), detecting and/or locating them is a challenging task. SeveralHTHs detection approaches have been proposed to address this problem.This paper focuses on so-called "side-channel analysis" methods,*i.e.*,methods that use power or delay measurements to detect potential HTHs. Itreviews these methods and raises some considerations about the experiments made to evaluate them. Moreover, an original case studyis presented in which we show that weak experiments may lead to misleading interpretations. Last, we evoke problems inherent to actual power and delay measurements.**

Keywords —**HardwareTrojan Horse (HTH), HTH detection, Side-channel analysis, Simulation**

I. INTRODUCTION

Hardware Trojan Horses (HTHs) are malicious inclusions put into an integrated circuit (IC) to result, under specific conditions, in a functional change (Wang, Tehranipoor, &Plusquellic, 2008). HTHs may be inserted during the design phase (Rajendran, Gavas, Jimenez, Pafman, & Karri, 2010), because of third parties IPs (Jin, &Makris, 2012) or rogue designers (Hicks, Finnicum, King, Martin, & Smith, 2010), or during the fabrication phase. The cost of new fabrication facilities is indeed becoming prohibitive and outsourcing the fabrication process to low-cost locations has become a major trend in IC industry in the last decade. Untrusted foundries may therefore manipulate the circuits with the possible insertion of HTHs.It is on this latter type of HTH that this paper focuses on.Methods for detecting such alterations are of prime interest.

In this paper, we focus onHTHs detection methods based on so-called *side-channel analysis,i.e.*,power or/and delay measurements.Wereview the evaluation approaches proposed in literature toanalyze the strengths and weaknesses of the detection methods.In particular, several detection methods are validated by simulation-based experiments. This raises the question: *Are the proposedsimulations accurate enough to be representative of what could be done with actual measurements?*And therefore: *Do the experiments really prove the effectiveness of the approach?*We present a case studyon HTHs found in literature (Trust-hub, 2013) to show how weak simulationcan lead to misleading interpretations.

This paper is organized as follows. Section II presentsexisting side-channel analysis methods on HTH detection. Section III discusses the experiments conducted for the evaluation ofeach approach,and highlights two main weaknesses: the imprecisionof the measurements and the non-representativeness of experimented HTHs. Section IV depicts the proposed case study. Furthermore, Section V details inner problems of delay and power measurements on real circuits. Finally, Section VI concludes the paper.

II. PRIOR WORK ON HARDWARE TROJAN DETECTION

The most reliable technique to detect the presence or absence of a HTH is to remove the package of the IC and to analyze the dievia "reverse engineering" techniques. However, this technique requires the destructionof the IC that has been proven to be HTH-free and does not produce evidence thatuntested ICs in the lot/wafer are HTH-free. Furthermore, this technique becomes even more difficult and expensive with shrinking technologies (Torrance, & James, 2011).Non-destructive methods are therefore needed*i.e.* methods that perform tests and/or measurements on the fabricated ICs without alteration of the devices. Non-destructive methods are categorized as either *side-channel analysis* or *logic testing* (Tehranipoor, &Koushanfar, 2010).

So-calledside-channel analysis methods consist in observingphysical parameters of the fabricated ICs such as power consumption, delay or electro-migration (EM).The assumption is that a HTH changes ICs' parametric characteristics in such a way that a comparison with a *golden reference*ICreveals a HTH in an under-test IC, if any.These methods therefore require golden references *i.e.* measurements on ICs that have been proven to be HTH-free (e.g. by reverse engineering as depicted before). In this paper, we focus on power consumption and delay, as they are the most studied criteria in the field of HTH detection.

In general, each method mentioned belowhas been evaluated by comparing the measurements resulting from HTH-free circuits and their corresponding implementation infected with aHTH. However, as shown in the next section, simulation-based approaches have been adopted. This paper therefore questions the accuracy of the simulations to prove the effectiveness of these approaches

A. Dynamic Power

Power-based side-channel analysis is introduced in (Agrawal, Baktir, Karakoyunlu, Rohatgi, &Sunar, 2007).Random patterns are appliedand dynamic power measurements are performed. The aim is to compare dynamic power between under-test ICs and the golden reference. However, simulations show that process and test environment variations (PE variations) mask the impact of small HTHs.To better take into account PE variations,(Rad, Wang, Tehranipoor, &Plusquellic, 2008)proposes to analyze regional dynamic power as well as signal calibration techniques.

In order to improve HTH detection sensitivity under large PE variations, several authors propose circuit partition based approaches to localize switching activity into a specific region.In (Banga, Chandrasekar, Fang, & Hsiao, 2008), (Banga, & Hsiao, 2008)and (Du, Narasimhan, Chakraborty, &Bhunia, 2010), it is proposed to simulate the circuit with patterns that induce maximum switching activity in one region and minimum activity in other regions.So as to be independent from test patterns, (Salmani, Tehranipoor, &Plusquellic, 2010) proposes a modification of the design to reorder scan cells, based on their geometric position. Based on the observation that during scan based testing, the power consumption of an IC is correlated with the number of transition in the scan cells, reordering scan cells based on their geometric position can restrict switching activity into a specific region.Another idea concerning input vectors generation is proposed in (Banga, & Hsiao, 2009). It consists in magnifying the HTH contribution by minimizing circuit activity. This is done by keeping constant the input vectors for several clock cycles, which is said to ensure the reduction of extraneous toggles within genuine circuits.

B. Static Power

In (Alkabani, &Koushanfar, 2009), a method is presented that uses static power to perform gate leakage estimation. The authors propose to build a system of equations that allows characterizing each single gate of the circuit. By comparing the characterization between the golden and the target circuit, it is possible to identify the presence of a HTH. However, the scalability to big circuits remains an issue.

C. Delay

In (Jin, &Makris, 2008), a new method is proposed, based on the generation of fingerprints that depend on path delay information. Delay test patterns are generated using an ATPG tool, and then a simulation is conducted to collect the delay information for each output of the circuit under each test pattern.

It is proposed in (Li, Davoodi, &Tehranipoor, 2012) to put additional gates on circuits to be able to compare on-chip delays, in order not to rely on a golden IC. One random path per primary input and flip-flop is selected.

D. Power and delay

A gate-level characterization is presented in (Potkonjak, Nahapetian, Nelson, & Massey, 2009) using a set of delay, switching and leakage power measurements. Starting from a large set of measurements of the circuits in different states and for different input values, the authors propose the use of linear programming to solve a system of equations that allows extracting the power consumption and the delay of each single gate. Theprocess detects gates which have inconsistent characteristics compared to their original specified characteristics.As in (Alkabani*et al*., 2009), the scalability to real circuits remains an issue.

In (Narasimhan, Du, Chakraborty, Paul, Wolff, Papachristou, Roy, &Bhunia, 2010), the authors present a multiple-parameter approach that exploits the intrinsic relationship between dynamic current and maximum operating frequency. The assumption is that aHTH will cause a modificationofthe dynamic current, while it will not have similar effects on the maximum operating frequency as induced by process variations. In other words, the expected correlation between current and frequency will be violated by the presence of a HTH. The approach fails in identifying HTHs whenever the impact of the HTH is smaller than the variability.

III. Evaluation of HTH DetectionMethods

The evaluation of a detection method requires a circuit and its equivalent affected by a HTH. However, due to the lack of available real HTHs on fabricatedICs, simulation-based approachesareadopted instead.To the best of our knowledge, very few papers report measurements on real circuits (Du *et al*. 2010), (Narasimhan*et al*., 2010) but only on FPGAs.This section therefore focuses on the state-of-the-art experiments that have been conductedto evaluate above-mentioned side-channel analysis HTH detection methods.

Experimental setups of related works are detailed in Table I. For each method, we have reported the type of measurement used to detect the HTH(*i.e*. dynamic/static power, delay, or both). Moreover, we detailthe experimental setup (when available):

- Theused benchmarks(3rdcolumn);
- Theused HTH(from column4to 6): itsfunction, the size overhead, and the level of insertion;
- Theevaluation setups (columns7 and 8): simulation level and, when available, the considered process and test environment variations(the worst case is reported when available);
- How the golden model is obtained (9thcolumn).

From this table, we deduce two important criteria for evaluating a method:the simulation accuracy andthe representativeness of the HTHs.

TABLE I. OVERVIEW OF SIDE-CHANNEL ANALYSIS EXPERIMENTS IN LITERATURE

Reference	Side-channel	Benchmarks	HTHs			Detection setups		Golden reference
			Function	Size overhead	HTH insertion	Simulation level	PE variations	
(Agrawal *et al*., 2007)	Dynamic power	RSA	16-bit counter, 3&8-bit comparators	Up to +1.4%	RTL level	Gate level	±7.5%	Reverse engineering
(Rad *et al*., 2008)	Dynamic power	ISCAS85	Comparator	-	Gate & Layout level	Layout level	Yes	-
(Banga *et al*., 2008)	Dynamic power	ISCAS89	-	Less then 1%	-	-	No	-
(Banga&Hsiao, 2008)	Dynamic power	ISCAS89	-	Up to +6%	-	-	±7.5%	-
(Du *et al*., 2010)	Dynamic power	32-bit ALU, FIR filter	-	+0.01%	Gate level	Gate level	±20%	-
(Salmani *et al*., 2010)	Dynamic power	ISCAS89	Comparators 4 to 18 inputs	-	Layout level	Layout level	No	-
(Banga *et al*., 2009)	Dynamic power	ISCAS89	-	Up to +3%	Gate level	Gate level	No	-
(Alkabani *et al*., 2009)	Static power	MCNC91	1&3 two-input gates	-	-	Layout level	12%	Simulation
(Jin *et al*., 2009)	Delay	DES	4-bit counter, 2-bit comparator	+0.13% & +0.76%	Gate level	Gate level	±7.5%	Reverse engineering
(Li *et al*., 2012)	Delay	ISCAS89	Chain of inverters	-	Layout level	Layout level	Yes	No
(Potkonjak *et al*., 2009)	Power & Delay	ISCAS85	1 inverter	-	-	Layout level	10%	-
(Narasimhan *et al*., 2010)	Power & Delay	AES	3 sequential, 1 combinational	-	Gate level	Gate level	±20%	Simulation or reverse engineering

A. Simulation

When evaluating the power consumption or the delay of a logic path, the difference that can be obtained between simulation and real measurements may be significant. Simulation measurements have therefore to be as precise as possible.

1) Simulation level

Several HTH detectionmethodsare evaluated by delay and power analysisthat are made at gate level (see Table I, column 7), without considering the impact of placement and routing.

While delay and power evaluation at early stages is very useful for the designprocess, these evaluations seem to be not accurate enough to reveal a HTH and thus to qualify a detection procedure. Indeed, as experimental evidences will be shown in the next section, the HTH impact is very small and very precise measurements are needed to effectively assess the robustness of the detection method.

Furthermore, this type of analysis is done with a HTH inserted at gate level or register transfer level (see Table I, column 6), which is not representative of a HTH inserted in the layout during the fabrication step.

2) Variability

Themeasurement ofphysical characteristics(either power consumption or delay of a path) can widely vary among different fabricated circuits, and even among elements of the same circuit. This phenomenon is called *process and test environment (PE) variations*.Process variation increases with the shrinking feature size in VLSI technologies. For instance, the transistor threshold voltage standard deviation was 4.7% in the 250nm node and rose to 16% with the 45nm technology (Onabajo, & Silva-Martinez, 2012). In nowadays circuits, the variability is in the order of 15% (Pang, Qian, Spanos, &Nikolic, 2009).

In order to cope with variability, proposed methods use variability-aware simulation. This is done creating several libraries with random variations (see Table I, column 8).

3) Golden reference

Due to simulation imprecisions, it is not realistic to rely on golden references obtained from simulation, as suggested in (Narasimhan*et al*., 2010). The accuracy of the golden reference is indeed also crucial; it is reasonable to assume that these references must be obtained with real measurements on chips that have been proven to be HTH free (e.g. by reverse engineering). This issue is seldom investigated in the literature.

B. Hardware Trojan

Another consideration is related to the choice of the HTH function. Indeed, the HTHs inserted in order to validate the effectiveness of the detection methodsmust be representative of real threats. In other words, if the experimented HTH is “large” enough to be revealed by any measure (e.g. large impact on the circuit critical path), the evaluation of the detection method is not a proof of its efficiency but just a proof that this HTH is detectable (possibly by any measure) (see Table I, columns 4 and 5).

Besides functional matters, the way the HTH is inserted into the target design must be carefully decided (see Table I, column

6). The insertion level may havedifferent impacts in delay and/or power consumption and the detection method may be considered successful or not according to the validation level (without correlation with detection after insertion at the foundry).In fact, a HTH inserted in RT level does not adequately represent a HTH inserted in a foundry. A HTH should be inserted at lower level, as the attacker would really do.

These points raise the problem of benchmarks for fair evaluation and comparison of detection methods, such as already mentioned in (Wei, Li, Koushanfar, &Potkonjak, 2012).The Trust-Hub website (Trust-hub, 2013) has recently released a set of HTH benchmarks circuits that could become a working basis for future articles.

IV. CASE STUDY

In this section we evaluate the impact of three HTHs in terms of deviation in circuit power and delay. This analysis show how different evaluation levels can bring to misleading results.

A. Circuit and HTH description

We used three benchmarks provided by Trust-Hub (Trust-hub, 2013): the b19, the s15850 and the AES.Table II describes the characteristics of the HTHs inserted in these circuits in terms of activation mechanism and effect. A HTH is usually composed of two components (Wolf, Papachristou, Bhunia, &Chakraborty, 2008): (a) triggering and (b) payload logic, such as presented in Figure 1. The triggering logic monitors several signals in order to activate the payload at the proper event.

- The HTH inserted in the b19 benchmark follows this model. It is an internally time-based triggered HTH: the HTH trigger is a specific value of 3 internal signals that awakens a counter (the counter is also restarted with another specific value). Whenever the counter reaches a specific value, the payload modifies the value of an internal signal.
- The HTH inserted in the s15850 benchmark follows also this model. The trigger consists in a specific value of 32 internal signals. The payload leaks an internal signal on an output port.
- The HTH inserted in the AES benchmark is of a different type, since it is always active (no trigger) and it leaks the secret key through a covert channel.

Table II also describes the abstraction levels used to insert the HTHs, along with the size of each HTHand the comparison with the size of each circuit.HTHs in the b19 and s15850 benchmarks were inserted at gate level *i.e.* in the Verilog netlists.The HTH inserted in the b19 benchmark represents an additional cost of 0.13% in number of cells, 1.25% for the s15850 benchmark.Besides, the b19 benchmark is also provided at the layout level (.def format): the HTH has been inserted after the place and route process, without changing the initial layout. This allows assessing the impact of a HTH inserted into the layout, which is the most representative of a HTH inserted in a foundry.The HTH in the AES benchmark has been inserted at RT level.The numbers presenting the size of this HTHare in italics since they result of thenetlists obtained after the synthesis of the HTH free and the infected circuits. As one can notice, the synthesis managed to produce a gate level description with fewer gates with the HTH inserted, which is not representative of a HTH inserted in a foundry. This shows a negative point of HTHs inserted at RT level.

TABLE II. TRUSTHUB HTS

	HT Taxonomy	**HT free** Nb cells Nb nets	**HT in** Nb cells Nb nets	**HT impact** Nb cells Nb nets
b19 benchmark	- Gate level& Layout level - Time based triggered - Change functionality	62 803 70 310	62 886 70 438	83**(+0.13%)** 128**(+0.18%)**
s15850 benchmark	- Gate level - Conditionally triggered - Change functionality	2 155 2 408	2 182 2 435	27**(+1.25%)** 27 **(+1.12%)**
AES benchmark	- RT level - Always on - Leak information	*141 391* *143 911*	*141 256* *143 778*	*-135* ***(-0.1%)*** *-133****(-0.1%)***

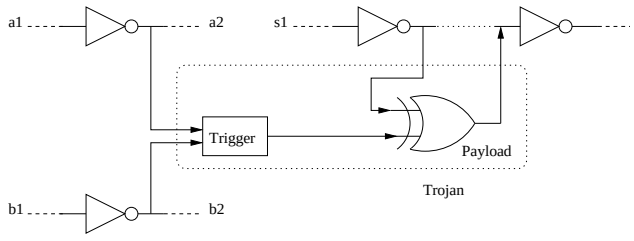

Figure 1. HT circuit model

B. Synthesis and simulation Environments

Synthesis and place and route were done with the Synopsys suite (Synopsys, 2013) and a 90nm standard cell library(Goldman, Bartleson, Wood, Kranen, Cao, Melikyan, &Markosyan, 2009). Delay and power consumption analysis were done with the Prime Time tool of the Synopsys suite.It allowsto analyze delay and power consumption at gate level and layout level. A vector-free dynamic power analysis has beenconducted. The Cadence suite (Cadence 2013) was also used to analyze the b19 benchmark in .def format.

For each HTH insertion, the characteristics are given along with the percentage increase compared to the HTH-free version. Furthermore, the evaluation of the impact of the HTHs has been conducted at several levels of abstraction.

In the following tables, the delay and power consumption evaluations are described as follows.

1) For HTHs inserted at RT level or gate level:

- "Gate level" lines: *i.e.*evaluation done on the Verilog netlist (in case of a HTH inserted at RT level, both HTH free and infected circuit have been previouslysynthesized to obtain a netlist).
- "Layout level" lines:*i.e.*evaluation done on the layoutafter the operation of place and route.
  In that case, the operations of place and route have been conducted separately for the HTH free circuit and for the circuit with the HTH in (a core utilization of 80% was used for each benchmark). This means that there may have been a place and route quite different for the two circuits that can lead to significant differences, not necessarily due to the addition of the HTH.
- "ECO level": in this case also, evaluationdone after place and route.
  However, in this case,the HTHhas been placed in the free space of the layout of the original circuit, thanks to the*Engineering Change Order* (ECO) optionof the IC Compiler tool. In this waythe HTH's gates are put along the existing gates with a minimum impact on the original placement and routing.

2) For HTH inserted at layout level:

- "Def level" lines: *i.e.*evaluation done on the layout with a HTH inserted manually at the layout level.

Figure 2 summarizes the flow and the different simulation performed. These different comparisons allow us to assess the impact of the level of abstraction used to do the evaluations and therefore to assess also the veracity of the results obtained at each level of abstraction.To the best of our knowledge, this is the first attempt at using the ECO option of a place and route tool to insert a HTH. This technique allows automating the insertion of a HTH in the layout while mimicking at bestwhat an adversary could do by manipulating the masks in the foundry.

C. Dynamic Power

Table III presents the HTH impact in terms of dynamic power. Firstly, one can note that the dynamic power is very undervalued at gate levelrelative to the layout level. This suggests that the gate-level analysis cannot replace an actual measurement. Secondly, the results are quite varied from one analysis to another (*e.g.* from -0.41% to -16.3% for the s15850 benchmark), making it difficult to know if the difference comes from theHTH or not. Besides, from these three examples, there is no general rule to deduct (*e.g.*always more impact on one level or another). Last but not least, one can see that the effect of the HTHs is minimal. This corroborates the assumption that a HTH is difficult to detect.

D. Static Power

Table IV presents the HTH impact in terms of leakage power. In this case, results at gate and layout level are closer. The effect of the HTHs is still minimal and the results still vary from one analysis to another.

E. Delay

Table V presents the HTH impact in terms of delay. We focused on the HTH inserted at gate level, which allowed us to clearly identify the paths affected by the HTH (finding the HTH fromthe two AES synthesized circuits was a much more complex task). First, a remark that applies to both benchmarks is that the different paths studied were far from being critical paths of the circuits.

The HTH inserted in the b19 benchmark contains 3 trigger paths and 1 payload path. All four signals are presented in the table. First, as one can see, the gate level estimations are much more pessimistic than the layout level estimations. Second, concerning more specifically the effect of the HTH, the additional delay is around +1% (resp. +5%) at gate level for the trigger paths (resp. the payload path). The layout level estimations show a shorter delay for 2 trigger paths out of 3, and an additional delay of 6% for the third one; as well as 4.3% for the payload path. As for the ECO mode, the additional cost is up to 15.5% for the trigger paths and 14.8% for the payload path. This is very different from previous results, which shows the strong influence of the place and route. Besides, the additional delayis generally greater in ECO mode. This is due to stronger constraints for place and route of theHTH when minimizing disturbances to the existing layout than when a new place and route is performed. For the same reasons of complexity of place and route, the additional cost is also important concerning the layout inserted HTH.

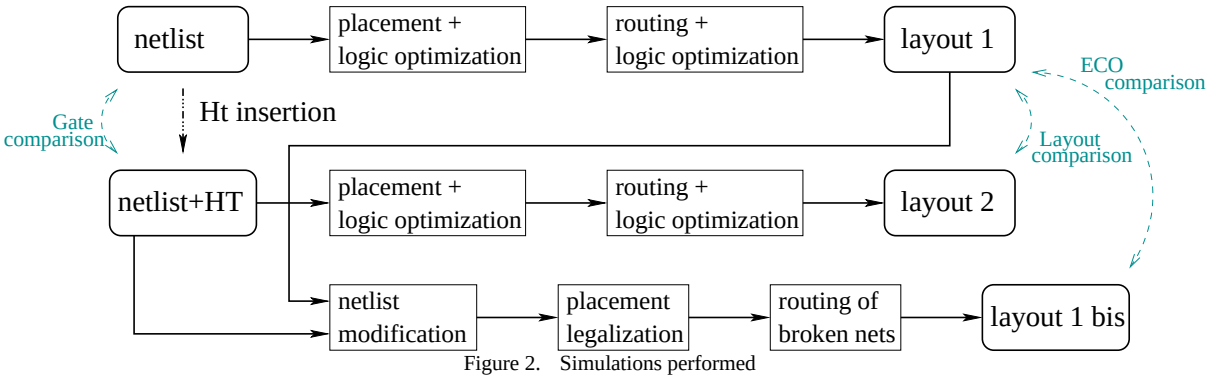

Figure 2. Simulations performed

TABLE IV. HT IMPACT ON DYNAMIC POWER

		HT free (µW)	**HT in (µW, %)**
b19	Gate level	3 731.4	3 696.3 **(-0.94%)**
	Layout level	9 595.2	9 600.2 **(+0.05%)**
	ECO level		4 556.6 **(-52.5%)**
	Def level	11 330	11 340 **(+0.09%)**
s15850	Gate level	751.34	748.23 **(-0.41%)**
	Layout level	1 260.7	1 236.6 **(-1.9%)**
	ECO level		1 054.8 **(-16.3%)**
AES	Gate level	21 920.3	22 329.7 **(+1.87%)**
	Layout level	35 718.8	36 628.6 **(+2.55%)**
	ECO level		36 177.0**(+1.28%)**

TABLE III. HT IMPACT ON LEAKAGE POWER

		HT free (µW)	**HT in (µW, %)**
b19	Gate level	3 457.9	3 465.4 **(+1.8%)**
	Layout level	3 438.3	3 447.4 **(+0.2%)**
	ECO level		3 465.4 **(+0.8%)**
	Def level	2 533	2 539 **(+0.24%)**
s15850	Gate level	127.23	129.52**(-0.41%)**
	Layout level	125.03	126.05 **(+0.8%)**
	ECO level		129.54 **(+3%)**
AES	Gate level	4 985.3	4 983.1 **(-0.04%)**
	Layout level	4 990.0	4 987.3 **(-0.05%)**
	ECO level		4 991.1 **(+0.02%)**

TABLE V. HT IMPACT ON PATH DELAY

			HT free (ns)	**HT in (ns, %)**
b19	Trigger path 1	Gate level	30.05	30.33 **(+0.9%)**
		Layout level	3.09	3.27 **(+5.8%)**
		ECO level		3.57 **(+15.5%)**
		Def level	10.23	10.61 **(+3.7%)**
	Trigger path 2	Gate level	30.05	30.64 **(+1,9%)**
		Layout level	3	2.96 **(-1.3%)**
		ECO level		3.44 **(+14.7%)**
		Def level	10.32	12.76 **(+23.6%)**
	Trigger path 3	Gate level	30.79	30.90 **(+0.36%)**
		Layout level	2.94	2.86 **(-2.7%)**
		ECO level		3.14 **(+6.8%)**
		Def level	10.25	12.08 **(+17.9%)**
	Payload path	Gate level	13.54	14.29 **(+5.5%)**
		Layout level	1.15	1.20 **(+4.3%)**
		ECO level		1.32 **(+14.8%)**
		Def level	5.28	5.53 **(+4.7%)**
s15850	Trigger path 1	Gate level	1.68	1.70**(+0.9%)**
		Layout level	1.26	1.31**(+3.6%)**
		ECO level		1.30**(+3.3%)**
	Trigger path 2	Gate level	1.72	1.73**(+0.8%)**
		Layout level	1.19	1.18**(-1%)**
		ECO level		1.23**(+3.7%)**
	Trigger path 3	Gate level	0.71	1**(+41.9%)**
		Layout level	0.19	0.22**(+14.1%)**
		ECO level		0.80**(+308%)**
	Trigger path 4	Gate level	0.69	0.99**(+43.3%)**
		Layout level	0.18	0.20**(+12.1%)**
		ECO level		0.79**(+334.6%)**
	Payload path	Gate level	0.1	0.2**(x2)**
		Layout level	0.0007	0.06**(x85)**
		ECO level		0.2**(x285)**

The HTH inserted in the s15850 benchmark contains 32 trigger paths and 1 payload path. The four paths with the largest and smallest additional costs are presented in the table. The average for the 32 paths is +5.9% at gate level, +7.3% at layout level and +45% for the ECO mode. Once again, one can notice the difference between the estimations at gate level and at layout level. Then, one can notice for this benchmark much larger differences at the layout level: up to +14% in layout mode and +334% in ECO mode for a trigger path. In addition to place and route constraints in ECO mode, it was observed for that benchmark thatthe place and route tools performed severallogic optimizations.The large extra costs in ECO mode come from the fact that the paths have been optimized differently in the two experiments. In the end, the two paths that are compared are not exactly the same(less buffers, gates with a different drive strength, *etc.*) regardless of whether a HTH has been inserted or not. This prevents to know whether the differences come from the HTH or not. Last, let us notice that it is difficult to draw conclusions about the payload path because it is a very special case. Without the HTH, this path is optimized during place and route and consists only of a wire between a primary input and a primary output. After insertion of the HTH, the path does contain a multiplexer, hence leading to a huge extra delay.

V. CONSIDERATIONS ON POWER AND DELAY MEASUREMENTS

In addition to the above-mentioned experimental-based considerations, there are some concerns purely related to the physical measurement of the power consumption and the delay of logic paths.First, let us mention the problem of PE variations. This problem is beyond the scope of this paper and is already widely discussed in the literature(Wei, *et al.*, 2012). We will focus instead on the feasibility of the measures; problem that would persist even in lack of variations.

A. Dynamic power

The main issue related to dynamic power consumption is that it strongly depends on the effectiveness of the test vectors used during power measurements. Indeed, if the logic gates belonging to the HTH do not switch, their contribution is not visible. In other words, the dynamic power induced by the HTH will remain stable as long as the HTH is not activated, which is rarely mentioned in the literature.

In this paper, vector-free dynamic power analysis has been conducted. One further question still remains: is a vector free analysis accurate enough? In other words, would the results be comparable with analysis using simulation and precise switching activity?

For the dynamic power analysis to be as representative as possible, it would be interesting that benchmarks be provided with user defined switching activity, since accurate power analysis depends on accurate signal activity.

B. Delay

The basic assumption of detection methods based on the measurements of path delay is that the presence of a HTH increases the delay of the paths that are impacted by the HTH. However, if one refers to the HTH model in Figure 1(Wolf, *et al*., 2008), one can notice that the different paths impacted by a HTH are only little affected from a delay point of view:

- Only one gate is usually added to the payload path (defined as the *payload gate*), which is very little from a delay point of view.
- The trigger paths are even less affected: the HTH only increases the fan-out of the logic gates that drive the first gate of the HTH (these gates are defined as the *driver gates*), therefore its response time becomes longer.

By measuring the delay of the paths that includes the *driver gate* or the *payload gate*, it should be possible to detect the presence of a HTH, however, the time difference is so small that it requires very precise measurements. This issue is not discussed in the literature.

Unexpected delay variations are well known in manufacturing testing. Structural defects affecting the transmission delay of gates or paths are modeled as *delay fault*s (Gate or Path Delay Faults). These faults are tested by generating test vectors that are able to excite the gate where the fault is supposed to modify its delay. These vectors intend to apply a transition (from 0 to 1 and from 1 to 0) at the gate input and to propagate this transition to an observable node (either a primary output or the input of a flip-flop). The test consists in checking the transition time at the output. Even if the use of test patterns for delay faults may seem a good procedure to find the presence of a HTH(like the method proposed in (Jin, *et al*., 2008)), there are substantial differences between testing a delay fault and detecting a HTH. Indeed, a delay fault is detected when it increases the propagation time in such away that it reaches the ending point later than the clock period(*i.e.*incorrect data are stored in flip-flops or captured on circuit outputs). In this context, only the delay faults affecting the circuit behavior at its nominal frequency are under the scope of delay testing activity.Generally, only 10% of the critical paths are tested wrt these faults assuming that delay-related defects on short paths could not affect the circuit behavior. Nevertheless, HTHs can be inserted anywhere in the design and, preferably on short paths such that they cannot be detected by delay fault testing.

Thus, standard delay test would fail for detecting HTHs.The following test procedure could be imagined. For each gate to be tested:

1. Find a path (possible the longest, to help point 3) that includes that gate, from a starting point to an ending point;
2. Find two couples of test patterns that allows testing the rising and falling transitions on that gate;

3. Set the clock period to the expected delay for that path (by using the golden model as reference). The period could be much shorter that the most critical path of the circuit, thus generating several timing violations that should be ignored. However, for the target path, there will not be violations.
4. Check if the result is correct. If the result is not correct, the additional delay that did not allow the transition to be correctly captured is imputed to the presence of a HTH.

Nevertheless, this procedure has very strong practical limitations. Indeed, for very short paths, the procedure would require an increase of the clock frequency that may not be easy to manage because of the parasitic capacitances on the clock network, which would filter high frequencies. This procedure would clearly become not practicable in the extreme case where the HTH is inserted between two flip-flops belonging to a shift register.

Eventually, even if it existed a technique able to precisely measure the delay of each gate, the attacker could slightly modify the circuit by resizing the driver gate, so that the increase of its fan-out would be compensated. In this way, no additional delay would be measured, such as mentioned in (Wei, *et al.*, 2012). However, to be performed by the attacker, this technique requires more skills.

VI. Conclusion

While side-channel analysis has been reported as an effective approach to detect HTHs, it seems that most approaches in literature lack at presenting satisfactory simulation results to prove the usefulness of the detection method. Power consumption and delay analysis is sensitive to process and test environment variations. Moreover, process variations increase with the shrinking feature size in VLSI technologies. Therefore, the impact of a HTHcan be so small that it can be hidden within the fluctuation to variations.Proposed solutions have addressed this problem but not the one of simulation imprecisions. However, for the simulations to be as close as possible to the real experiments, HTHs insertion and proposed side-channel detection techniques should be performed using layout level information.The same study could be done concerning EM analysis, in order to evaluate the capability of analysis tools such as RedHawk-SEM (Apache, 2013) to detect the presence of HTH.

A second important point about the analysis of a detection method is to use experimented HTHs that are representative of real threats. This is not always the case in some mentioned approaches.

Due to the lack of available real HTHs on fabricatedICs, the only option apart from simulation-based approachesis the use of a FPGA such as in the SASEBO board (Bechtsoudis, Sklavos, 2010). Once again, whether such measures may reflect measurements made on real ICs is another worthwhile question.

Furthermore, the difficulty of testing manufactured ICs is seldom investigated, especially in terms of delay measurements. In fact, delay based techniques do not seem realistic:not only measuring all paths on a chip seem not practical, especially for short paths, but alsothese measurements will not be effective against even the simplest HTH hiding techniques such as gate resizing.

All these facts underline the need of benchmarks for evaluating side-channel analysis approaches, such as the ones proposed in the Trust-Hub website (Trust-hub, 2013), as well a strict rules on the use of simulation tools. Until now, it is indeed difficult to compare the different approaches and differentiate the most effective one.

Acknowledgments

This project has been funded by the French Government under grant FUI #14 **HOMERE** (**H**ardware tr**O**jans :**M**enaces et robust**E**sse des ci**R**cuitsint**E**grés).

References

Wang, X. Tehranipoor, M., & Plusquellic, J. (2008). Detecting Malicious Inclusions in Secure Hardware: Challenges and Solutions. In Proceedings of the IEEE International Workshop on Hardware-Oriented Security and Trust (HOST'08), pp. 15–19.

Tehranipoor, M., & Koushanfar, F. (2010). A Survey of Hardware Trojan Taxonomy and Detection. InIEEE Design & Test of Computer, 27:10– 25.

Rajendran, J., Gavas, E., Jimenez, J., Padman, V., & Karri, R. (2010)Towards a comprehensive and systematic classification of HT. InProceedings of the *IEEE International Symposium on Circuits and Systems (ISCAS'10)*, pp. 1871–1874.

Jin, Y., &Makris, Y. (2012) Proof Carrying-Based Information Flow Tracking for Data Secrecy Protection and Hardware Trust. In Proceedings of the IEEE VLSI Test Symposium (VTS'12), pp. 252–257.

Hicks, M., Finnicum, M., King, S.T., Martin, M.M.K., & Smith, J.M. (2010) Overcoming an Untrusted Computing Base: Detecting and Removing Malicious Hardware Automatically. InProceedings of the IEEE Symposium on Security and Privacy (SP'10), pp. 159–172.

Trust-Hub Website. https://trust-hub.org/ (2013).

Torrance, R.,& James, D. (2011) The state-of-the-art in semiconductor reverse engineering. In Proceedings of the Design Automation Conference (DAC'11), pp. 333–338.

Agrawal, D., Baktir, S., Karakoyunlu, D., Rohatgi, P., & Sunar, B. (2007)Trojan Detection using IC Fingerprinting. In Proceedings of the IEEE Symposium on Security and Privacy (SP'07), pp. 296–310.

Jin, Y., & Makris, Y. (2008) Hardware Trojan Detection Using Path Delay Fingerprint. In Proceedings of the IEEE International Workshop on Hardware-Oriented Security and Trust (HOST'08), pp. 51–57.

Rad, R.M., Wang, X., Tehranipoor, M., & Plusquellic, J. (2008) Power Supply Signal Calibration Techniques for Improving Detection Resolution to Hardware Trojans. In Proceedings of the IEEE/ACM International Conference on Computer-Aided Design (ICCAD'08), pp. 632–639.

Banga, M.,Chandrasekar, M., Fang, L., & Hsiao, M.S. (2008)Guided Test Generation for Isolation and Detection of Embedded Trojans in ICs. In Proceedings of the ACM Great Lakes Syposium on VLSI (GLSVLSI'08), pp. 363–366.

Banga, M., & Hsiao, M.S. (2008) A Region Based Approach fot the Identification of Hardware Trojans. In Proceedings of the International Workshop on Hardware-Oriented Security and Trust (HOST'08), pp. 40–47.

Du, D., Narasimhan, S., Chakraborty, R.S., & Bhunia, S. (2010) Self- referencing: A Scalable Side-Channel. In Proceedings of the International Conference on Cryptographic Hardware and Embedded Systems (CHES'10), pp. 173–187.

Salmani, H., Tehranipoor, M., & Plusquellic, J. (2010) A Layout-aware Approach for Improving Localized Switching to Detect Hardware Trojans in Integrated Circuits. In Proceedings of the IEEE International Workshop on Information Forensics and Security (WIFS'10), pp. 1–6.

Banga, M.,& Hsiao, M.S. (2009) A Novel Sustained Vector Technique for the Detection of Hardware Trojans. In Proceedings of the 22nd International Conference on VLSI Design (VLSI'09), pp. 327–332.

Alkabani, Y.,& Koushanfar, F. (2009) Consistency-based characterization for IC HT detection. In Proceedings of the International Conference on Computer-Aided Design (ICCAD'09), pp. 123–127.

Li, M., Davoodi, A., & Tehranipoor, M. (2012) A Sensor-Assisted Self- Authentication Framework for Hardware Trojan Detection. In Proceedings of the Design, Automation and Test in Europe (DATE'12), pp. 1331–1336.

Potkonjak, M., Nahapetian, A., Nelson, M., & Massey, T. (2009) HardwareTrojan horse detection using gate-level characterization. In Proceedings of the 46th ACM/IEEE Design Automation Conference (DAC'09), pp. 688–693.

Narasimhan, S., Du, D., Chakraborty, R.S., Paul, S., Wolff, F., Papachristou, C., Roy, K., & Bhunia, S. (2010) Multiple-Parameter Side-Channel Analysis: A Non-Invasive Hardware Trojan Detection Approach. In Proceedings of the IEEE International Workshop on Hardware-Oriented Security and Trust (HOST'10), pp. 13–18.

Onabajo, M.,& Silva-Martinez, J. (2012) Analog Circuit Design for Process Variation-Resilient Systems-On-A-Chip, Springer.

Pang, L.T., Qian, K., Spanos, C.J., & Nikolic, B. (2009)Measurement and Analysis of Variability in 45 nm Strained-Si CMOS Technology". In IEEE Journalof Solid-State Circuits, vol. 44,*n°8*.

Wei, S., Li, K., Koushanfar, F., & Potkonjak, M. (2012) Hardware Trojan horse benchmark via optimal creation and placement of malicious circuitry. In Proceedings of the Design Automation Conference (DAC'12), pp. 90–95.

Synopsys Website. http://www.synopsys.com/ (2013).

Goldman, R., Bartleson, K., Wood, T., Kranen, K., Cao, C., Melikyan, V., & Markosyan, G. (2009) Synopsys's Open Educational Design Kit: Capabilities, Deployment and Future. In Proceedings of the IEEE International Conference on Microelectronic Systems Education (MSE'09), pp. 20–24,.

Cadence Website. http://www.cadence.com/ (2013).

Wolff, F., Papachristou, C., Bhunia, S., &Chakraborty, R.S. (2008)Towards Trojan-Free Trusted ICs: Problem Analysis and Detection Scheme. In Proceedings of the Design, Automation and Test in Europe (DATE'08), pp. 1362–1365.

Apache Website. http://www.apache-da.com/ (2013).

Bechtsoudis, A., & Sklavos, N. (2010) Side Channel Attacks Cryptanalysis Againt Block Ciphers Based on FPGA Devices. In Proceedings of the IEEE Computer Society Annual Symposium on VLSI (ISVLSI'10), pp. 460–461.

BIOGRAPHIES

Sophie Dupuis received the M.S. degree in Integrated Systems Architectures and Micro-Electronics and the PhD degree in Computer Science from the Laboratoire d'Informatique de Paris 6 (LIP6) at UniversityPierre & Marie Curie (France), in 2004 and 2009 respectively. She is currently an Associate Professor at the Laboratoire d'Informatique, de Robotique et de Microélectronique de Montpellier (LIRMM) at University Montpellier 2 (France). Her research interests include VLSI design, CAD tools, andare currently particularly oriented toward the conception and verification of digital and secure circuits.

Giorgio Di Natale received the PhD in Computer Engineering from the Politecnico di Torino (Italy) in 2003. Currently, he is a researcher for the French National Research Center (CNRS) at the LIRMM laboratory in Montpellier. His research interests include test, reliability, and fault tolerance of digital circuits, focusing in particular on 3D circuits and secure devices. He serves the European Test Technology Technical Council of the IEEE Computer Society as Vice Chair, and he is the Action Chair of the COST Action IC1204 (TRUDEVICE).

Marie-Lise Flottes received her M.S. degree in Electrical Engineering and PhD degree in Microelectronics from the University of Montpellier (France), in 1987 and 1990 respectively. She is currently researcher for the French National Scientific Research Center (CNRS). Since 1990, she has been conducting research in the domain of digital system testing at LIRMM laboratory (France). Her research interests include Design For Testability, Test Infrastructure for Integrated Systems (SoC, SiP and three-dimensional Systems), Testability and Fault Tolerance of Secure Circuits/Systems.

Bruno Rouzeyrereceived the master degree in Mathematics in 1978, Doctoratedegree (PhD) degree on CAD in 1984, all degreesfrom the University of Montpellier. Currently, heisProfessorat the University of Montpellier and conductshisresearchat LIRMM. Hisresearchinterestsincludeseveral aspects of CAD for digital circuits and are particularlyorientedtowardoptimization, verification, test and test synthesis of digital and secure circuits.