Using Approximate Circuits Against Hardware Trojans

Honorio Martin, Sophie Dupuis, Giorgio Di Natale, Luis Entrena

Using Approximate Circuits Against Hardware Trojans

Honorio Martin Sophie Dupuis Giorgio Di Natale and Luis Entrena

***Abstract*—Hardware Trojans (HTs) are malicious alterations in Integrated Circuits (ICs) that pose an important threat to safety-critical systems. Many techniques based on logic testing or side-channel analysis have been proposed in the literature aiming at detecting such malicious modifications in fabricated ICs. The detection of HTs is becoming more challenging with the shrinking of the technology and the impact of process variations. Therefore there is a need to neutralize the effect of HTs when the typical detection mechanism fails. In this work, we propose to tackle the effect of HTs by leveraging fault-tolerant techniques like Triple Modular Redundancy (TMR). More specifically, we propose to use an approximate TMR in order to neutralize the effects of HTs while saving area and increasing the complexity of inserting HTs. The efficiency of the proposed approach has been evaluated by using the ISCAS'85 benchmarks and stealthy ad-hoc HTs.**

***Index Terms*—Design-for-Hardware-Trust, Hardware Trojan, Approximation.**

I. Introduction

Globalization and the need to lower costs in the design and manufacturing processes of Integrated Circuits (ICs) require the involvement of many third-party companies in the IC industry. This model has proved unreliable due to the impossibility of guaranteeing the trustworthiness in all the steps of the design and manufacturing flow. In this context, Hardware Trojans (HTs), defined as malicious modifications that damage the functionality or/and the trustworthiness of ICs, constitute a potential threat that is growing in the IC industry.

HTs can be inserted in ICs in almost all design steps, e.g. RTL design, logic and physical synthesis and manufacturing process. Denial-of-Service and leakage of confidential information are among the common goals of an HT attack. An HT is expected to evade different detection mechanisms, executed at both pre- and post-manufacturing processes. Indeed, they are designed to be activated under very rare conditions and to have a tiny footprint (in terms of area occupancy, performance degradation and power consumption).

The hardware security and trust research community has been focused on developing effective detection mechanisms to uncover different kinds of HTs during the design and manufacturing processes of ICs. Among the tools that can detect HTs in pre-silicon phase stand out the COTD tool, VeriTrust, FANCI or the recently published HTDet tool [1]. These tools have proven to be effective against the HTs contained in widespread HT benchmarks. Nevertheless, researchers have also shown that some of these schemes can be circumvented [2]. Among the post-fabrication detection methods stand out those based on side-channel analysis or logic testing [1]. Finally, different prevention methods have been developed during the last decade. These so-called Design-for-Trust or Design-for-Hardware-Trust (DfHT) techniques include the encoding of internal registers, scan flip-flops insertion and logic locking [1]. All in all, it is recommended to use some of these prevention and detection techniques in order to prevent HT attacks.

In the case of critical systems such as military or space applications, HT threat poses a special challenge due to the high economic and strategic interests at stake. In fact, in 2007, DARPA initiated its TRUST program to develop technologies that ensure the trust of ICs used in military systems such as weapons systems, but designed and fabricated under untrusted conditions.

Some of these critical systems typically embed fault-tolerant techniques for mitigating the effects of aging, single event upsets or single event transients. The most straightforward fault-tolerant techniques are based on full replication: Dual or Triple Modular Redundancy (DMR or TMR).

The use of DMR and TMR to thwart HTs has been introduced in [3], [4], [5]. However, straightforward replication is not considered as an obstacle to insert an HT in these ICs. Indeed, replicating the HT in all replica of the original circuit will successfully activate the HT.

In this paper, we extend the work presented in [6] where we proposed the use of a novel approximation circuit technique [7] in order to make more difficult the insertion of an HT, and, even if present, to neutralize its effects during the lifetime of devices. In this work, we deepen into the explanation of the proposed method, introducing a different variant of the neutralization mechanism and extending the experimental results to other circuits.

The rest of the paper is organised as follows. In Section II, we present a brief description of the the considered threat model, the HT prevention methods based on redundancy and the basis of the used approximation method. In Section III, we describe the proposed approach including two different variants. In Section IV are presented the experimental results and the discussion about the proposed method. Finally, some conclusions are drawn in Section V.

H. Martin and L. Entrena are with Department of Electronics Technology, Universidad Carlos III de Madrid, (e-mail: (hmartin,entrena)@ing.uc3m.es)

S. Dupuis is with LIRMM, Univ. Montpellier, CNRS, (e-mail: (dupuis@lirmm.fr)

G. Di Natale is with TIMA, Univ. Grenoble Alpes, CNRS, Grenoble INP, (e-mail: (giorgio.di-natale@univ-grenoble-alpes.fr)

II. Related work

A. Threat model

The threat model used in this work put the focus on digital IPS and trigger activated digital HTs which have digital payloads. Such HTs are commonly divided into two parts : the triggering condition (or trigger) that activates the HT, and the payload that introduces the wrong behavior [8].

Regarding the trigger, it is commonly agreed that a stealthy triggering condition must be created to evade detection i.e. the HT must be activated under an extremely rare condition that is not likely to occur during the ICs test procedure. In addition, the HT must not impact delay and impact the layout as little as possible. An attacker is then likely to create triggers by choosing as trigger inputs low-controllable nodes – individually excited to their rare value – with a positive time margin, and by grouping them according to their proximity in the layout.

The goal of many logic-based detection methods is to activate such HTs during the test phase in order to observe an erroneous behavior. The considered scenario contemplates that different detection systems (logic testing, side-channel, etc) have failed in the detection of such HTs and safety-critical systems have been deployed in the field containing the malicious modification.

The target of the proposed technique will be to neutralize the payload of potential HTs.

B. HT prevention methods based on redundancy

The use of DMR to thwart HT insertion was introduced in [3]. This technique is based on the creation of a redundant and functionally equivalent circuit to the original one along with a comparator. If an HT is inserted in one of the two replicas, the comparator reports the abnormal behavior once the HT is activated and both replicas do not provide the same value. Such technique, therefore, allows monitoring the ICs once in the field. However, this proposal reports significant area overheads. Furthermore, further research is needed to prevent an attacker from inserting the same HT into both replicas. The insertion of the same HT in both circuits is indeed supposed to be prevented only by synthesising, placing and routing the original circuit and its replica into two different layouts. Despite these design differences, it was shown in [9] that it is almost impossible to create two circuits that do not contain nodes with identical behavior. An attacker indeed only needs small subsets of nodes with identical behavior to create two HTs that will be activated exactly at the same time.

The use of TMR to thwart HT insertion has been proposed in [10], [4], [5] by N. Gunti et al. In such a TMR based method, an HT has to be introduced in at least two copies in order not to be blocked by the majority voter. Authors claim that such duplication of a potential HT makes it relatively big, therefore also relatively easy to detect through side-channel based techniques. Besides, in order to limit area overhead, the proposed TMR is implemented only on carefully chosen paths of the IC. Authors also propose to maximize their neutralization rate through multiple levels of TMR implemented after logic partitioning. This choice is based on the assumption that paths leading to equally probable outputs are more vulnerable to HT insertion. Indeed, if an output has an equal probability of being '0' or '1', the effect of an HT is impossible to predict since the switching of '0' and '1' is morphed by the overall probability distribution. TMR is therefore implemented only on the paths that lead to equally probable outputs. Further work should be done to better assess the trade-off between area overhead and limitation in the choice of paths to duplicate and the possibility of inserting the same HT on two replicas of the TMR.

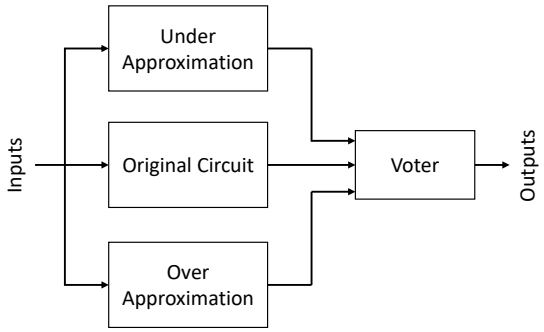

Fig. 1: TMR scheme using approximate circuits

C. Approximate Logic Circuits

An approximate logic function can be defined as a logic function that correctly predicts the result of the original function (G) for a fraction of its input space. We can define a logic function F which satisfies the implication $F \Rightarrow G$, i.e, $F \subseteq G$ as an under-approximation or 1-approximation with respect to G. Conversely, a logic function H is an over-approximation or 0-approximation of G if $\overline{H} \Rightarrow \overline{G}$ i.e. if $G \subseteq H$ [7].

Using the over and under approximation circuits instead of exact replicas, a circuit similar to the TMR can be designed as shown in Fig.1. In this scheme, the implication-relationship $F \subseteq G \subseteq H$ guarantees that the correct result is obtained in the absence of faults, because at least one of the two approximations agrees with the original circuit for every input vector. If approximations are properly chosen, relevant resource savings can be obtained with a low impact on the error masking capabilities.

In this work, a method for approximate circuit generation is used [7], denoted as fault approximation, which consists in assigning constant logic values to specific circuit nodes. The tool developed in [7] allows us to select different strategies depending on the final goal of the approximate circuits. We refer the reader to the original work for further details about circuit approximation and this tool.

III. Approximated TMR neutralization approach

In this work, we leverage the combined effects of two well-known techniques in the field of HT detection and Design-for-Reliability to neutralize HT effects. Firstly, our approach makes use of a logic-based detection principle that consists

in the discovery of nodes that are most likely to be used as trigger inputs. Secondly, an approximate TMR scheme is used to mask the errors induced by HTs. The selection of the nodes to be approximated is the cornerstone of this approach. As we use a fault approximation methodology, the circuit nodes to be approximated will depend on the fault testability of the circuit and the approximation strategy selected.

A. Fault testability assessment

It is necessary to assess the testability of the different nodes in order to apply different approximation strategies. For this purpose, a stuck-at fault model is applied to this process using the simulation tool HOPE [11]. HOPE provides information about the faults which are detected/undetected for each test vector, so the fault sensitivity will depend on the set of test vectors.

We have generated two different sets of test vectors. The first set of vectors is composed of 50,000 random test vectors, including stuck-at vectors provided by the Tetramax ATPG tool. This set of test vectors will derive in a representative distribution of the fault sensitivity of the circuit. The second set of vectors is obtained thanks to a tool generating test vectors dedicated to HT detection [8]. This tool aims at triggering potential triggers, according to the assumptions described in the threat model. This subset will lead to a biased fault sensitivity distribution towards the low controllable nodes.

B. Approximation strategy

Once the testability of each node has been obtained using different sets of test vectors, the next step is to decide which nodes to approximate (i.e. to connect to a constant value) based on their fault sensitivity. We have explored two opposite approximation strategies:

- **Strategy-1**: With this strategy, we aim at the approximation of the nodes that are more likely to be used as HT triggers. Therefore, we will approximate the nodes with a low fault sensitivity, tying them to logic constants.
- **Strategy-2**: With this strategy, in contrast to the previous approach, we aim at the approximation of the nodes with a high fault sensitivity because a HT that uses these nodes as trigger will be likely detected during the test phase.

Before delving into details, let us first introduce the concept of *testability threshold* that determines which nodes to approximate. In Strategy-1 (resp. Strategy-2), every node whose testability lies under (resp. over) the threshold value is approximated.

The testability threshold provides the required flexibility to the method. Setting a proper testability threshold according to the requirements of the target application is crucial, because it determines the actual trade-off between resource consumption and neutralization capabilities [7]. For instance, in Strategy-1, the lower the testability threshold, the fewer approximated nodes. This implies that approximate circuits will be more similar to the original one and therefore the error masking rate higher (in the extreme case where the testability threshold is set to 0, a pure TMR will be generated). Conversely, Strategy-2 follows the opposite trend, for which a higher testability threshold allows approximating more nodes. This results in greater savings in terms of area and power consumption, at the expense of reducing robustness (in the extreme case, a trivial approximation is generated).

The approximations are generated for each of the aforementioned set of test vectors and strategies. Faults that produce an under-approximation are assigned to one of the replicas of the original circuit, and faults that generate an over-approximation are assigned to the other replica. Using these approximations, the circuit shown in Fig.1 is generated. A different approach in terms of synthesis, place and route can be followed in each of the TMR blocks to hinder an attacker from infering information of the complete scheme. Furthermore, it is important to note that the voting system will be subjected to an exhaustive test in order to guarantee that it is HT free, as proposed in [3]. As this is a critical point for our proposal, spare logic (e.g. scan chain) can be added in order to guarantee the correct functionality of the voting system. In addition, physical inspection and advanced image processing techniques can be used to that task.

IV. Experimental Results and analysis

A. Methodology

To show the feasibility of the proposed neutralization method and to perform a preliminary analysis of its efficiency, the following experimental set-up was devised.

As in other similar works that use TMR as neutralization method [10], [4], [5], we have selected the ISCAS'85 benchmarks as target circuits [12]. We have selected two circuits – c499 and c7552 – based on their different sizes and functionalities, to carry out a thoroughly study about the proposed approach. The c499 circuit is a 32-bit Single-Error-Correcting circuit with 41 inputs and 32 outputs. The c7552 circuit is a 34-bit adder and magnitude comparator with input parity checking of 207 inputs and 108 outputs. For both circuits, we have completed an in-depth study including a complete scan of thresholds and numerous HTs.

As explained before, the first step of our approach consists in assessing the fault testability of the different nodes in order to generate the approximations. Fig.2 and Fig.3 show the fault sensitivity distribution of each circuit for two sets of test vectors: 50,000 random vectors (RND) and vectors dedicated to HT detection, termed as *HT detection vectors* (HTD). It can be appreciated how the fault sensitivity changes with different test vectors. On the one hand, the vector set containing 50,000 random test vectors generates a more abrupt error distribution, which means that a high percentage of the errors are concentrated in a few nodes. On the other hand, the set containing HT detection vectors (around 500 vectors) produces a smooth error distribution. It is important to remark that in the second case, some nodes are not considered as faulty nodes because they are not even tested. Taking as a reference these error distributions, several approximate circuits have been generated using different testability thresholds and both approximation strategies.

For each of the aforementioned circuits, we have generated 30 infected versions that contain HTs designed using the assumptions described in the threat model, that is, HTs triggered

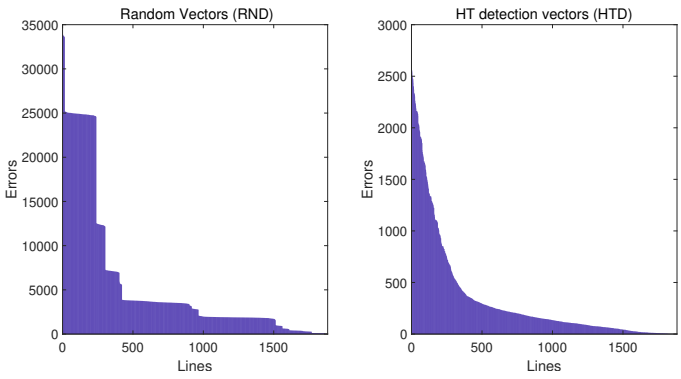

Fig. 2: c499 Fault distribution

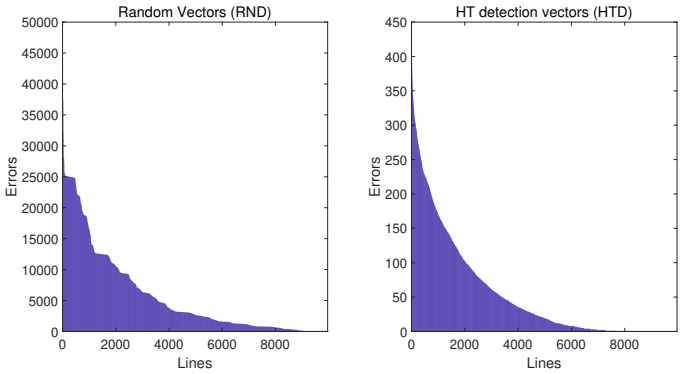

Fig. 3: c7552 Fault distribution

by subsets of low controllable nodes (individually excited to their rare value) with a positive time margin and in close proximity in the layout. Different sizes of triggers have been created: 2, 4 and 8 inputs-triggers (it is commonly believed that larger sizes would generate too large HTs, hence easily detectable). The HTs' triggers depend on the rare value of each trigger input – e.g. for a 2-input trigger with both nodes low controllable to 1, the trigger will consist of an AND gate – and the payloads consist of a XOR gate that inverts a randomly chosen output when the trigger is activated.

After that, a TMR scheme (cf. Fig.1) has been generated for each approximate circuit, replacing the original circuit with an infected circuit. Each TMR scheme has been simulated using 50,000 random test vectors (different from those used in the generation) in Modelsim and then synthesised using the Saed90 library, Synopsys and the default synthesis options.

B. Results for Strategy-1

Table I summarizes the results for both circuits using Strategy-1. The column *vectors* point out the set of vectors used to generate the approximated circuits (RND or HTD). The column *Trigger Inputs* indicates the complexity of the HT trigger mechanism (10 HTs for each of the different input-triggers have been tested). The column *Fault detected* corresponds to the number of faults neutralized by a TMR scheme where one of the replicas contains an HT. Finally, under the *Thresholds* label, we can find the percentages of neutralized faults with respect to the TMR, according to different thresholds used for the generation of the approximated

TABLE I: Percentage of Neutralized faults and area saving using Strategy-1

C499							
Vectors	Trigger Inputs	Faults detected	Thresholds 0.01	0.05	0.1	0.5	1
RND	2	6263	100 %	100 %	100 %	100 %	100 %
	4	10523	100 %	100 %	100 %	100 %	18 %
	8	1847	100 %	100 %	100 %	100 %	68 %
AREA Saving respect TMR			1 %	1 %	1 %	13 %	18 %
HTD	2	6263	100 %	100 %	100 %	90 %	0 %
	4	10523	98 %	97 %	97 %	75 %	54 %
	8	1847	100 %	99 %	99 %	82 %	7 %
AREA Saving respect TMR			-9 %	-9 %	-6 %	4 %	10 %
C7552							
Vectors	Trigger Inputs	Faults detected	Thresholds 1	5	10	15	20
RND	2	1614	100 %	100 %	100 %	100 %	100 %
	4	753	100 %	100 %	100 %	100 %	100 %
	8	126	100 %	100 %	100 %	100 %	100 %
AREA Saving respect TMR			13 %	43 %	54 %	58 %	66 %
HTD	2	1614	100 %	100 %	100 %	100 %	100 %
	4	753	100 %	100 %	100 %	99 %	99 %
	8	126	100 %	100 %	100 %	100 %	100 %
AREA Saving respect TMR			7 %	45 %	57 %	61 %	65 %

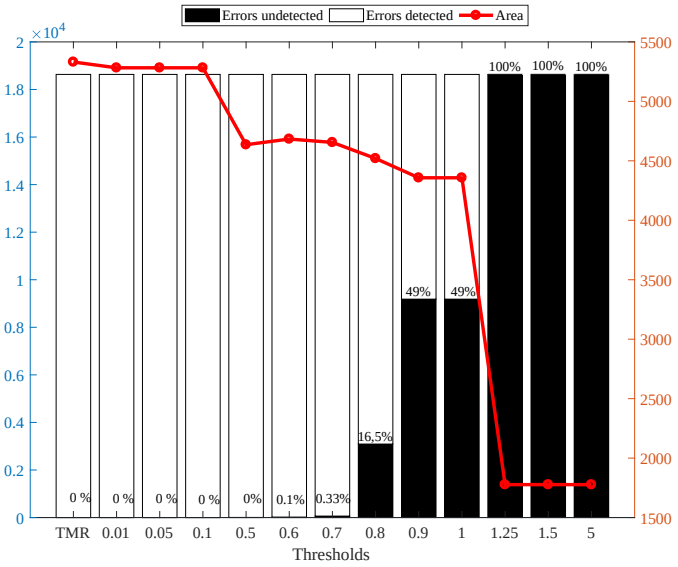

Fig. 4: Undetected/Neutralized errors and area vs thresholds for the circuit c499 (Strategy-1-RND vectors)

circuits: from 0.01 to 1 (resp. from 1 to 20) for circuit c499 (resp. c7552). This difference in the thresholds is due to the different sizes, architecture and functionality of the circuits that generate a completely different distribution of the node testability. In addition, the green row represents the area saving of our proposal with respect to the TMR scheme.

The top part of Table I shows the results for the c499 circuit. As can be seen, for the approximated circuits generated using the RND set of vectors, a threshold of 0.5 can be used to reduce the area by 13 % with respect to the full TMR, while neutralizing all the errors.

Very poor results were obtained in the case of the approximate TMR scheme generated using HTD vectors, where none of the generated approximations was able to thwart the effects of the HTs. This can be partly explained by the fact that important nodes (not considered as faulty nodes) were approximated and therefore the rare nodes, and consequently, the small size of the corresponding vector set.

TABLE II: Percentage of Neutralized faults and area saving using Strategy-2

C499							
Vectors	Trigger Inputs	Faults detected	Thresholds 95	90	85	80	70
RND	2	6263	100 %	100 %	100 %	100 %	100 %
	4	10523	100 %	100 %	100 %	100 %	100 %
	8	1847	100 %	100 %	100 %	100 %	100 %
AREA Saving respect TMR			0%	0 %	0 %	0 %	0 %
HTD	2	6263	100 %	100 %	100 %	100 %	81 %
	4	10523	100 %	100 %	100 %	91 %	75 %
	8	1847	100 %	100 %	100 %	94 %	49 %
AREA Saving respect TMR			0 %	0 %	0 %	2 %	5 %
C7552							
Vectors	Trigger Inputs	Faults detected	Thresholds 95	90	85	80	70
RND	2	1614	100 %	100 %	100 %	100 %	100 %
	4	753	100 %	100 %	100 %	100 %	100 %
	8	126	100 %	100 %	100 %	100 %	100 %
AREA Saving respect TMR			0 %	3 %	6 %	6 %	6 %
HTD	2	1614	100 %	100 %	100 %	100 %	81 %
	4	753	100 %	100 %	96 %	96 %	87 %
	8	126	100 %	100 %	100 %	100 %	61 %
AREA Saving respect TMR			-2 %	-2 %	-5 %	-8 %	-7 %

It is important to highlight the cases where the approximate TMR schemes use more area than the traditional TMR. In these cases, the synthesis tool may not manage well the optimization of logic constants obtaining an area overhead with respect to the original circuit. Nevertheless, this is a secondary effect that is only observable with low thresholds

Fig. 4 shows a more in-deep analysis of the results for circuit c499 using Strategy-1 and RND vectors, by detailing a full-scan for possible thresholds (from 0.01 to 5). The white bars represent the neutralized faults for all HTs. On the contrary, black bars are the undetected errors. In addition, we have depicted the percentage of undetected errors for each configuration.The area for each configuration(red line, left axe) is also depicted. A very good trade-off between neutralized errors and area saving is reached using a threshold of 0.7.

The bottom part of Table I shows the results for the c7552 circuit. For this circuit, a set of 20, 10 and 26 HTs have been designed with 2, 4 and 8 inputs-trigger respectively.

The obtained results show that the proposed approach is more effective for circuits with a larger footprint. More precisely, in our experiments, area saving starts to be noticeable when the total footprint is over the 3,000 Gates Equivalents (GE). In this case, a total of 2,493 errors have been originated by the HTs. Once again, the best results were obtained when random vectors (RND) were used to generate the approximations. It is noteworthy the area savings in both cases, RND and HTD. This is mainly due to the size of the circuit, which allows the approximation of many nodes resulting in area savings. In fact, the trivial approximation is almost reached for thresholds over 20%. Nevertheless, in this context, high area savings are not necessarily good because they may compromise the security of the circuit.

C. Results for Strategy-2

Table II shows the results of Strategy-2 where the nodes with a higher fault sensitivity are approximated. The number of HTs used to validate this strategy is the same than for Strategy-1. In that case, the higher thresholds are presented in descending order from 95 to 70 for both circuits.

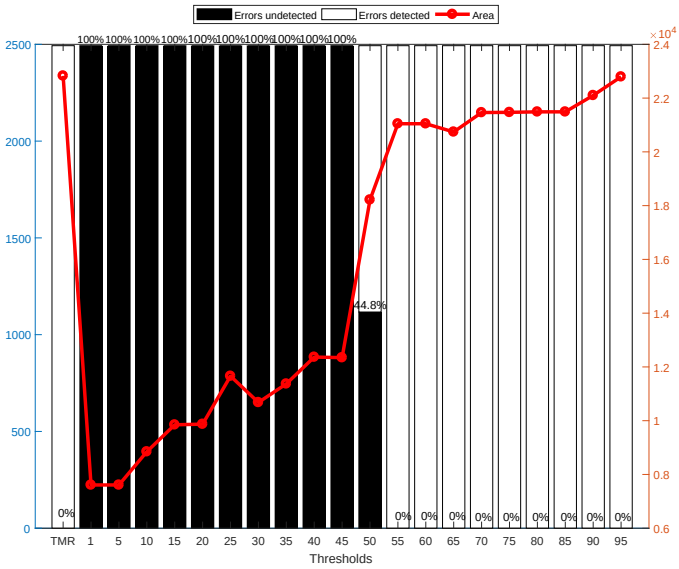

Fig. 5: Undetected/Neutralized errors and area vs thresholds for the circuit c7552 (Strategy-2-RND vectors)

It can be seen that it is not possible to reach an acceptable rate of neutralized faults while saving area. An area saving of a 6% is reached for the circuit c7552 circuit using RND vectors.

Fig. 5 illustrates a full-scan of thresholds for the c7552 circuit using Strategy-2 and RND vectors. It can be appreciated that only a few nodes are approximated for high thresholds, thus the area saving is minimum (red line). The area saving is noticeable when using a threshold lower than 50% but the percentage of neutralized errors is very low ($\sim 50\%$). In the rest of the cases, for both circuits, (included the results for the HT detection vectors) where all errors are neutralized, the area used is the TMR area or more.

The use of this approach has been discarded for future developments.

D. Discussion

The results presented for Strategy-1 show that the proposed approach is valid to neutralize HTs that could be inserted during the design and manufacturing processes. In a more generic way, we have also made experiments on other ISCAS's circuits, obtaining similar results.

There are two main advantages in comparison with other neutralization techniques that use TMR ([4] and [5]): resource savings and the use of approximations itself. On the one hand, the area reduction achieved with this technique can suppose an important cost-saving in complex circuits and makes easier to detect HTs by using side-channel techniques. On the other hand, the use of approximations makes impossible to integrate the same HT in the three TMR replicas. In addition, it makes difficult to design an HT not detectable during the test phase because a little change in the original circuit will generate several mismatches in the TMR output. Although we present results for combinational circuits, this technique can be easily

implemented for sequential circuits creating TMRs for each combinational part of the circuit.

The main limitation of the proposed approach is the assumption of using free-HT voters in TMR schemes. As suggested on [3], they could be exhaustively tested even using visual inspection techniques if the size of the circuit allows it. The voting system can also serve as a starting point to reverse-engineering the scheme, so using an obfuscation strategy for the implementation of the replicas is recommended. Finally, this HT neutralization system is expensive in terms of resources so is intended only for safety-critical systems that need to guarantee their functionality at any cost.

V. Conclusions

HTs pose a major threat for today's safety-critical systems and applications. In this work, we have devised an effective method based on approximated circuits that can neutralize the effect of HTs. The proposed method makes use of a fault approximation methodology to decide which circuit nodes to approximate. We have considered different sets of test vectors to assess the fault testability of the circuit nodes and different approximation strategies. With the generated under/over-approximations, an approximate TMR has been generated. Through experiments, we have proved that our TMR scheme is effective in the neutralization of stealthy HTs.

The future work for this study will include the selection of different test vectors (e.g. RND+HTD) and other approximation methodologies that are not based on fault testability. In addition, we will try to provide a metric to show the increased difficulty of inserting an HT without being detected.

References

[1] C. Dong, Y. Xu, X. Liu, F. Zhang, G. He, and Y. Chen, "Hardware trojans in chips: A survey for detection and prevention," *Sensors (Switzerland)*, vol. 20, no. 18, pp. 1–37, 2020, cited By 0.

[2] J. Zhang, F. Yuan, and Q. Xu, "Detrust: Defeating hardware trust verification with stealthy implicitly-triggered hardware trojans," ser. CCS '14. New York, NY, USA: Association for Computing Machinery, 2014, p. 153–166. [Online]. Available: https://doi.org/10.1145/2660267.2660289

[3] M. Palanichamy, P.-S. Ba, S. Dupuis, M.-L. Flottes, G. Di Natale, and B. Rouzeyre, "Duplication-based concurrent detection of hardware trojans in integrated circuits," in *Workshop on Trustworthy Manufacturing and Utilization of Secure Devices (TRUDEVICE)*, 2016, pp. 1–4.

[4] N. B. Gunti and K. Lingasubramanian, "Effective usage of redundancy to aid neutralization of hardware Trojans in Integrated Circuits," *Integration, the VLSI Journal*, vol. 59, no. January, pp. 233–242, 2017. [Online]. Available: http://dx.doi.org/10.1016/j.vlsi.2017.06.002

[5] N. B. Gunti and K. Lingasubramanian, "Neutralization of the effect of hardware trojan in scada system using selectively placed tmr," in *2017 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS)*, 2017, pp. 99–104.

[6] H. Martin, L. Entrena, S. Dupuis, and G. Di Natale, "A novel use of approximate circuits to thwart hardware trojan insertion and provide obfuscation," in *2018 IEEE 24th International Symposium on On-Line Testing And Robust System Design (IOLTS)*, 2018, pp. 41–42.

[7] A. Sanchez-Clemente, "Transient error mitigation by means of approximate logic circuits," Ph.D. dissertation, Departamento de Tecnologia Electronica, Universidad Carlos III de Madrid, Nov 2017.

[8] S. Dupuis, P.-s. Ba, M.-l. Flottes, G. Di Natale, and B. Rouzeyre, "New Testing Procedure for Finding Insertion Sites of Stealthy Hardware Trojans," in *Design Automation & Test in Europe (DATE)*, 2015, pp. 776–781.

[9] S. Dupuis, M. Flottes, G. Di Natale, and B. Rouzeyre, "Protection against Hardware Trojans with Logic Testing: Proposed Solutions and Challenges Ahead," *IEEE Design and Test*, 2017.

[10] N. B. Gunti, A. Khatri, and K. Lingasubramanian, "Realizing a security aware triple modular redundancy scheme for robust integrated circuits," in *IEEE/IFIP International Conference on VLSI and System-on-Chip (VLSI-SoC)*, 2014.

[11] H. K. Lee and D. S. Ha, "Hope: an efficient parallel fault simulator for synchronous sequential circuits," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 15, no. 9, pp. 1048–1058, Sep 1996.

[12] F. Brglez and H. Fujiwara, "A neutral netlist of 10 combinatorial benchmark circuits and a target translator in FORTRAN," in *In Int. Symposium on Circuits and Systems, ISCAS'85*.

Honorio Martin is an associate professor at University Carlos III of Madrid withing the Electronic Technology Department. He received his Ph.D from University Carlos III of Madrid, Spain, in 2015. His research interests include hardware security and trust, lightweight cryptography and approximate computing.

Sophie Dupuis is an associate professor at university of Montpellier within LIRMM, France. She received her Ph.D. from Pierre Marie Curie university, Paris, France, in 2009. Her research interests include hardware trust, test and security, VLSI CAD and VLSI circuit design.

Giorgio Di Natale is CNRS Director of Research, and director of TIMA laboratory in Grenoble (France). His research interests include hardware security and trust, secure circuits design and test, and reliability evaluation. He serves as chair of the TTTC, he is Golden Core member Computer Society and Senior member IEEE.

Luis Entrena is Full professor at University Carlos III of Madrid. He received is Ph.D degree in electronic engineering from the Universidad Politecnica de Madrid, Spain, in 1995. His current research interests include on-line testing, fault tolerance, soft error sensitivity evaluation and mitigation and approximate computing.