Securing Hardware from Malicious Attacks

Mohamed M. A. Abdelgawad [1]

[1]Affiliation not available

October 30, 2023

Abstract

Abstract—Hardware security is considered a major design and manufacturing target area with a broad range of research and development topics such as protection of intellectual property (IP), metering of hardware, detection of hardware Trojans, and a lot of other topics. This paper discusses Trojan realization in integrated circuits (ICs), as well as the possible security measures, also exploring the usage of the 3-D integration in hardware security where additional hardware can be mounted after fabrication to foster secure execution just for those systems which need it.

Hosted file

Securing Hardware from Malicious Attacks

Mohamed Abdelgawad
Information and Communications Engineering
Berliner Hochschule für Technik
Berlin, Germany
mohamed.abdelgawad@bht-berlin.de

Marianne A. Azer
National Telecommunication Institute
Nile University
Cairo, Egypt
mazer@nu.edu.eg

Citation: M. Abdelgawad and M. A. Azer, "Securing Hardware from Malicious Attacks," 2021 16th International Conference on Computer Engineering and Systems (ICCES), 2021, pp. 1-4, doi: 10.1109/ICCES54031.2021.9686147.

URL: https://ieeexplore.ieee.org/document/9686147

Abstract—**Hardware security is considered a major design and manufacturing target area with a broad range of research and development topics such as protection of intellectual property (IP), metering of hardware, detection of hardware Trojans, and a lot of other topics. This paper discusses Trojan realization in integrated circuits (ICs), as well as the possible security measures, also exploring the usage of the 3-D integration in hardware security where additional hardware can be mounted after fabrication to foster secure execution just for those systems which need it.**

Keywords*—*attacks, countermeasures, hardware Trojan, integrated circuit, intrusion detection, security

I. Introduction

The importance of hardware security comes from the need to secure the Integrated Circuits (ICs) due to their usage in many critical domains of our lives. Due to economic reasons, ICs are manufactured by foundries built in countries which have non or low measures for Intellectual Property (IP) protection [1]. At the same time ICs may contain Intellectual Property (IP) rights provided by other third parties. Also, IC suppliers use third-party automation tools and outsource design and test services. Such dependency on third parties gives many chances for an opponent to ruin the task of an IC, especially military purpose ICs, by Trojan logic insertion; which may expose critical systems to high risks. Such risks may result in halting weapon systems, providing back door access to secure systems, and destabilizing civilian infrastructure such as banking systems, electric grid, and communication networks [1][2][3][4][5].

In the seventies, the most important synthesis and design objective for ICs was the area reduction, in the eighties, the objective was execution speed, and in the nineties, the objective was power dissipation. Although the objectives mentioned earlier still exist in a lot of new applications, security, privacy, and Digital Right Management (DRM) have become among the most important objectives [6][7].

The purpose of this paper is to discuss Trojan realization in integrated circuits (ICs), as well as the possible security measures, also exploring the usage of the 3-D integration in hardware security where additional hardware can be mounted after fabrication to foster secure execution just for those systems which need it.

The rest of this paper is organized as follows. Section II presents a background about intrusions, attacks and Hardware Trojans. Section III presents intrusion detection techniques. Section IV presents reverse engineering as a tool in hardware attacks. Section V presents secure design measures against hardware attacks. Section VI presents security through 3-D integration. Finally, Section VII presents the conclusions of the paper.

II. Background

This section presents a background about intrusions, attacks and Hardware Trojans. Section A focuses on the difference between intrusions and attacks, while section B presents the Hardware Trojans in detail.

A. Intrusion sand Attacks

Before discussing hardware Trojans, it is important to differentiate between intrusions and attacks.

1) Intrusions

Intrusion means a change of an IC that happens during the design or manufacturing phase for a bad purpose; to be exploited during an attack which may happen during the normal running of the installed IC afterward. Intrusions may change the design of an IC at different phases, for instance, Register Transfer Logic (RTL), gate-level netlist, or GDSII layout. Intrusions may target the supplemental functional logic, or the infrastructure logic added to the design for circuit testability, reliability, or manufacturability purposes. Focused Ion-Beam (FIB) circuit modifications are intrusions that target an already fabricated IC [2][5][8]. As an example of how an intrusion works, a FIB intrusion works in two phases: In the first phase it adds a Trojan to the IC layout as spare gates not connected to the IC functional logic. Then, in the second phase after fabrication, it connects the Trojan to the IC functional logic using a FIB [5].

2) Attacks

An attack tries to harm the target system, such as stopping the operation of the system or stealing valuable information [9]. Prior intrusions are not always necessary for an attack to happen. For instance, tampering attacks of type non-invasive, such as putting the IC under radiation effect or running the IC out of its normal voltage, temperature, or frequency limits, can happen in the absence of any circuit changes [5].

B. Hardware Trojans

A Hardware Trojan (HT) is a design that pretends itself as the authentic design, through emulation of the real design task, and insertion of supplemental circuit components before or during design manufacturing, to take access or control to the running HW or to ruin its task [6][8].

1) Classification and characteristics

Hardware Trojans can be classified based on three general criteria: physical characteristics (Size, Type, Distribution, Structure), activation characteristics (Internally Activated, Externally Activated), and threat types (Confidentiality, Integrity, Availability) [9]. The following set of characteristics are specific to a HT as mentioned in [9]:

a) Size is small compared to the overall IC area

Hardware Trojan implementations are small enough to be inserted without modifying the IC dimensions and its pin count.

b) Invisibleness and hidden triggering

Hardware Trojans are barely noticeable due to deep insertion into the IC. Furthermore, the possibility of spreading HT parts all over the IC, makes the HT less detectable. In addition, till the HT is activated using a specific situation, it can remain idle during the overall IC running time.

c) Harmful function

Hardware Trojans have harmful objectives to rob *c*lassified information or hold up IC tasks.

Fig. 1 presents a basic example of HT circuit; which can change a logic signal by applying it to an input of XOR gate with the other input is the trigger signal. The circuit will be activated when Trigger = 1, then the signal will be inverted [9]. Table I presents the manipulated scheme of the HT circuit, which shown in Fig. 1 [9].

2) Design Model

The Hardware Trojans insertion can target safety-critical, security, and military systems, for instance, arm control systems, battleground communication systems, data collection and decision-making systems, satellite systems, banking systems, cryptosystems, etc. [9]. An IC design model exploited by HT circuit insertion is presented in Fig. 2 as shown in [9].

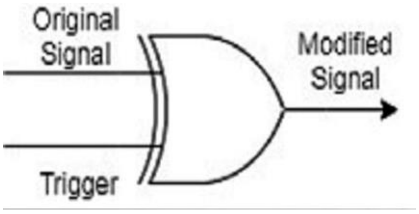

Fig. 1. Example of a hardware Trojan circuit [9]

TABLE I. LOGICAL BEHAVIOR OF HT CIRCUIT [9]

Original Signal	Trigger	Modified Signal
0	0	0
1	0	1
0	1	1
1	1	0

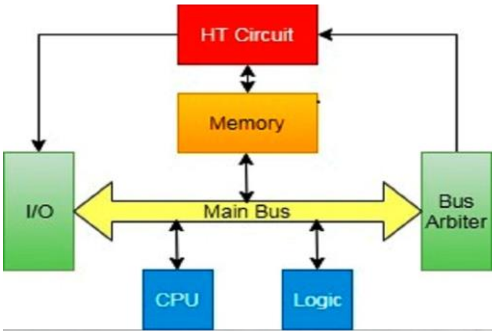

Fig. 2. Insertion of a hardware Trojan circuit [9]

By sending on the Main Bus a dedicated value such as a memory address of the saved targeted data, the Trojan activation can happen [9].

The risks of Trojan circuits at the moment of activation are dangerous. One of the following can happen: Halting the system, transferring targeted data to non-intended destinations through embedded interfaces, collecting memory accessed data for future use, elevating security permissions for a process currently executing in the system. Once triggered by specific input, the HT can change data by error transmission to the output, as seen in Fig. 1, or enable the side channel to transmit classified information, as seen in Fig. 2. Finding the inputs that trigger and uncover all the HT functionality is a difficult verification activity. This is because as these inputs are rare, so the HT detection can be hard especially in complicated digital designs [9].

III. INTRUSION DETECTION

Intrusion detection needs to be done before attacks happen to prevent or at least minimize the harm of the attacks. This can be accomplished either in pre-silicon stages; throughout the design verification, or in post-silicon stages; throughout fabrication test, validation of silicon, and finally test and validation of system [5][10]. This is presented in sections A and B respectively.

A. Pre-Silicon Detection

Detection during pre-silicon would be preferred than during post-silicon. However, Trojans are possibly designed so that the detection during pre-silicon is hopeless in practice. For example, a Trojan injected in the RTL model of an IP core is possibly designed to be turned on after a long time of IC installation in the field. The long time before Trojan activation ensures that the activation will not happen within simulation or emulation activities of pre-silicon verification, or even within the validation of silicon. If the Trojan was never detected using simulation or emulation, it could be detected by analysis of low functional coverage areas within pre-silicon verification [5][11]. From the above, it is obvious that there is no insurance that ICs installed in the field are free of Trojans. This shouldn't lead to ignoring and not using the methods of pre-silicon detection, but only shows that even such methods are needed but not enough [5].

B. *Post-Silicon Detection*

In the majority of suggested post-silicon methods, several physical aspects of the IC (for instance consumed power, structures of layout, and variations of time) can be analyzed compared to a golden-reference model. Such model existence is not feasible if there exists a Trojan in the IC RTL model, which makes the main assumption as the cornerstone of major pre-silicon detection methods invalid. Because an RTL golden-reference model only represents the IC functional logic, so regardless of the existence of such a model, invisible Trojan injection is more possible by injection of infrastructure logic in the IC [5][10].

IV. Reverse Engineering

Reverse engineering is finding out by inspection the components, construction, and task of an actual device, object, or system. This procedure is beneficial to avoid expensive redesign of products in case any part turned out to be extinct or if the part suppliers stopped their business. To achieve this, suitable reverse engineering tools and skills can be used to reproduce the task of the unavailable part [12][13].

IC reverse engineering can be done as follows: First, the silicon chip is removed from its package, then the top metal layers are taken away by etching the chip. From then, by an expert engineer, much of the circuit inside the chip can be visually recognized and its task can be concluded. To uncover circuit deeper layers, extra layers of the chip needed to be etched, but the outcome turns out to be inaccurate increasingly with each etched layer, due to the various rate of removing various materials in the etching procedure. To reverse engineer a complicated IC, a group of expert engineers might be needed to examine a lot of chips [12].

An extra complex and costly method to reverse engineer an IC is by measuring its runtime voltage. The alternating voltage of the running circuit can be denoted and logged by a specific instrument. By analyzing the recorded voltage figures, the circuitry of the IC and even the on-chip RAM data can be exposed [12].

Although reverse engineering is possible to be a decent action, also it is possible to act as a pernicious spying tool used to decode critical electronics in either civilian or military systems [12][13].

V. Security Measures

Different aspects are needed to prohibit hardware attacks in a thorough process. The ultimate significant objective is to carry out secure design measures which can deny or at least resist attacks once they happen. These measures are costly, so the cost of time, money, and effort will be needed to secure an IC. Also, the increased cost of power, performance and area (PPA) needed to be considered, especially for commercial applications. This cost comes from including a small quantity of additional hardware in the secure IC to monitor the chip internally and implement a group of security defences. These defences can jump into place within a very tiny time, once an antagonistic activity is recognized, to determine the attack cause and defeat it with countermeasures [1][14]. Table II summarizes the security measures which are mentioned in [1][14].

VI. Security Through 3-D Integration

The layer stacking procedure of 3D-IC hides most up to complete circuit details, which is considered the important security benefit of 3D-IC. The external face of the finished chip is possibly made totally blank unless for I/O pins, by making the face of the lowest stacked-layer looks upward and the face of the highest stacked-layer looks downward. This way of stack structuring defeats most reverse engineering trials because etching through the substrates uniformly would be highly complex although removing layers is feasible in theory [12].

Separating the security components from the design is one security mechanism of 3D-IC stacking, this is achieved by combining them onto a distinct layer of circuitry to act as a security shield, named a control plane that is stacked on the highest layer of an IC. In a secure IC, the control plane with many die-stacking methods, possibly be attached to the underlying circuit; named the computation plane. Keeping the control plane detached from the computation plane results in an unsecured IC which is possibly sold by the IC manufacturer at a cheaper price. Stacking many planes in 3D stacks with each other already examined by IC manufacturers as a modern marketed technology [15] [16].

For the success of this process, many issues need to be fixed. For instance, circuit-level abilities for observing and limiting activity if required are needed for the control plane's capability to apply security policies. The issue is that, some functions in the computation plane possibly are stopped by such limitation abilities, but in the case of the non-existence of these limitation abilities the computation plane must be entirely functional. Another issue is how distinct silicon technology nodes for the control and computation planes to be combined in the same manufacturing process [15].

VII. ConclusionS AND FUTURE WORK

ICs' complexities and capabilities are increasing, but also their susceptibilities to attacks are increasing. ICs by default contain multi-sourced designs. A hardware Trojan inserted in one of these designs could arise long after the circuit has been deployed in the field. In this paper, we presented a few simple precautions which could go further away toward securing hardware against malicious attacks. In future, this effort can be extended to cover in-depth review for specific aspects of hardware security.

References

[1] D. M. Luria and R. Vemuri, "Logic encryption for resource constrained designs," IEEE Access, vol. 9, pp. 29312-29345, 2021.

[2] 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, Sep. 2020.

[3] Y. Shen, A. Rezaei, and H. Zhou, "SAT-based bit-flipping attack on logic encryptions," in Proc. DATE'18, 2018, paper 8342086, p. 629–632.

[4] R. JayashankaraShridevi, D. M. Ancajas, K. Chakraborty, and S. Roy, "Security measures against a rogue Network-on-Chip," Springer Journal of Hardware and Systems Security, vol. 1, pp. 173–187, Jun. 2017.

[5] M. Abramovici, and P. Bradley, "Integrated circuit security: new threats and solutions," in Proc. CSIIRW'09, 2009, paper 55, p. 1–3.

[6] F. Koushallfar, and M. Potkonjak, "Hardware security: preparing students for the next design frontier," in Proc. MSE'07, 2007, paper 48, p. 67–68.

[7] S. Ravi, A. Raghunathan, P. Kocher, and S. Hattangady, “Security in embedded systems: design challenges,” ACM Transactions on Embedded Computing Systems, vol. 3, pp. 461–491, Aug. 2004.

[8] Y. Shen, Y. Li, A. Rezaei, S. Kong, D. Dlott, and H. Zhou, “BeSAT: behavioral SAT-based attack on cyclic logic encryption,” in Proc. ASPDAC’19, 2019, paper 3287670, p. 657–662.

[9] A. Adamov, and V. Hahanov, “Security risks in hardware: implementation and detection problem,” in Proc. EWDTS’10, 2010, paper 5742118, p. 425–427.

[10] S. Moustakidis, K. Liakos, G. Georgakilas, N. Sketopoulos, S. Seimoglou, P. Karlsson, and F. Plessas, “A novel holistic approach for hardware trojan detection powered by deep learning (HERO),” in Proc. ATTRACT’20, 2020.

[11] S. Rob, “Hacking passports exposing the vulnerabilities of ‘Smart Card’ technology,” The Social Contract, vol. 20, pp. 287-295, 2010.

[12] “3D-ICs and integrated circuit security,” (2008) media webpage on TEZARRON. [Online]. Available : http://tezzaron.com/media/3D-ICs_and_Integrated_Circuit_Security.pdf/

[13] S. Quadir, J. Chen, D. Forti, N. ASADIZANJANI, S. SHAHBAZMOHAMADI, L. WANG, J CHANDY, and M. TEHRANIPOOR, “A survey on chip to system reverse engineering,” ACM Journal on Emerging Technologies in Computing Systems, vol. 13, pp. 1–34, Apr. 2016.

[14] J. Villasenor, “The hacker in your hardware,” Scientific American, vol. 303, pp. 82–87, Aug. 2010.

[15] T. Huffmire, J. Valamehr, T. Sherwood, R. Kastner, T. Levin, T. D. Nguyen, and C. Irvine, “Extended Abstract: trustworthy system security through 3-D integrated hardware,” in Proc. HOST’08, 2008, paper 4559061, p. 91–92.

[16] G. Cox, Z. Yan, A. Bhattacharjee, and V. Ganapathy, “3D-stacked architecture for secure memory acquisition,” Rutgers University, Computer Science Tech. Rep. DCS-TR-724, 2016.

TABLE II. PREVENTIVE SECURITY MEASURES AGAINST HW ATTACKS [1][14]

SECURITY MEASURE	**OBJECTIVE**	**METHOD**
Memory Gatekeeper	Prevention of any trial to access restricted ranges of memory addresses by a deceptive block; the benefit of measure is that snooping, or deterioration of data is prevented	Ensuring that only permitted ranges of memory addresses can be accessed by blocks and recording any trials to access restricted ranges of memory addresses
Secure System Bus	Protection of a system bus from pernicious requisitions by which the circuit could stop completely or extremely slowed execution	Analyzing statistical patterns of actions done on the bus by various working blocks and recording suspected actions
Input/output Monitor	Impedance to hidden espionage--whenever the chip tries to copy data to locations out of the chip	Analyzing the transfer of data in and out the chip, comparing this movement with the anticipated pattern, and recording any deviations
On-chip Block Integrity Tester	Safeguard against a Trojan attack that tries to destroy a block that previously was working correctly	Testing on occasion the blocks to assure they keep functioning as anticipated
Additional Configurable Hardware Logic	Enablement of the circuit to isolate a jeopardized block and reproduce its task	Replacing the isolated functional block by the configured additional logic, however probably at a lower speed
Attack Alarm System	Enablement of other circuits to safeguard themselves precautionary against close attacks	Establishing countermeasures by the circuit exposed to attack and sending an alarm about the attack to different devices which includes the same circuit
Logic Encryption	Protection for integrated circuit designs from being pirated or maliciously modified	Adding logic gates to the design, such logic gates controlled with an additional bus for key input, hence the recovery of circuit behaviour is possible only using the valid true key