Natl. Acad. Sci. Lett. (November–December 2023) 46(6):521–524
https://doi.org/10.1007/s40009-023-01247-6

SHORT COMMUNICATION

Review on Hardware Trojan Detection Techniques

R. Naveenkumar[1,2] · **N. M. Sivamangai**[1] · **A. Napolean**[1] · **S. Sridevi Sathayapriya**[1]

Received: 26 July 2022 / Revised: 19 January 2023 / Accepted: 1 March 2023 / Published online: 20 May 2023

Abstract As a result of globalization, chip design and manufacturing are becoming more susceptible to harmful actions and modifications. However, to develop a reliable and effective system there should be no role of hardware Trojan. In microelectronic systems, hardware security plays a vital role. Hardware security as a discipline originated out of cryptography and involves hardware design, and secure multi-party computations. Hardware Trojan (HT) is a major threat to hardware security because HT can change the circuit's behavior and leak the information, once it is activated. To improve the reliability of the system and the trust of the circuits HT should be detected. This paper deals with various hardware trojan identification like pre-silicon design stage-based detections and post-silicon fabrication stage-based detections.

Keywords Hardware trojan · Hardware security · Reliability · Pre-silicon detection · And Post-silicon detections

✉ R. Naveenkumar
naveentamil256@gmail.com

N. M. Sivamangai
nmsivam@gmail.com

A. Napolean
nepojustin@gmail.com

S. Sridevi Sathayapriya
s.d.s.priya@gmail.com

[1] Department of ECE, Karunya Institute of Technology and Sciences, Coimbatore 641114, Tamilnadu, India

[2] Department of ECE, Karpagam Academy of Higher Education, Coimbatore 641021, India

Introduction

With the recent development of integrated circuits, communication networking, and security system, electronic gadgets are attracted by all users. These electronic gadgets play an important role in human life not only for sharing information apart from that security-wise it has some drawbacks. Most of the electronic gadget has a large amount of internal memory. It can store the user's files like banking details, account numbers, pin details, and passwords, etc. So if this personal detail can easily share with others by inserting of HT in the device [1]. Generally hardware trojan is a malicious function of the circuits. Malware or suspicious which is available in the hardware it is named HT. This kind of HT can change the behavior of the circuits.

Figure 1 depicts the structure of HT represents a process of changing the circuit functionality. HT causes wrong activity (by changes of the 1–0) when it is triggered. Generally, trigger circuits represent the activation mechanism of HT. Payload is the effect of modification like Deny of Service (DOS), Reduce reliability, changing the function, and leakage of information.

Generally HT is classified into pre-silicon-based HT detection (Run-time monitoring (RM), Auxiliary detection (AD), Post-silicon-based HT detection as shown in Fig. 2.

In a pre-silicon-based HT detection, the HT detection only analyzed in the system design level. The monitoring run time activity method is a non-destructive approach; it can monitor the abnormal behavior and function during run time activity. Comparing the response based choose the trusted part to avoid an affected part of the circuits. If it is test time authentication, identify the HT throughout the test duration (Example: Logic testing and side-channel analysis). During the operation, frequently inspect the design, device structure, and objects. This is a simple concept to easily

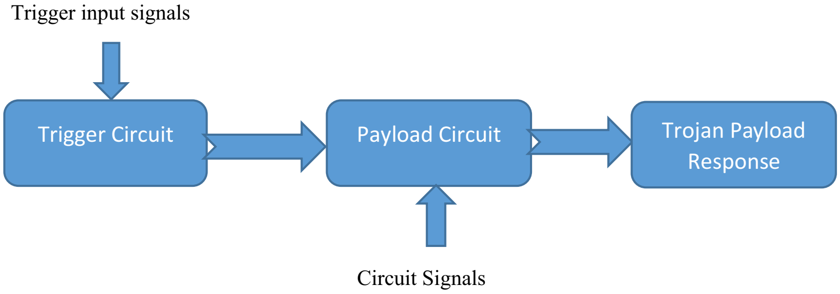

Fig. 1 Structure of hardware Trojan

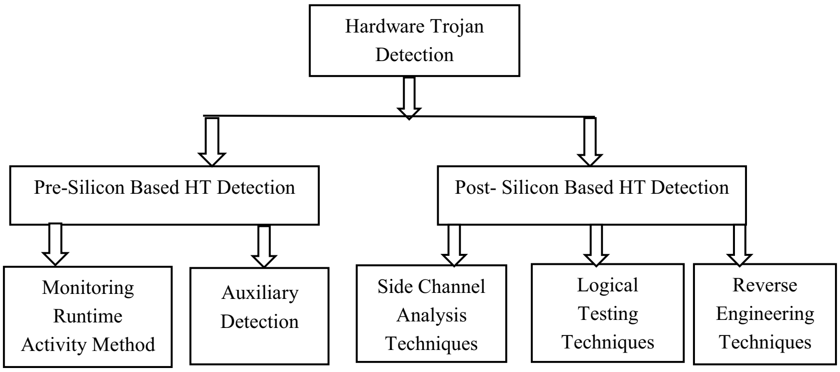
Hardware Trojan Detection
Pre-Silicon Based HT Detection
Post- Silicon Based HT Detection
Monitoring Runtime Activity Method
Auxiliary Detection
Side Channel Analysis Techniques
Logical Testing Techniques
Reverse Engineering Techniques

Fig. 2 Classification hardware Trojan identification

identify the activities of the HT [1]. While using the IC, the entire process-based HT will be identified. And it is not a single-time identification response. The drawback is a little complex to all types of HT activities. Suggested to detect the HT by use of the formal checking approach. It consumes less area and improves the test time overhead by 5–30 times [2]. Introduced designer authentication approach for avoiding unauthorized third party access in the system on chip and network-on-chip [3].

The Auxiliary method improves the accuracy of logical testing and side-channel analysis. And it is comparing with the HT affected and HT not affected circuit [1]. Virtual scanning concept is dealt with a high probability of triggering with a high probability of transition. This approach gives better identification with a decrease in the activation time. Introduced hardware trust and verification concept, it is used to identify the HT in the design area [4]. HT is generally input trigger-based activated and it is not sensitive to the trigger input signals. Here the verification process is done by inspecting the modules to identify the HT. This approach is suggested based on electron microscopy scanning for identifying a single layer in a chip. Authors done the comparison with the standard model circuit, after that, SEM-based images will verify which one has modified like area, placement, routing, or any addition of the circuitry or design in the internal circuits. Here compare the HT by SEM-based images. The advantage of this one is accurately identifying the HT and the drawback is higher cost [5]. For some specific condition only designer needs reference model, example SEM imaging, hardware verification and authentication purpose. So these are the places with help of same golden reference model based only designer could find the variation in the HT free circuit and HT affected circuit.

In a post-silicon-based HT detection, the HT detection only analyzed in the fabrication level, The HT impacted in the chip can change the characteristics of power consumption in side-channel signal analysis (SCA). Trojan partial activation can be quite helpful for power analysis. Physical side-channel metrics including switching current, leakage current, temperature, route latency, time data, electromagnetic emission (EM), and power consumption are used to identify side-channel Trojans by looking for their impacts. SCA is used to compare the standard IC with our experimenting IC in all kinds of aspects of the side-channel analysis parameters mainly like Voltage (V), Temperature (T), and Path delay (Pd). It is vulnerable to process noise. Extremely suitable for large Trojans and Easy to produce the test patterns but Ultra small Trojan identification is difficult and better fault coverage. It is determining whether the experimenting IC is affected by HT (or) not affected HT. SCA will not change the circuit design and hardware overhead, some of encryption design like logical locking utilized for trust of the design [6]. And generally, SCA identification is a common term in VLSI and also it has another way to inspect the design in side-channel signal parameter aspects. It can easily get the result by comparing delay with an experimenting circuit with a standard reference circuit model [7].

Table 1 Various parameter analysis of HT identifications

Pre-silicon identifications

Detection	Methodology	Golden reference model needed	Detection efficiency	Area, power ahead	Cost	Influence of external factors	References
AD	Fast SEM imaging	Yes	Good	Low	High	No	[5]
AD	Timing analysis	No	Good detection probability: 95% False positive:5%	Low Area over head: 1.3–3.94%	Design based	Yes	[12]
AD	Hardware trust verification	Yes	Good	Depends on design	Moderate	No	[4]
AD	Virtual scan trigger	No	Good	Less area and power overhead	Depends on design	No	[13]
RM	Formal modeling of burst mode communication	No	Good	Less area and power overhead	Depends on design	No	[2]
RM	Detection framework	No	Good	Low	Depends on design	No	[14]
RM	Authentication scheme	Yes	Good	Low Area over head: 3.37% Power: 2.61%	Depends on design	No	[3]
RM	Temperature in IC	No	High accuracy	Low overhead	Very low cost	No	[15]

Post-silicon identifications

Detection	Methodology	Easily locate and better Identification	Reference golden model needed	Process variation interference	Overhead	References
SCA	Thermal	✓	✓	NA	NA	[8]
SCA	Temperature, matrix	✓	✓	High	–	[16]
SCA	Path delay	✓	✓	Low	High area overhead	[7]
SCA	Light emission	✓	✓	Low	–	[17]
LT	Scalable logic testing	✓	✓	Low	–	[18]
LT	Probability Signature	✓	✓	Low	–	[10]
RE	Visual inspection at the circuit level	✓	✓	Low	Low area overhead LUT:0.5%	[11]
RE	SVM (Support Vector Machine)	✓	✗	Low	High area overhead	[19]
RE	Path retrace algorithm	✓	✗	Low	–	[20]

A new side-channel signal analysis identification is introduced depending on the path delay. This is the simple and shortest way to get the results by programming or coding. In the thermal image method, the latch structure is merged with the design circuit. Also, the latch structure can easily display all possible causes of inserting HTs. And this approach can eliminate the influences of noises, and it also compensates the poor performance of the side-channel signal analysis. Suggested the position of HT identifying by the thermal images. It is generally used to identify the HT when the gate count is less than 20. Here the activity factor is determined by the thermal changes of the HT in the redundant thermal map. If the gate count is 10–100 gates, it is more accurate and electromagnetic-based side-channel identification [8].

Logical testing (LT) is used to create many number of test vector data to meet certain rare activation conditions to stimulate the hardware Trojan. It is robust under the process noise, extremely suitable for ultra-small Trojans but difficult to produce the test patterns. Large amount Trojan identification is difficult, Easy to differentiate and Fault coverage is lower. This technique is applied when comparing the experimental results with the standard original model results of the simulation measurements. In case of the results from the IC are affected during the experimental procedure, then easily HT will be identified [9]. It is mainly focused on the test vector generation for activating the Trojan circuits and observing that circuit malicious issues on the payload at the primary outputs. It is suitable for the structural and functional of the test vectors. Presented a probability signature type-based HT identification [10].

The goal of reverse engineering (RE) is to directly scan the internal physical structure of the IC. And the scanning electron microscope and delayering are utilized with the RE to retrieve the layer-by-layer pictures. Then utilizing the template matching method to determine the transistor, gates, and routing components. It is based on the golden layout model. Here comparing the experimental image with the standard original reference image. This is a kind of visual inspection done by microscope. Generally, reverse engineering-based identification or detection rates are much higher and HT is directly observed based on the physical structure. To inspect the HT, auxiliary type analysis can be used. Suggested an HT identification concept is based on direct physical inspection on the circuit level [11]. Initially, it compares the image of the experimenting circuit with a normal standard image circuit. And destructive reverse engineering-based images extracted. Table 1 shows the various parameters of HT identifications.

From the table, The analysis represents the Pre-silicon, run time monitoring is better for identifying HT, based on good detection, less area, power head, and influence of external factors. A post-silicon detection method investigation shows logical testing, based on probability signature analysis is efficient because it is not affected by process variation interference and overhead, Moreover visual inspection in circuit level the RE is better.

Declarations

Conflict of interest Nil.

References

1. Naveenkumar R, Sivamangai N M, Napolean A, Janani V (2021) A survey on recent detection methods of the hardware Trojans. In: 3rd International Conference on Signal Processing and Communication (ICPSC), pp 139–143. https://doi.org/10.1109/ICSPC51351.2021.9451682
2. Khalid F, Hasan SR, Hasan O, Awwad FR (2018) Runtime hardware Trojan monitors through modeling burst mode communication using formal verification. Integr 61:62–76. https://doi.org/10.1016/j.vlsi.2017.11.003
3. Hussain M, Guo H, Parameswaran S (2018) A Customized authentication design for traffic hijacking detection on hardware-trojan infected NoCs 6:135–152. https://doi.org/10.4236/jcc.2018.61015
4. Zhang J, Yuan F, Wei L, Liu Y, Xu Q (2015) VeriTrust: verification for hardware trust. IEEE Trans Comput Aided Des Integr Circuits Syst 34:1148–1161. https://doi.org/10.1109/TCAD.2015.2422836
5. Courbon F, Loubet-Moundi P, Fournier J J, Tria A (2015) A high efficiency Hardware Trojan detection technique based on fast SEM imaging. In: Design, automation and test in Europe Conference & Exhibition (DATE), pp 788–793. https://doi.org/10.7873/DATE.2015.1104
6. Rathor VS, Garg B, Sharma GK (2018) A novel low complexity logic encryption technique for design-for-trust. IEEE Trans Emerg Top Comput 8:688–699. https://doi.org/10.1109/TETC.2018.2795706
7. Zarrinchian G, Zamani MS (2017) Latch-based structure: a high resolution and self-reference technique for hardware trojan detection. IEEE Trans Comput 66:100–113. https://doi.org/10.1109/TC.2016.2576444
8. Tang Y, Fang L, Li S (2019) Activity factor based hardware trojan detection and localization. J Electron Test 35:293–302. https://doi.org/10.1007/S10836-019-05803-1
9. Rathor VS, Garg B, Sharma GK (2020) New lightweight Anti-SAT block design and obfuscation technique to thwart removal attack. Integr 75:178–188. https://doi.org/10.1016/j.vlsi.2020.05.001
10. Zheng ZX, Li YF, Yu L, Tian Y, Liu ZL (2014) Hardware Trojan detection technology based on probabilistic signature. Comput Eng 40:18–22
11. Bhasin S, Danger J, Guilley S, Ngo X T, Sauvage L (2013) Hardware Trojan horses in cryptographic IP cores. In: Workshop on Fault Diagnosis and Tolerance in Cryptography, pp 15–29. https://doi.org/10.1109/FDTC.2013.15
12. Xue H, Ren S (2018) Hardware Trojan detection by timing measurement: theory and implementation. Microelectron J 77:16–25. https://doi.org/10.1016/j.mejo.2018.05.009
13. Salmani H, Tehranipoor M M, Plusquellic J F (2012) A novel technique for improving hardware trojan detection and reducing Trojan activation time. IEEE Trans Very Large Scale Integration (VLSI) Syst 20:112–125. https://doi.org/10.1109/TVLSI.2010.2093547
14. Hou Y, He H, Shamsi K, Jin Y, Wu D, Wu H (2019) On-chip analog trojan detection framework for microprocessor trustworthiness. IEEE Trans Comput Aided Des Integr Circuits Syst 38:1820–1830. https://doi.org/10.1109/TCAD.2018.2864246
15. Bao C, Forte D, Srivastava A (2015) Temperature tracking: toward robust run-time detection of hardware Trojans. IEEE Trans Comput Aided Des Integr Circuits Syst 34:1577–1585. https://doi.org/10.1109/TCAD.2015.2424929
16. Zhong J, Wang J (2018) Thermal images based Hardware Trojan detection through differential temperature matrix. Opt Int J Light Electron Opt 158:855–860. https://doi.org/10.1016/J.IJLEO.2017.12.145
17. Song P, Stellari F, Pfeiffer D, Culp J, Weger A J, Bonnoit A, Wisnieff B, Taubenblatt M A (2011) MARVEL—Malicious alteration recognition and verification by emission of light. In: IEEE International Symposium on Hardware-Oriented Security and Trust, pp 117–121. https://doi.org/10.1109/HST.2011.5955007
18. Bazzazi A, Shalmani MT, Hemmatyar AM (2017) Hardware Trojan detection based on logical testing. J Electron Test 33:381–395. https://doi.org/10.1007/s10836-017-5670-0
19. Bao C, Forte D, Srivastava A (2014) On application of one-class SVM to reverse engineering-based hardware Trojan detection. In: International symposium on quality electronic design, pp 47–54. https://doi.org/10.1109/ISQED.2014.6783305
20. Rajendran SR, Regeena ML (2022) A novel algorithm for hardware trojan detection through reverse engineering. IEEE Trans Comput Aided Des Integr Circuits Syst 41:1154–1166. https://doi.org/10.1109/TCAD.2021.3073855

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.