Performance analysis of Hardware Trojan detection methods

Ehsan Sharifi, Kamal Mohammadiasl, Mehrdad Havasi and Amir Yazdani

***Abstract*— Due to the increasing use of information and communication technologies in most aspects of life, security of the information has drawn the attention of governments and industry as well as the researchers. In this regard, structural attacks on the functions of a chip are called hardware Trojans, and are capable of rendering ineffective the security protecting our systems and data. This method represents a big challenge for cyber-security as it is nearly impossible to detect with any currently practical detection scheme. Due to Various methods of this type of attack, many different methods are presented by the researchers to detect them. Each of these methods has been proposed different techniques to detect the Hardware Trojan horse, and are varied in terms of performance and conditions of use. In this paper, we survey the published methods and evaluate the strengths and weaknesses of each of them and analyze the efficiency of the proposed method to introduce efficient methods for Hardware Trojan horse detecting.**

***Keywords*—Hardware Trojan, Information security, Backdoor, Detection method.**

I. Introduction

A Trojan horse is a nonself-replicating type of malware containing malicious code that cannot spread itself like a worm, but disguises itself as a useful program which will be run by a user and then can bring its malicious code into position. The Trojan term is derived from the story of the big handmade horse used to trick defenders of Troy into taking concealed warriors into their castle [1].

Although in The early introduction of the use of Trojans, software was the target of these type of attacks, but nowadays, using this malware in hardware are far more dangerous than Software Trojans. Hardware Trojans are created through the malicious and deliberate alteration of hardware which produce effects unintended by initial design. They reside at the lowest level of information processing - on the integrated circuit (IC) board.

Hardware Trojans are able to leak critical information, they can cause incorrect functioning of a component. Hardware Trojans are an increasing threat to every processing environment, particularly for commercial applications, as well as to critical infrastructure like military Industries. The possibility for hardware Trojans to be inserted into hardware has been a growing concern. Integrated circuits can be infected with a Hardware Trojan either during manufacture or post-manufacture tampering. With the Outsourcing services and globalization of electronic component manufacture It is very difficult or impossible to ensure hardware, safety and the risk of hardware Trojans is increased rather than when the all phases of production of the product is done in same manufacture or at least in the same country [2].

Hardware Trojan horses can affect circuits during normal and routine activities or in the idle time and cause failure in the security mechanisms of the system. These attacks can acquire critical information of the system during executing, storing and transferring of information and Send it to the specified destination. Also Hardware Trojan can cause hardware damage and adversely effect on the system's normal operation [3].

On the other hand, backdoor Malware often Besides the Hardware Trojan will be used to harm the system. A backdoor is a means of access to a computer program that bypasses security mechanisms. A programmer may sometimes install a back door so that the program can be accessed for troubleshooting or other purposes. However, attackers often use back doors that they detect or install themselves, as part of an exploit.

Backdoor Trojan differs from a Trojan in that it also opens a backdoor to the system. They're also sometimes called Remote Access Trojans (RAT). These are the most widespread and also the most dangerous type of Trojan. They are so harmful because have the potential to allow remote administration of the system to assess to the all options of the system [4].

II. Examples of the hardware Trojans using

For the first time, Hardware Trojan was used during the Cold War between USA and USSR. At the time, the USSR and USA used the Hardware Trojan to intercept the communication signals of each other [5].

Hardware Trojan has been the subject academic research a few years ago when the US Department of Defense publicly expressed concerns over the military reliance on

Manuscript sent March 30, 2015. Ehsan Sharifi is with the Department of computer and IT engineering, Payam Noor University (PNU) of Urmia, Iran (phone: 0098-9141490599; e-mail: Sharifi.eh89@gmail.com).

Kamal Mohammadiasl is with the Department of computer and IT engineering, Payam Noor University (PNU) of Urmia, Iran (e-mail: Mohammadiasl@pnu.ac.ir).

Mehrdad Havasi is with the Department of computer Engineering, Yazd University, Iran (e-mail: Mehrdadhavasi@gmail.com).

Amir Yazdani is with Department of computer engineering, Islamic Azad University (IAU) of Shahrerey, Iran (e-mail: Amiryazdani@gmail.com).

integrated circuits manufactured abroad. A recently reported Trojan attack involves US Navy, who discovered a hardware "backdoor" in a microchip used in Different industries. For example the chips could have been hacked, able to shut off a missile in the event of war or just lie around waiting to malfunction [6]

In another case Chinese Information Technology firms have long attracted suspicion from international governments, with telecommunications firms recently coming under suspicion in both the US and UK. Also other Chinese firms have grown to become one of the top PC makers, but its popularity with consumers has not translated over to classified government networks [7]. In other hand Edward Snowden's revelations about the NSA surveillance activities evidenced the effort spent by US intelligence with major chipmakers for the introduction of backdoors into hardware sold to other countries [8].

In the one of the last examples of using a Hardware Trojan by Modifying the conductive behaviors of electrical components, adding a dopant elements team of security researchers from the U.S. and Europe has released a paper that shows they are being able to insert their stealthy Hardware Trojan on Intel's random number generator design used in Ivy Bridge series processors [9].

III. HARDWARE TROJAN DETECTION METHODS

Attack detection is the first and perhaps most important step in any security system. So the attack detection is the most important action to counter the Hardware Trojan. It is not possible to completely prevent the insertion of a Hardware Trojan into the system during the design phase. Where preventative measures are used to protect against Hardware Trojans being inserted into an IC, detection techniques are used to discover the presence of a Hardware Trojan.

Hardware Trojan detection methods can be divided into some categories that is shown in Figure 1.

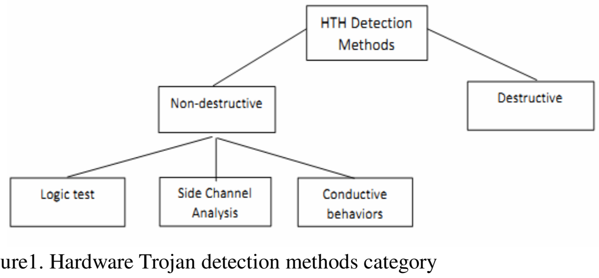

Figure1. Hardware Trojan detection methods category

A. Destructive methods

The Destructive methods for Hardware Trojan detection completely destroy the IC that they examine, lessening the usefulness of such techniques. In this method that is the first and easiest method to detect the Hardware Trojan the first protective layer of the circuit are going to be opened and then all of its components separated by reverse-engineering techniques and are checked by specific physical devices or chemical materials. But it should be considered that reverse-engineering a complex modern IC is a time consuming and expensive process. In Destructive methods, scanning optical microscopy (SOM) and light induced voltage alteration (LIVA) techniques are used for reverse engineering [10].

Destructive methods are more Costly and time consuming. Because Hardware Trojan can be inserted into the circuit by remove or modify a few logic gates. the new circuits including large-scale integration (LSI) and Very-large-scale integration (VLSI) circuits may be contain billions of logic gate and if destructive methods are used to detect hardware Trojans all of these gates should be checked [11].

On the other hand, reverse engineering can be used to provide reliable and safe integrated circuit (Golden IC) that are used in other Hardware Trojan detection methods to compare with examining circuit [12].

Agrawal and et al. use destructive methods reverse engineering to find known good ICs. Before being reverse - engineered, a random sample of ICs from a batch are “finger printed” using such parameters like path delay, power and temperature which are known as Side-channel parameters. Once a consistent set of parameters is obtained, all of the sampled chips are then reverse - engineered to ensure that they are safe and not infected by Hardware Trojan. The finger print can then be used in a non -destructive test on the rest of the chips in the batch [13].

Destructive methods have many Problems beside its benefits. A Hardware Trojan may be infecting the IC by the insertion, deletion or modification of as few as two logic gates whereas modern ICs may consist of billions of gates. Finding this “needle in a haystack” requires complete reverse – engineering at the gate level of the IC [14]. In addition, there is no guarantee that IC that have a Hardware Trojan will generate a different fingerprint.

B. Non-destructive methods

Difficulties and high costs of destructive methods caused the introduction of nondestructive methods. Non - destructive methods for Hardware Trojan detection do not destroy the IC being tested, and are classified as being either invasive, or non - invasive. Non - invasive techniques leave the design unaltered, whereas the invasive techniques modify the design in order to embed features to assist with Trojan detection.

These methods can be divided into several categories that in the following are reviewed.

1) Logic test methods

Logic testing includes equivalence checking at the pre-silicon design phase and generation of specific test patterns through Automatic Test Pattern Generation (ATPG) to excite critical paths during chip testing. These methods are based on the analysis of the IC’s logic structures and divided into functional behavior analysis and Find hidden features methods. In functional behavior analysis method, researchers insert some test vector into the inputs of electronic circuit and analyze the outputs. If the output is incompatible with the input, an anomaly is recognized. In fact, this method generally is used for the detection of functional errors and beside it can detect parametric Hardware Trojan (adding hardware Trojans by modify in the structure of the circuit) and cannot detect functional hardware Trojans (adding hardware Trojans by Add / subtract some elements in the circuit) [15].

The most important problem with logic test’s functional behavior analysis methods is large scale of the test environment in ICs. It even makes the entire test almost is impossible in large ICs. To overcome this limitation, some methods have been presented. Jha proposed a method Based on randomization. In this method, different patterns implement in the input of circuit and then a probabilistic fingerprint has been formed for circuit by the outputs of the circuit. Then the same pattern implemented to examined circuit and compare the output result with the probabilistic finger print. If there are differences, it is assumed that circuit infected by a Hardware Trojan. The results given in this study relate to their "random" modification of ISCAS Benchmark circuits (to "infect" the circuit) and Jha claim that their technique was able to detect 10 out of 12 modifications [16].

In this context, in other study Chakraborty and et al. propose a new method to detect the Hardware Trojan. They propose a methodology for the statistical test generation and coverage de-termination of hardware Trojans. The main objective of the proposed methodology is to derive a set of test patterns that is compact (minimizing test time and cost), whereas maximizing the Trojan detection coverage. basic concept in their method to maximize efficiency in hardware Trojans detection is detect low probability conditions in the design at the internal nodes and then derive an optimal set of vectors than can trigger each of these nodes individually to their rare logic values multiple times. By increasing the toggling of nodes that are random-pattern resistant, it improves the probability of activating an unknown Trojan compared to purely random patterns. It does not require a trusted design environment - is the test generation can be performed on a tapered design [17].

In other similar method Wolf and et al. focused on region of circuit that are rarely activated to detect hardware Trojans. They produce the vectors for trigger the region of circuit that are rarely active and try to check circuit behaviors [18].

Find hidden features methods of logic test focused on identifying characteristics of the IC structure that is not very well known. One of the related studies is done by Skorobogatov and Woods. Most important benefits of this research are performed on the actual hardware instead of the simulation environment. They focus further on the JTAG interface of the FPGA. In this study some hidden commands detected in JTAG by power analyzing. They also found that one of the hidden command requests a 128-bit block of data that by using this 128-bit as the key, some of the chip features that previously were unavailable be activated and programmable [19].

2) *Side Channel Analysis*

Side Channel Analysis based methods examine the anomalous behavior (resulting from HTH) in the circuit's parameters. These parameters can include power, delay, electromagnetic wave propagation and dynamic current values. In this method, parameters of the channel were calculated in Golden IC and compared these values with the values of the examined circuit. The insertion of Trojan cause variations in these parameters which can be utilized to detect the Hardware Trojan.

Side channel based methods divided into some categories by the parameters that are used in this method.

Power based side channel methods use the power parameter of the circuit for Hardware Trojan detection.

On the one of related studies Alkabani and Koushanfar proposed a technique for gate-level timing and power characterization via nondestructive measurements. Each measurement form one equation. After a linear number of measurements are taken, a system of equations for mapping the measured characteristics to the gate level is formed [20].

To get result in the Hardware Trojan detection by power analyze method there are need to a process for analyzing the feedbacks that received from the circuit. Some of the related studies is noted in the following.

Baktir and et al. insert Hardware Trojan into 8 of the 16 circuit in the simulation environment. In their first attempt by comparing the results of the analysis of circuits that containing Trojan by using the usual and customary methods there was no remarkable results. But by using methods such spectrogram and neural network they could detect the Hardware Trojan in the infected circuit [21].

On the other hand, it should be noted that the problem with Application Specific Integrated Circuit (AS IC) systems supply cause that Researchers use simulator environment instead of the actual hardware, whereas using actual hardware is recommended for achieving reliable results. For this reason and to solve this problem, researchers often use Field-programmable gate array (FPGA) which is similar to ASIC For their experiments in actual environment. For example, Wang and LUO proposed Very fast method to detect and implement hardware Trojans on the circuits by using FPGA [22].

In the path delay based Hardware Trojan detection methods according to other side channel analyze methods and by replacing the delay factor instead of other parameters trying to detect Hardware Trojan.

In this regard Jin and Markis try to detect Hardware Trojan by calculating the delay between the gates on the circuit. In the presented method probabilistic fingerprint produced based on the calculated delay between the circuit's gates and then this fingerprint compare with the two results of other circuits to detect hardware Trojans [23].

They claim to be able to detect 100% of explicit Hardware Trojans and 36% of implicit Hardware Trojans. Their experiments were conducted in a simulator, and their Trojans were simple modifications designed specifically to affect power draw and path delay. Similarly, both path delay and leakage current are used as the side – channel for analysis by Potkonjak and et al. [24].

Wang and et al. use current charge integration from multiple current measurement points on an IC, and then localized current analysis to detect Trojan circuitry [25]. The current analysis is once again compared with a golden reference and the authors claim to be able to detect Hardware Trojan.

Wei and et al. present a method that by solving the problem of path delay based methods that related to several parallels paths between the input and output of circuit try to detect hardware Trojans. In this method problem solved by adding multiple testing point (D flip flop) in these parallel paths [26].

Multiple parameters based methods are one of the other approaches in the side channel based Hardware Trojan detection method. In this regard Narasimhan and et al. use the simulator and FPGA to present a new Method to detect hardware Trojans by using current flow (I_{DDT}) and the maximum operating frequency (F_{max}) parameters together. They produce a Diagram by I_{DDT} and F_{max} values and circuits with the Dissimilar diagram assumes as Infected circuit and by this technique they have been able to achieve significant results [27].

Parameter affecting from the process variation is one of the most important problems in the methods based on the side channel. Any Change in these parameters may cause faults in the Hardware Trojan diction process [28].

To solve this problem Rad and et al. propose transient power signal analyze method based on the IC region that were able to have good results [29].

In another study Reece proposed a method that can detect Hardware Trojan without using the Golden IC that are used in side channel based methods. In this study, the process development kit that used in the design of electronic circuits are used to extract the fingerprint from the parameter that is not affected from the process variation [30].

The efficiency of side-channel-based techniques can be improved by adopting design-for-hardware-trust (DFHT) techniques, which, for example, add circuitry to support the measurement and analysis processes of the method. On-chip voltage and temperature sensors can be installed to increase the level of sensitivity of side-channel based methods by providing local observability at various positions across the 2-D layout of the chip. The DFHT strategy must also incorporate a validation strategy for the on-chip support circuits because of the potential of the adversary to sabotage the sensors [31].

3) Detect by added structure in design phase

In this method before the end of the construction phase an extra structure added to circuit to detect the Hardware Trojan. In most cases, this extra element is a small circuit or is part of the circuit also known as Design for Hardware. On the other hand it should be noted that this method can be used in situations that can modify the circuit in production phase. In fact, can say this method can be used in ASIC circuits to detect Hardware Trojan. Also, due to difficulties in ASIC production, this method can be used in the FPGA by Minor change in its structure.

In this context, Chakraborty and et al. used logic test for present structure to detect Hardware Trojan in circuits. They added a logic Test and some I / O port to circuit So that the chip include normal and transparent mode. In the transparent mode of Chip, circuit produce fingerprint values and send them to output. Test mode begin with implementing pseudo fingerprint to circuit. With Assuming that the hardware Trojans are often placed in areas that are rarely active, Hence the control circuits inserted into these areas [32].

If there are discrepancies in the values that evaluated by the control circuit with the expected value (fingerprint) it is assumed that the circuit infected by Hardware Trojan. The main disadvantage of this method is circuit confusion and Complexity by adding some additional structure.

Salmani and et al. propose a procedure to insert dummy flip –flops Into logic to increase Hardware Trojan activity, making for easier detection using side – channel techniques [33]. Abramovici and Bradley proposed more efficient and also complex method than previous methods to detect hardware Trojans. They have added a control logic to circuit which by logic control structures can detect Hardware Trojan during normal operation of the circuit. Capability of programming the circuit after the design phase of it for implementing these Measures is the most important advantage of this method [34].

In the other study Reece put the ring oscillator in certain parts of the FPGA and propose a new method to detect hardware Trojans [35]. Zhang and Tehranipoor proposed more efficient method by using the same technique. They put a ring oscillator network in the circuit and try to detect Hardware Trojan by value changes in oscillator [36]. Ferraiuolo and et al. performed this method on ASIC circuits to detect Hardware Trojan [37].

IV. COMPARISON OF REQUIREMENTS AND PERFORMANCE OF HARDWARE TROJAN DETECTION METHODS.

In table 1, we generally classify these methods to examine the efficiency and effectiveness of these methods. As you can see, we use need for infrastructure, cost, implementation time, the likelihood of success and the ability to implement parameters to compare methods.

TABLE 1. HARDWARE TROJAN DETECTION METHODS REQUIREMENTS AND PERFORMANCE

	Time need	Success chance	Infrastructure need	Implement ability	Repeatability	Coverage scope	Performance
Reverse engineering	**Very long**	**High**	**High**	**Low**	**Low**	**Low**	**Low**
Side channel analyses	**Middle**	**Middle**	**Middle**	**Middle**	**Middle**	**High**	**High**
Logic behavior	**Middle**	**Low**	**Middle**	**High**	**Middle**	**High**	**Middle**
structure Manipulation	**Long**	**High**	**High**	**Low**	**Low**	**Low**	**Middle**

Despite the high success probability of destructive based methods there are several flaws in these methods. The high cost and time need and need to complex infrastructure are major disadvantages of this method and therefore the ability to implement these methods is very low.

In addition, in each time repeating of these methods all steps of the procedure should be done and require the same time and cost at the each time. On the other hand, reverse engineering operations can be well implemented only on ASIC circuit. For this reason and due to these problems in terms of efficiency this method cannot be recommended to use. In nondestructive method can say that in adding a control circuit technique of this method, need to same cost, infrastructure and time of reverse engineering method. In this method the redesign of the circuit and insertion of the additional diagnostic circuit in the main circuit are the major disadvantages of this method. Also this method only can be used in the ASIC circuits. But on the other hand due to the low charge of this method rather than destructive methods as well as the high probability of success in the ASIC structure, this method is efficient for Hardware Trojan detection in this type of structure.

Logic test method In terms of infrastructure, financial cost and time required, is a suitable method to detect hardware Trojans. But the chances of success of this method is low. But the major advantage of this method is that this method can be used in places where none of the other methods cannot be implemented. For example, in cases that there isn’t any information about circuit or the circuit recently has been proposed can use this method. For this reason, this method is considered to be very good in terms of efficiency.

Side channel method has numerous advantage in cost and required infrastructure parameters and this method can be used in different structures. On the other hand, this method can be a good help for the other logic methods. Also due to the suitable chance of success, this method is the most appropriate and reliable Hardware Trojan detection method that nowadays are used in many security systems to protect system against this type of attack.

V. Conclusion

Due to the increasing importance of information security and counter security threats, in Hardware Trojan horse detection field different people have present different method to deal with these attacks, each of which provide different performance and effectiveness against this type of attack. In this paper we studied important methods to detect hardware Trojan and examine the advantages and disadvantages of each of them. We also study the needs and requirements of these methods and finally introduced the most effective method to detect the Hardware Trojans.

References

[1] C. P. Pfleeger and S. L. Pfleeger, Security in computing: Prentice Hall Professional Technical Reference, 2002.

[2] J. Li and J. Lach, "At-speed delay characterization for IC authentication and Trojan horse detection," in Hardware-Oriented Security and Trust, 2008. HOST 2008. IEEE International Workshop on, 2008, pp. 8-14.

[3] S. Wei and M. Potkonjak, "The undetectable and unprovable hardware trojan horse," in Proceedings of the 50th Annual Design Automation Conference, 2013, p. 144.

[4] P. Ferguson, "Observations on emerging threats," in Proceedings of the 5th USENIX conference on Large-Scale Exploits and Emergent Threats. USENIX Association, 2012, pp. 4-4.

[5] T. E. Levin, T. P. Sherwood, T. D. Huffmire, C. E. Irvine, R. C. Kastner, T. D. Nguyen, et al., "Superpositional Control of Integrated Circuit Processing," ed: Google Patents, 2011.

[6] S. Bhunia, M. Abramovici, D. Agrawal, P. Bradley, M. S. Hsiao, J. Plusquellic, et al., "Protection Against Hardware Trojan Attacks: Towards a Comprehensive Solution," IEEE Design & Test, vol. 30, pp. 6-17, 2013.

[7] M. Chung and B. Mascitelli, "Huawei’s Battle: Cold War or Commercial War?," Asian Business and Management Practices: Trends and Global Considerations: Trends and Global Considerations, p. 107, 2014.

[8] G. Greenwald, E. MacAskill, and L. Poitras, "Edward Snowden: the whistleblower behind the NSA surveillance revelations," The Guardian, vol. 9, p. 2013, 2013.

[9] G. T. Becker, F. Regazzoni, C. Paar, and W. P. Burleson, "Stealthy dopant-level hardware trojans," in Cryptographic Hardware and Embedded Systems-CHES 2013, ed: Springer, 2013, pp. 197-214.

[10] S. Wei and M. Potkonjak, "Scalable hardware Trojan diagnosis," Very Large Scale Integration (VLSI) Systems, IEEE Transactions on, vol. 20, pp. 1049-1057, 2012.

[11] S. Narasimhan and S. Bhunia, "Hardware trojan detection," in Introduction to Hardware Security and Trust, ed: Springer, 2012, pp. 339-364.

[12] A. Davoodi, M. Li, and M. Tehranipoor, "A Sensor-Assisted Self-Authentication Framework for Hardware Trojan Detection," Design & Test, IEEE, vol. 30, pp. 74-82, 2013.

[13] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, and B. Sunar, "Trojan detection using IC fingerprinting," in Security and Privacy, 2007. SP'07. IEEE Symposium on, 2007, pp. 296-310.

[14] C. Sturton, M. Hicks, D. Wagner, and S. T. King, "Defeating UCI: Building stealthy and malicious hardware," in Security and Privacy (SP), 2011 IEEE Symposium on, 2011, pp. 64-77.

[15] Y. Jin, N. Kupp, and Y. Makris, "DFTT: Design for Trojan test," in Electronics, Circuits, and Systems (ICECS), 2010 17th IEEE International Conference on, 2010, pp. 1168-1171.

[16] S. Jha, "Randomization based probabilistic approach to detect trojan circuits," in High Assurance Systems Engineering Symposium, 2008. HASE 2008. 11th IEEE, 2008, pp. 117-124.

[17] R. S. Chakraborty, F. Wolff, S. Paul, C. Papachristou, and S. Bhunia, "MERO: A statistical approach for hardware Trojan detection," in Cryptographic Hardware and Embedded Systems-CHES 2009, ed: Springer, 2009, pp. 396-410.

[18] F. Wolff, C. Papachristou, S. Bhunia, and R. S. Chakraborty, "Towards Trojan-free trusted ICs: Problem analysis and detection scheme," in Proceedings of the conference on Design, automation and test in Europe, 2008, pp. 1362-1365.

[19] S. Skorobogatov and C. Woods, Breakthrough silicon scanning discovers backdoor in military chip: Springer, 2012.

[20] Y. Alkabani and F. Koushanfar, "Consistency-based characterization for IC Trojan detection," in Proceedings of the 2009 International Conference on Computer-Aided Design, 2009, pp. 123-127.

[21] S. Baktir, T. Gucluoglu, A. Ozmen, H. F. Alsan, and M. C. Macit, "Detection of Trojans in integrated circuits," in Innovations in Intelligent Systems and Applications (INISTA), 2012 International Symposium on, 2012, pp. 1-5.

[22] L.-W. Wang and H.-W. Luo, "A power analysis based approach to detect Trojan circuits," in Quality, Reliability, Risk, Maintenance, and Safety Engineering (ICQR2MSE), 2011 International Conference on, 2011, pp. 380-384.

[23] Y. Jin and Y. Makris, "Hardware Trojan detection using path delay fingerprint," in Hardware-Oriented Security and Trust, 2008. HOST 2008. IEEE International Workshop on, 2008, pp. 51-57.

[24] M. Potkonjak, A. Nahapetian, M. Nelson, and T. Massey, "Hardware Trojan horse detection using gate-level characterization," in Design Automation Conference, 2009. DAC'09. 46th ACM/IEEE, 2009, pp. 688-693.

[25] X. Wang, M. Tehranipoor, and J. Plusquellic, "Detecting malicious inclusions in secure hardware: Challenges and solutions," in Hardware-Oriented Security and Trust, 2008. HOST 2008. IEEE International Workshop on, 2008, pp. 15-19.

[26] S. Wei, S. Meguerdichian, and M. Potkonjak, "Malicious circuitry detection using thermal conditioning," Information Forensics and Security, IEEE Transactions on, vol. 6, pp. 1136-1145, 2011.

[27] S. Narasimhan, D. Du, R. S. Chakraborty, S. Paul, F. Wolff, C. Papachristou, et al., "Multiple-parameter side-channel analysis: A non-invasive hardware Trojan detection approach," in Hardware-Oriented Security and Trust (HOST), 2010 IEEE International Symposium on, 2010, pp. 13-18.

[28] M. E. Wieder, D. C. Hone, M. J. Cook, M. M. Handsley, J. Gavrilovic, and D. A. Russell, "Intracellular photodynamic therapy with photosensitizer-nanoparticle conjugates: cancer therapy using a ‘Trojan horse’," Photochemical & Photobiological Sciences, vol. 5, pp. 727-734, 2006.

[29] R. Rad, J. Plusquellic, and M. Tehranipoor, "Sensitivity analysis to hardware Trojans using power supply transient signals," in Hardware-Oriented Security and Trust, 2008. HOST 2008. IEEE International Workshop on, 2008, pp. 3-7.

[30] T. Reece and W. H. Robinson, "Hardware Trojans: The defense and attack of integrated circuits," in Computer Design (ICCD), 2011 IEEE 29th International Conference on, 2011, pp. 293-296.

[31] M. Tehranipoor and C. Wang, Introduction to hardware security and trust: Springer Science & Business Media, 2011.

[32] R. S. Chakraborty, S. Narasimhan, and S. Bhunia, "Hardware Trojan: Threats and emerging solutions," in High Level Design Validation

and Test Workshop, 2009. HLDVT 2009. IEEE International, 2009, pp. 166-171.

[33] H. Salmani, M. Tehranipoor, and J. Plusquellic, "New design strategy for improving hardware Trojan detection and reducing Trojan activation time," in Hardware-Oriented Security and Trust, 2009. HOST'09. IEEE International Workshop on, 2009, pp. 66-73.

[34] M. Abramovici and P. Bradley, "Integrated circuit security: new threats and solutions," in Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies, 2009, p. 55.

[35] T. Reece, "Detection of Malicious Hardware in ASICs and FPGAs," 2009.

[36] X. Zhang and M. Tehranipoor, "RON: An on-chip ring oscillator network for hardware Trojan detection," in Design, Automation & Test in Europe Conference & Exhibition (DATE), 2011, 2011, pp. 1-6.

[37] A. Ferraiuolo, X. Zhang, and M. Tehranipoor, "Experimental analysis of a ring oscillator network for hardware trojan detection in a 90nm asic," in Proceedings of the International Conference on Computer-Aided Design, 2012, pp. 37-42.