Hardware Trojans and Their Detection for Cryptography Algorithms and Open Issues

[1]Dixita Gupta, [2]Ajay Kumar, [3]Kiranjit Kaur, [4]Alpana Agarwal, [5]Manu Bansal

[1]Master of Teshnology, [2]Research Scholar, [3]Lab Engineer, [4]Associate Professor, [3]Assistant Professor
[1]Electronics & Communication Engineering Department,
[1]TIET, Patiala, India.

Abstract : Due to time-to-market and effective cost competition, these days the Integrated Circuits are designed and fabricated in a multivendor environment. In these environments, there are many un-trusted foundries involved in IC design and fabrication. Therefore, it is easy to add a hardware Trojan at any level of design or fabrication process. Hardware Trojan is a malicious modification in the integrated circuits. There are three types of Trojan depending on how they are activated and their action affects the functional circuit. These Trojans are Trojan with payload, Trojan with only trigger, and Trojan with trigger and payload. The effects are functional failure of IC, decrease expected lifetime, and leakage of secret information. This paper defines the different techniques to add hardware trojans from RTL to gate level and various detection techniques. In addition, analysis of different hardware trojans and detection is presented. The study suggests that currently bit-stream and memory modifications are the parameters used for Trojan insertion in FPGA and obfuscation is used for security purposes. Also, based on the analysis different research issues are discussed.

IndexTerms **- Trojan, Register Transistor Logic (RTL), Field Programmable Gate Array (FPGA), Application Specific Integrated Circuits (ASIC).**

I. INTRODUCTION

Due to globalization of integrated circuit (IC) industry, it's easy for the third party to add Hardware Trojan in the circuit. Hardware Trojan is basically a modification in the circuit which alters the functionality of an IC. The modern Integrated Circuit design flow is shown in Fig. 1.

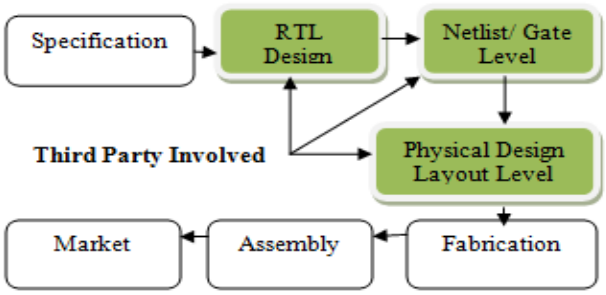

Fig.1 Modern Integrated Circuit Design Flow (K. Xiao et al. 2016).

The first step involved is the translation of specification into a RTL level using Hardware Description Language (HDL). Next, the behavioral description is transformed into design implementation using Net listing. After the Netlist, the layout is design at the physical design level. Then, the digital GDSII file is handed to a foundry for IC fabrication. Once the foundry fabricates IC, it goes to the wafer/die level testing process to check and ensure its correct operation. Those dies who pass testing are packaged by assembly unit and sent to market (K. Xiao et al. 2016).

1.1 Overview of Trojans

Trojan is a malicious circuit which is added in the circuit, to alter or leak the secret information from it. The simplest trojan is the insertion of an extra hardware in the circuit as shown in Fig. 2, which passes the input data directly to output after triggering at the select line.

Fig. 2 Basic Block Diagram of Hardware Trojan

1.2 Comparative Analysis between Software and Hardware Trojans

Table 1 shows the comparative analysis between software and hardware trojan. Software Trojan is a malware program which harms the Operating System (OS) or may steal the information. On the other hand, Hardware Trojan is a malicious circuit which on being added to an IC leaks or increases power, delay or both in the circuit.

Table 1 Comparative analysis between Software and Hardware Trojan (Swarup Bhunia et al. 2014)

Software Trojan	Hardware Trojan
A malware code inside the main program and activates during its execution.	Hardware Trojan inside the IC and activates during operation
Once executed effected the system, like making multiples files, slows the system.	Once executed effects the system like power consumption increases, leakage of bit stream, delay increases.
Software trojan can be easily removed using protection software available.	Hardware trojans can never be removed, once the IC is fabricated.

1.3 Hardware Trojan Design

Hardware Trojan contains two parts: Trigger and Payload. A Trojan trigger mechanism monitors the various signals or event in the circuit and at particular combination the Trojan is activated. There are two types of triggering.

- Internal Triggering
- External Triggering

In Internal Triggering, the Trojan node monitors the internal signal of the logic to activate the Trojan. On the other hand, in an external triggering, the malicious circuit is added externally on the chip like antenna or other sensors which trigger the Trojan nodes. There are two triggering methods.

- Combinational Trigger Circuit
- Sequential Trigger Circuit

The Combinational Trigger circuits depend on simultaneous occurrence of a node condition. For example, in Fig. 3 on a whenever a predefined condition occurs on a and b, it triggers a malfunction. These combinational Trojan circuits add up on rare occurrence of condition and are difficult to predict. On the other hand, in sequential trigger circuits the malfunction activates after undergoing a sequence of state transitions. For example, as shown in Fig. 3, at a predefined counter value Trojan triggers in the circuit.

The Payload taps the signal from the original circuit and on the activation of the trigger circuit; it performs malicious operation in the circuit. Most of the time payload is inactive and is not easy to detect. There are three types of Trojan and payload combinations available. These are

- Trojan with Payload
- Trojan with only Trigger
- Trojan with Trigger and Payload

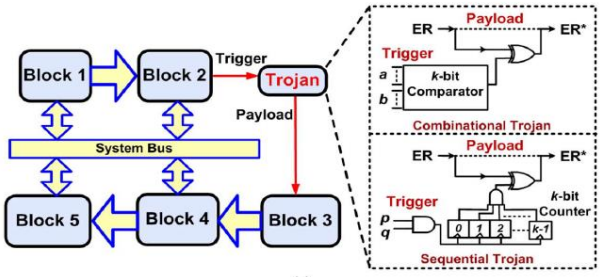

Fig. 3 General Model for Combinational and Sequential Trigger Circuit (Swarup Bhunia et al. 2014)

The rest of the paper is organized as follows. Section II defines a survey on hardware trojan and detection techniques. Further, section III defined the open research issues for future work. Section IV the paper has been concluded.

II. LITERATURE SURVEY

In this section, the literature is divided into two parts which includes Hardware Trojan Insertion techniques and Hardware Detection techniques.

2.1 Hardware Trojan Insertion Techniques

Pawel Swierczynski et al. 2015 discuss how, Trojan weaken the security system of AES and 3-DES algorithms by modify the bitstream. They have analyzed the LUT for extracting the S-boxes or key bits. Their algorithm has an advantage that detection of bitstream even if there is no knowledge of internal routing. Also, disucssed the counter-measure how to protect the bit stream for detection.

Rajat Subhra Chakraborty et al. 2013 discuss how insert Hardware Trojan by directly modifying the FGPA configuration bit-stream. The strength of their attack is that it bypasses all predeployment design validation mechanism. They defined some techniques to prevent from attacks.

Pawel Swierczynski et al. 2016, discuss how on the target device, a FIPS 140-2 level 2 Certified USB flash drive from Kingston used. The user data is encrypted using AES 256 in XTS mode. For Trojan insertion scenario the USB flash drive is intercepted before being delivered to victim.

Hassan Salmani and Mohammed Tehranipoor 2013 discuss how Hardware Trojans are inserted at behavioral level. Also, work on which part of circuit is more susceptible to Hardware Trojan.

Deian Stefan et al. works on Alpha Project. Alpha is a portable communication system designed to securely encrypt and transmit secret message. There are two trigger mechanism. One is based on, waits for the user to simultaneously press the start encryption and transmit button to activate Trojan. Other based on modify the keyboard interpretation.

2.2 Hardware Trojans Detection Techniques

Shane Kelly et al. 2015 discuss how, on chip sensor's effectiveness is measured using Ring Oscillator Network for Trojan detection. They inserted 23 trojans on chip to check the effectiveness of RON structure. Also, implemented and fabricated on an ASIC test chip using IBM 90nm technology.

Bao Liu and Brandon Wang 2015 defined the VLSI design security methodology based on reconfiguration based VLSI obfuscation, reconfiguration based VLSI moving target defense, and generic reconfiguration. In their case studies they prevent software and hardware based code injection attacks at a cost of 0.72% area increase, negligible power consumption and no performance degradation on SPARC V9 LEON 2 processor. They further work on preventing unauthorized memory access at cost of 4.42% area increase, negligible power consumption increases, and 11.30% critical path delay increases.

Rajat Subhra Chakraborty and Swarup Bhunia 2011. To protect the Integrated Circuit from Hardware Trojan, they design the Obfuscation technique. The Obfuscation provides protection against trojans that tries to leak secret information from an IC.

Sabyasachi Deyati et al. 2016 Due to Hardware Trojan insertion, the node capacitance increases. A high resolution pulse propagation technique is used to capture these nodes capacitance. There technique is independent of logic depth in the path.

M. Ritesh et al. 2015 Discusses how reducing the trojan activation time by dummy scan. In this, first the nodes with fewer transitions are determined and then at each node according to transition probability a threshold probability is defined. The nodes which has the transition probability lesser than the threshold probability are suspects for Trojan activation line and a dummy flip-flop inserted to each of these nodes such that its transition probability increases and thereby reducing the activation time of trojan, which makes the trojan visible during simulation.

Nicole Fern and Kwang-Ting Cheng 2015 Based on Mutation testing, they define an automated Trojan Detection Methodology. The technique has wide range of abstraction level for Trojan detection. The Mutation Testing technique detects Trojan that leak secret information from the design by modifying unspecified functionality.

Jeyavijayan Rajendran et al. 2016 Due to globalization, third party has involved in the designing process. So, overall system security depends on third party trustworthiness. They are using duplication, diversity, and isolation principal for Hardware Trojan detection. The overhead increases by 100% but there technique not required Golden IC for Trojan detection.

Hirak Kashyap and Richardo Chaves 2016 In the last few years to add Hardware Trojan on FPGA, modify the configuration bitstream. They improve the security of dynamic reconfiguration of FPGA. They change the remotely received key with randomly generated key, unique for each configuration. There proposed work increases overhead by 1% the resource available.

Christian Krieg et al. 2014 Defined the verification method at design level to detect Hardware Trojans. They define assets and attackers, and outline which verification methods are suited to defend against which type of attack.

Tony F. Wu et al. 2016 most of the Hardware Trojan detection techniques apply during IC testing. But it is still possible the attack to go undetected. So, they prevent the attacks during synthesis, place and-route, and fabrication of IC with few overheads in power and area.

Yu Liu et al. 2015 based on Continuous extraction of side channel fingerprint and evaluation by on chip neural classifier they design a Concurrent Hardware Trojan Detection Methodology. Their proposed technique identifies hardware trojans when they are active.

Nicole Fern et al. 2015. discuss how, using don't care bits for leak internal circuit information without affecting the original functionality. The detection of such Trojans is impossible through functional simulation/ verification. So, they proposed a novel X-analysis technique which prevents the insertion of new trojans.

Mainak Banga and Michael S. Hsiao 2009 designed a sustained vector methodology to detect Trojans. They apply each vector multiple times at the input of both genuine and the Trojan circuits to ensure the reduction of external trigger circuit on the genuine circuit.

III. RESEARCH ISSUE

This section highlights the research issues that have been determined from the literature survey.

1. In most of the papers, for Trojan Detection the golden IC is used as a reference to compare with the Trojan IC. So, overall performance depends on how much the Golden IC is secure and reliable.
2. In Hardware implementation, a large number of Trojans attacks have been reported on cryptography algorithms. To overcome these issues some locks and watermarking techniques must be added so that no one violates the systems.
3. In FPGA, there is no nonvolatile memory available. So during configuration, the bit stream is loaded from external memory in FPGA. So one research direction can be towards securing a bit stream being loaded to FPGA.

IV. CONCLUSION

Due to globalization, the modern Integrated Circuit design flow has been explained and the various levels of the third party involvement have also been described. So, system's overall security depends on the trustworthiness of the third party. Based on the available literature, an analysis between software and Hardware Trojans, Trojan insertions and how to detect Trojan on FPGA has been done. From the survey it has been concluded that the bit stream modification is used for Trojan insertion and Obfuscation technique is used for security purposes. Moreover, this work also defines some research issues that can be worked upon in future.

REFERENCES

[1] K. Xiao, D. Forte, Y. Jin, R. Karri, S. Bhunia and M. Tehranipoor, 2016. Hardware Trojans: Lessons Learned after One Decade of Research.ACM transactions on Design Automation of Electronic Systems, 22(1): 6.1-6.23.

[2] Swarup Bhunia, Michael S. Hsiao, Mainak Banga and Seetharam Narasimhan, 2014.Hardware Trojan Attacks: Threat Analysis and Countermeasure.Proceeding of the IEEE, . 8: 1229-1247.

[3] Pawel Swierczynski, Marc Fyrbiak, Philipp Koppe, and Christof Paar, 2015 .FPGA Trojans through detecting and weakening of Crytpographic Primitives.IEEE transaction on Computer Aided Design of Integrated Circuits and Systems, 34(8): 1236-1249.

[4] Rajat Subhra Chakraborty, Indrasish Saha, Ayan Palchaudhuri, and Gowtham Kumar Naik,2013.Hardware Trojan Insertion by Direct Modification of FPGA Configuration Bitstream. IEEE Design and test: 45-54.

[5] Pawel Swierczynski, Marc Fyrbiak, Philipp Koppe, and Christof Paar, 2016.Interdiction in practice: Hardware Trojan against a high security USB flash drive.Journal of Cryptographic Engineering:1-13.

[6] Hassan Salmani and Mohammed Tehranipoor, 2013. Analyzing Circuit Vulnerability to hardware trojan insertion at the behavioral level.IEEE International Symbolism on Defect and Fault Tolerance in VLSI and Nanotechnology Systems: pp. 190-195.

[7] Deian Stefan, Christopher Mitchell and Christian Garcia Almenar.Trojan Attacks for Compromising Cryptographic Security in FPGA Encryption System.Information System and Internet Security.

[8] Shane Kelly, Xuehui Zhang, Mohammed Tehranipoor, and Andrew Ferraiuolo, 2015.Detecting Hardware Trojans using On-Chip Sensors in an ASIC Design.Journal of Electron Test.31: 11-26.

[9] Bao Liu and Brandon Wang,2015. Reconfiguration based VLSI Desgin for Security. IEEE Journal on Emerging and Selected Topics in Circuits and Systems.5(1):98-108.

[10] Rajat Subhra Chakraborty and Swarup Bhunia,2011.Security Against Hardware Trojan Attacks Using Key Based Design Obfuscation.Journal of Electron Test,27:767-785.

[11] Sabyasachi Deyati, Barry J. Muldrey, and Abhijit Chatterjee,2016.Trojan Detection in Digital Systems Using Current Sensing of Pulse Propagation in Logic gates. IEEE 17th International Symposium on Quality Electronic Design:350-355.

[12] M. Rithesh, G. Harish and Siva Yellampalli, 2015. Detection and Analysis of Hardware Trojan using Dummy Scan Flip Flop. International Conference on Smart Technologies and management:439-442.

[13] Nicole Fern and kwang-Ting Cheng,2015. Detecting Hardware Trojans in Unspecified Functionality Using Mutation Testing. IEEE/ ACM International Conference on Computer Aided Design:560-566.

[14] Jeyavijayan Rajendran, Ozgur Sinaoglu, and Ramesh Karri,2016.Building Trustworthy Systems Using Untrusted Components: A High Level Synthesis Approach. IEEE transactions on Very Large Scale Integration Systems: 1-11.

[15] Hirak Kashyap and Richardo Chaves, 2016. Compact and On the Fly Secure Dynamic Reconfiguration for Volatile FPGA. ACM Transactions on Reconfigurable Technology and Systems, 9(2): 11.1-11.22.

[16] Christian Krieg, Michael Rathmair, and Florian Schupfer, 2014. A Process for the Detection of Design Level Hardware Trojans Using Verification Method. IEEE 6th International Symposium on Cyberspace Safety and Security:729-734.

[17] Tony F. Wu, Karthik Ganesan, Yunqing Alexander Xu, H.S Philip Wong, Simon Wong, Subhasish Mitra, 2016.TPAD: Hardware Trojan Prevention and Detection for Trusted Integrated Circuits. IEEE transaction on Computer Aided Design of Integrated Circuits and Systems, 35(4): 521-534.

[18] Yu Liu, Georgios Volanis, Ke Huang, and Yiorgos Makris,2015.Concurrent Hardware Trojan Detection in Wireless Cryptographic ICs.IEEE International Test Conference: 1-8.

[19] Nicole Fern, Shrikant Kulkarni and Kwang- Ting Cheng, 2015.Hardware Trojans Hidden in RTL Don't Cares-Automated Insertion and Prevention Methodologies. IEEE International Test Conference: 1-8.

[20] Mainak Banga and Michael S. Hsiao, A Novel Sustained Vector Technique for the Detection of Hardware Trojans. 22nd International Conference on VLSI Design:327-332.