IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 13, Issue 3, Ver. I (May. - June. 2018), PP 68-73
www.iosrjournals.org

Dynamic Hardware Reconfigurable System Using Partial Reconfiguration Procedure of FPGA

S.Murali[1*], K.Rakesh[2]
[1*](Department of ECE, MVGR college of engineering (A), vizianagaram, India)
[2](Department of ECE, MVGR college of engineering (A), vizianagaram, India)
Corresponding Author: S.Murali

Abstract : *Recently, reports about hardware Trojan insertions have been insertions have been on rise. Outsourcing of designs and usage of third party IP cores have put the end user information at stake. It is necessary to have a detailed study to be able to develop organized methods to identify their presence. Many identification methods have been proposed which require a Trojan free chip (Golden Chip). In this paper we introduce about Trojan insertion, methods to detect the Trojan. Reconfigurable systems have been proposed in order to safeguard from Trojan attack. By using the Partial reconfiguration, dynamic modification of the system is analyzed.*

Keywords - *Dynamic Reconfiguration, Hardware Trojan, Partial reconfiguration, Reconfigurable systems, Third-party IP cores.*

Date of Submission: 14-05-2018 Date of acceptance: 29-05-2018

I Introduction

Day by Day advancements in technology has brought multiple new devices into the market. The continuous evolution of electronics brought a huge competition between the manufacturers. Faster marketing of a product is necessary in order to win over the competitors, which led to usage of Third Party IP cores in the design. The third party IP cores are provided by different vendors, which reduce the reliability of circuit designs. Some third party IP cores are infected by malicious circuitry which tends to leak sensitive information. End users need to be guaranteed that their designs are free from hardware Trojans.

A hardware Trojan is defined as unwanted extraneous logic inserted in the original design. Trojans can be inserted at any point during manufacturing or during design. Due to high maintenance cost of fab units and continuous changes in fabrication facilities, there tend to be very less fabrication units. Most of the design houses are fab-less due to which the manufacturers depend on offshore facilities for their designing. This is due to increase in system complexity, high maintenance cost, shorter marketing time and increased competition.

The presence of Hardware Trojans inside a design is very difficult to detect as these Trojans remain embedded in the system. Multiple methods have been proposed for detection of Trojans. These methods try to detect the existence of Trojans either by studying side channel analysis [1-2], [3-6] or by introducing architectural changes. Most of these methods compare the suspected chip with a golden chip (Trojan free chip). But the availability of golden chip is very rare and cost effective.

We can classify hardware Trojan detection methodologies into two major categories, Architectural methodologies and Side channel methodologies [9]. In architectural methodologies the Trojans are detected by modifying the proposed architecture which tries to increase the chances of Trojan activation during testing. Salmani et al tried to increase the Trojan activity by inserting a dummy flip flop [8]. Rajendran et al introduced a method in which all gates are secured using ring oscillators [7]. The changes in ring oscillator frequency are used to detect the Trojans.

Side channel methodologies localize the impact of a Trojan, without activating them. In this methodology Trojans are detected for different circuit parameters such as delay, power consumption, quiescent current etc. Yousra Alkabani et al used nonintrusive external IC quiescent current measurements for Trojan detection [2]. Gate level characterization for different parameters such as delay, switching power and leakage measurements were discussed by M.Potkonjak et al [10]. These methods are discussed under different constraints. Moreover with the parallel increase of number of gates and scaling of the device size, gate level characterization is limited to a particular size.

Third Party IP's are incorporated for faster designing of circuits but at the cost of information security of end user. The side channel analysis and architectural modifications require a golden chip model for comparison which is not readily available. When using a third party IP the chances of availability of Golden Chip are less and the available models for Trojan detection provided by the Third Parties are not dependable.

With the advancement of FPGA technology and the partial reconfiguration feature of FPGA, dynamic reconfiguration of a function is possible. With the dynamic reconfiguration feature a part of FPGA is possible to reconfigure. Dynamic function replacement for system on chip security in the presence of hardware based attacks has been described by Lok-Won Kim in (11). During dynamic replacement, direct multiplexing of bus signals has been proposed. AMBA based bus protocol is a standard for communication between different blocks of the system. Modified bus architectures such as address decoder, arbiter, and bus multiplexer have been described in (12). Multiplexing reconfigurable IP's outputs and CRC Trojan detection Schema, Multiple Variants method in which multiple IP's outputs from different vendors are replaced dynamically. The outputs of different IP's are voted against each other by the CRC voting circuit [13].

II Trojan Classification

Due to the increase of outsourcing by IC vendors, there is a serious risk that malicious third-party vendors insert hardware Trojans very easily into their IC products. However, detecting hardware Trojans is very difficult because today's ICs are huge and complex. A hardware Trojan taxonomy helps us to identify different types of Trojan and their affects. Effectiveness of designed detection methodologies requires a comparison metric, Trojan taxonomy lets us compare and thus helps the researcher to develop comprehensive detection methods.

To implement a method for detection of Trojan, it is essential to define the classification of Trojan. Classification of Trojan is based upon different characteristics such as physical, activation and action characteristics. Further classification of physical characteristics is divided into type, size, distribution, structure. [9]

Several Trojan taxonomies that group Trojans based on triggering and leaking mechanisms have been developed. All these classifications assume that Trojans have been inserted at fabrication step only. However, insertion of Trojans is possible at different stages of manufacturing. A detailed Trojan classification is shown in figure 1. Different levels of Trojan insertions is grouped under insertion phase, a designer can insert hardware Trojans by modifying the original logic. During testing, the test cases can bypass the Trojan detection. In the abstraction phase, system level, gate level, physical level, development environment and other factors can lead to insertion of Trojans [16].

Activation characteristics refer to Trojan activation mechanism during which disruptive function takes place. Activation Characteristics are categorized into internally activated and externally activated. Action characteristics define the type of modification to the original design.

Trojans can be classified by the undesirable effects caused in the system. Severity of these effects can range from small effect to disastrous system failures. A Trojan hiding the core may affect the system by changing the functionality, degrading the performance, leaking of sensitive user information based on the designed Trojan.

A Trojan can be present at one single location or in multiple components. These Trojans can either act independently or together as a group and can affect the system at different levels. During detection of Trojans, it is important to locate the Trojan in order to tackle with it. Hence, location of a Trojan also becomes a part of Trojan Taxonomy.

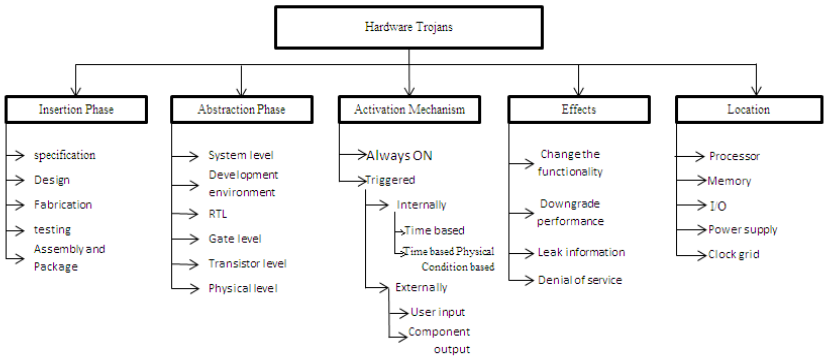

Fig 1 Hardware Trojan Classification

III Trojan Insertion

A hardware manipulation can be introduced at different levels of manufacturing. The reliability of Third party IP's is also questionable. In this work we designed three types of Trojans based on their activation mechanism. These Trojans are activated at different instances which affects the circuit behavior. Three different types of designed Trojans are: Always on Trojan, Condition based Trojan, User Input Trojan. Assuming that,

any kind of Trojan is intended to defeat the original functionality/stealth of information etc. The designed Trojans in the work shows two kinds of effects on the original logic; Change of Functionality, Denial of Service. Change of functionality represents the change in the functioning behavior of the logic. When this kind of Trojan gets activated the functionality of the original logic is manipulated and the intended behavior of the original logic changes.

Some Trojans block the entire system such that the required functionality is ceased. This kind of blocking can be stated as denial of service. During the designing phase manipulation can be made in the logic. Some unwanted logic is inserted which cannot be detected during the regular testing. In large systems writing test cases for every instance and verifying them is a tedious process. The designer takes care such that the Trojan gets activated for a rare combination and hence remains dormant during testing. Trojan insertion by direct bit stream modification is discussed in [14].

IV Trojan Detection

In this section, we try to identify the inserted Trojans and their effect on the design. A System-on-chip consists of multiple functioning modules, which requires interconnection among each other for the purpose of data transfer and to communicate among other interfacing logic. A system bus hence serves for this purpose and hence has a very crucial role in a SoC. A system bus is a component which connects different resources on a system. The allocation of memory and other resource sharing for the intended functions are to be provided by the system bus. In general a bus mediates the bus master ship, during multiple signals requesting for access of a particular block. This process requires decrypting the master module signal to requesting slave module and hence forming an interconnection between both the modules.

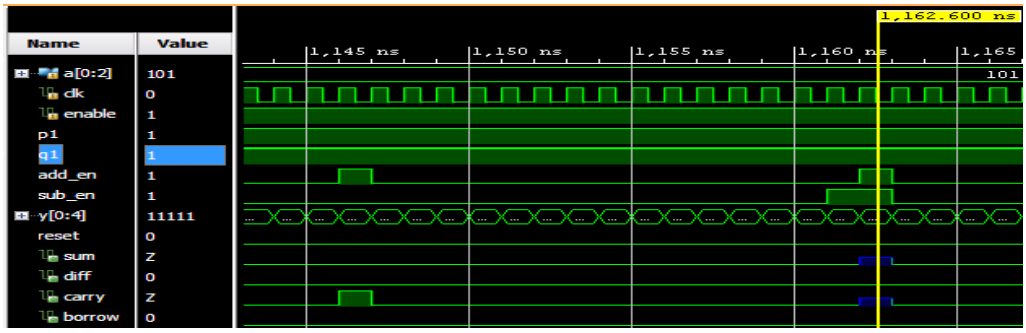

Fig 2 Simulation result for denial of service Trojan

In our design, the inserted Trojans hang the system bus during their activation. As designed the Trojan gets activated for a particular event during which it denies the normal functioning i.e. it denies the regular services. This can be verified by the simulation results as shown in Figure-2. The above simulation results shows that when a Trojan gets activated for a brief period of time the system bus is taken into its control. This small time frame can be utilized to leak data or to downgrade performance of the system. The activation time of a Trojan may be small but it could affect the circuit in a large proportion.

Not only denial of service, there may be different kinds of effects as per the designed Trojan and its activation time. For a particular condition based Trojan designed, the change of functionality can be observed when there is Trojan activation.

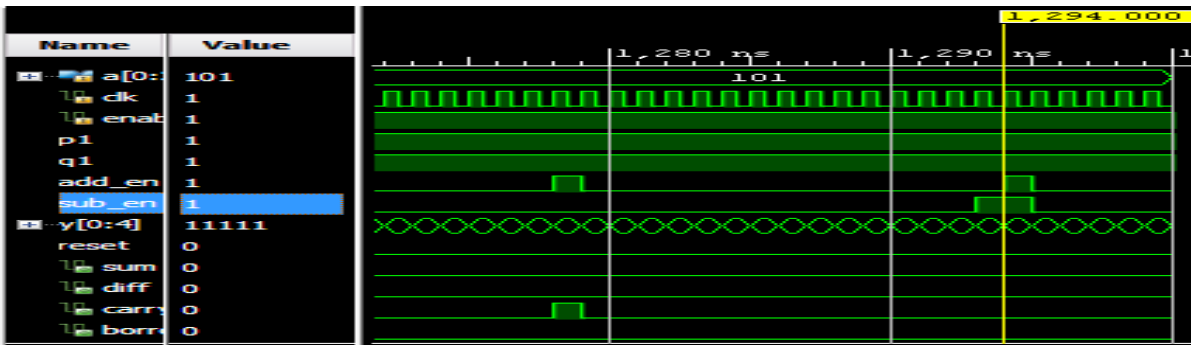

Fig 3 Change of Functionality Trojan

In this result we can find that when the add_en and sub_en are high the adder function is not as intended. The simulation results can be seen in figure 3. Detection of a Trojan is a challenging task as the

designers try to hide the Trojan's such that they aren't detected while testing. This has been a difficult task in order to verify the trust of a designed module. In order to verify, a golden model is required, which may not be available at all times this has brought different methods to verify the third party modules. A Sustained Vector technique for Trojan detection has been discussed in [2], in which the detection and isolation of a Trojan is based on the differential power profile. Side channel analysis techniques have been introduced in [3].

V Recoverable Methodologies

Trojan attack on a system doesn't cause permanent failure of the whole system. These systems can be recovered from Trojan attack by reconfiguration. Full reconfiguration requires the complete chip data to be formatted thus in order to recover the system from the Trojan attacks. In this paper, we propose partial dynamic reconfiguration technique. In this technique we try to change the Trojan based design dynamically at run time without affecting the other running modules. Partial reconfiguration enables us to divide the system into static and Reconfigurable parts, where a reconfigurable part can be modified multiple times. A simple illustration of Partial reconfiguration is shown in figure 4.

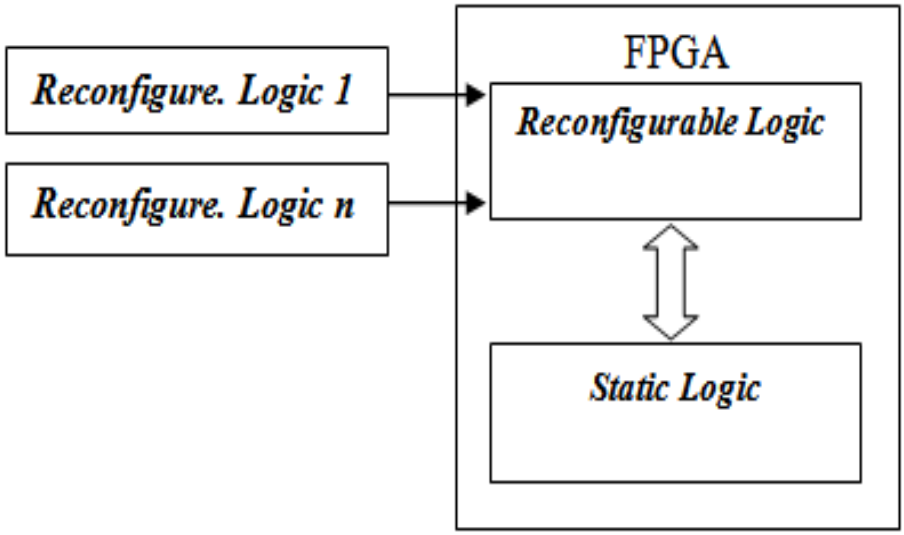

Fig 4. FPGA Partial reconfiguration

With the advent of FPGA and Partial reconfiguration features, the error module can be replaced with Trojan free module. When a particular Trojan attacks the system the Trojaneous module is replaced dynamically. In our model, we practically performed Trojan insertion, detection and recovery by using Partial reconfiguration. By using partial dynamic reconfiguration reusability is achieved and system resources and time is saved. The PR methodology and steps have been discussed in [15]. The total steps undergone during partial reconfiguration is shown in the below figure 5.

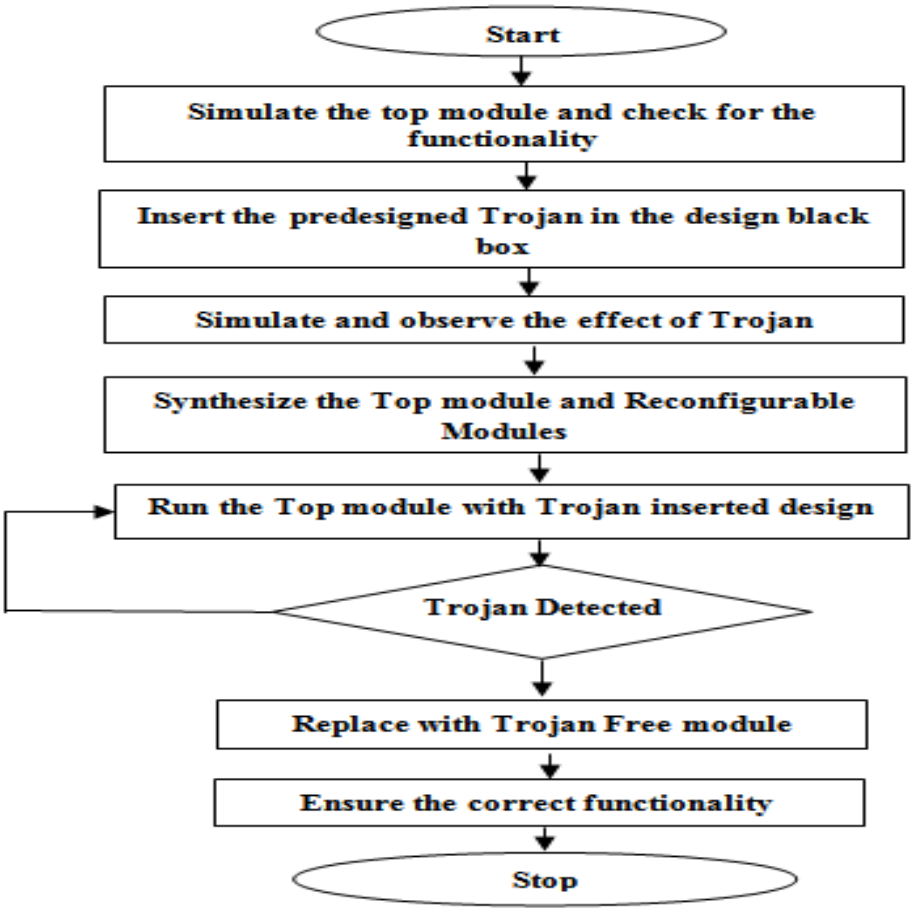

Fig 5. Flow chart for Partial Reconfiguration

The presence of Hardware Trojans affects multiple system parameters. Considering the overall power utilization we can observe the variations in power for Top module, where only logic definition is stated, without the hardware Trojans and during the presence of hardware Trojans. The increase in power can be seen when compared with Trojan free module. The Table 1 shows power summary of different modules.

Table- 1 Power summary of different modules

Power Summary			
Module	Total On chip Power (W)	Junction Temperature (°C)	Thermal Margin (°C)
Top (Logic definition)	0.557	27.5	57.5
With Hardware Trojan	1.142	30.2	54.8
Without hardware Trojan	1.119	30.1	54.9

VI Conclusion

Hardware Trojans pose a serious threat. In this work we present, insertion of hardware Trojans, detection and recovery, using the dynamic partial reconfiguration. By replacing the infected logic we are able to remove the Trojan from the original logic, which means we are eliminating the Trojan logic. This technique can be implemented on the field and hence has high practical application compared to the earlier discussed solutions. This technique also serves very cost effective way as the changing of reconfigurable modules requires minimum expertise.

References

[1]. M. Banga, M. Chandrasekar, L. Fang, and M. Hsiao. Guided test generation for isolation and detection of embedded trojans in ICs.In Proceedings of the 18th ACM Great Lakes symposium on VLSI, GLSVLSI '08, pages 363–366, 2008.

[2]. M. Banga and M. S. Hsiao. A novel sustained vector technique for the detection of hardware trojans. In Proceedings of the 22nd International Conference on VLSI Design, pages 327–332, 2009.

[3]. D. Du, S. Narasimhan, R. Chakraborty, and S. Bhunia. Self-referencing: a scalable side-channel approach for hardware Trojan detection. In Proceedings of the 12th international conference on Cryptographic hardware and embedded systems, CHES'10, pages 173–187, 2010.

[4]. Y. Jin and Y. Makris. Hardware Trojan detection using path delay fingerprint. In Proceedings of the IEEE International Workshop on Hardware-Oriented Security and Trust, pages 51–57, 2008.

[5]. F. Koushanfar, A. Mirhoseini, and Y. Alkabani. A unified sub modular framework for multimodal IC Trojan detection. In Proceedings of the12th international conference on Information hiding, IH'10, pages 17– 32, 2010.

[6]. M.Potkonjak, A.Nahapetian, M.nelson, and T.Massey. Hardware Trojan horse detection using Gate level Characterization. In proceedings of the 46th annual design automation conference, DAC, pages 688-693, July 2009

[7]. J. Rajendran, V. Jyothi, O. Sinanoglu, and R. Karri. Design and analysis of ring oscillator based design-for-trust technique. In VLSI Test Symposium (VTS), 2011 IEEE 29th, pages 105–110, may 2011.

[8]. H. Salmani, M. Tehranipoor, and J. Plusquellic. New design strategy for improving hardware trojan detection and reducing trojan activation time. In Proceedings of the IEEE International Workshop on Hardware-Oriented Security and Trust, HOST '09, pages 66–73, 2009.

[9]. M.tehranipoor and F.Koushnfar. A survey of Hardware Trojan Taxonomy and detection. IEEE Design and Test of computers, pages10-25, February 2010.

[10]. Xiaoxiao Wang, Hassan salmani and M.tehranipoor, Jim Plusquellic. Hardware Trojan detection and Isolation using current Integration and Localized Current analysis. In proceedings of the IEEE International Symposium on defect and fault Tolerance of VLSI Systems, Page 87-95, October 2008.

[11]. Lok-won kim and john D.villasenor. Dynamic function replacement for system-on-chip security in the presence of hardware-based attacks. IEEE transaction on reliability, pages 661-674. June 2014.

[12]. Lok-Won Kim and John D.Villasenor. A System-On-Chip Bus Architecture for Thwarting Integrated circuit Trojan Horses. IEEE transactions on very large Scale Integration(VLSI) Systems, pages:1921-1926. October 2011

[13]. Amr Al-Anwar, Yousra Alkabani, M.Watheq El-Kharashi, Hassan Bedour. Hardware Trojan Detection Methodology for FPGA. IEEE Pacific Rim Conference on communications, computers and signal processing (PACRIM), pages 177-182, October 2013.

[14]. RS chakraborty, Indrasish saha, Ayan Palachaudhuri et al. Hardware Trojan Insertion by Direct Modification of FPGA Configuration Bit stream. IEEE design and Test, pages 45-54, February 2013

[15]. https://www.xilinx.com/support/documentation/sw_manuals/xilinx2017_1/ug947-vivado-partial-reconfiguration-tutorial.pdf

[16]. R. Karri, K. Rosenfeld, J. Rajendran and M. Tehranipoor, "Trustworthy Hardware: Identifying and Classifying Hardware Trojans," in IEEE Compute society, vol. 43, pages: 39-46, 2010.

IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) is UGC approved Journal with Sl. No. 5016, Journal no. 49082.

S.Murali, "Dynamic Hardware Reconfigurable Systems Using Partial Reconfiguration Procedure of FPGA." IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) 13.3 (2018): 68-73.