ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2015

A SoC Trojan Virus Detection and Correction Using Multiple Monitoring Schemes

Prof.N.Ravi[1], S.Beulah Hemalatha*[2]

Assistant Professor, Dept. of ECE, Jerusalem College of Engineering, Chennai, Tamil Nadu, India[1]

Assistant Professor, Dept. of ECE, Bharath University, Chennai, Tamil Nadu, India[2]

* Corresponding Author

ABSTRACT*:* A design of 16 bit processor is programmed in VHDL. The processor module is added with extra hardware logic calle d Trojan .A fault bit pattern is injected into the circuit along with the processor clock. The fault bit patterns triggers the extra hardware hidden in the processor that can be detected by verifying the output result from memory and cpu.

I. INTRODUCTION

Hardware Trojan detection is an extremely challenging problem and traditional structural and functional tests cannot effectively address it. Trojan circuits have stealthy nature and are triggered in rare conditions. Trojans are designed such that they are silent most of their life time and may have very small size relative to their host design, with featuring limited contribution into design characteristics. These suggest that they most likely connect to nets with low controllability and/or observability[1].

A hardware Trojan (hardware Trojan horse (HTH) or malicious circuit) is a malicious modification of the circuitry of an integrated circuit. A hardware Trojan is completely characterized by its physical representation and its behavior. The payload of an HTH is the entire activity that the Trojan executes when it is triggered[2]. In general, malicious Trojans try to bypass or disable the security fence of a system: It can confidential information by radio emission. HTHs also could disable, derange or destroy the entire chip or components of it. Motivated adversary takes advantage of restriction to tamper IC supply chain by maliciously implanting extra logic as hardware Troj an circuitry into an IC. Consequently serious concerns rise about security and trustworthiness of electronic systems. An attacker can change a design net list or subvert the fabrication process by manipulating design mask, without affecting the main functionality of the design. In this paper, we develop a methodology to increase the probability of generating a transition in functional Trojan circuits and to analyze the transition generation time[5],[6].

Today's business is global and for this reason outsourcing tasks is a common method to increase companies' revenues. That is why embedded hardware devices are produced abroad. But outsourcing poses a serious threat, especially for government agencies. Typically threatened sectors are the military, finance, power or the political sector. The hardware integrity, i.e. a chip has no modifications in comparison with the original chip design, is not ensured. Everyone that has access to the manufacturing process of a chip can do malicious alterations to the design[7].[8]. The fabrication of integrated circuits that are manufactured in untrustworthy factories is common. An adversary tries to hide the additional components; hence advanced detection techniques are necessary[9].

One of these physical Trojan characteristics is the type. The type of a Trojan can be either functional or parametric[10]. A Trojan is functional if the adversary adds or deletes any transistors or gates to the original chip design. The size of a Trojan is its physical extension or the number of components it is made of[3],[4]. Because a Trojan can consist of many components, the designer can distribute the parts of a malicious logic on the chip. The additional logic can occupy the chip wherever it is needed to modify, add or remove a function. If the function of the Trojan demands it, on the one hand malicious components can be scattered. This is called loose distribution. On the other hand a Trojan can consist of only few components, so the area is small where the malicious logic occupies the layout of the chip. In contrast this is called tight distribution. The typical Trojan is condition-based: It is triggered by sensors internal logic states, a particular input pattern or an internal counter value. Condition-based Trojans are detectable with power traces to some degree when inactive. That is due to the leakage currents generated by the trigger or counter circuit activating the Trojan.

design. In this paper, we develop a methodology to increase the probability of generating a transition in functional Trojan circuits and to analyze the transition generation time.

II. PERIPHERAL DEVICE HARDWARE TROJAN HORSES

A relatively new threat vector to networks and network endpoints is a HTH appearing as a physical peripheral device that is designed to interact with the network endpoint using the approved peripheral device's communication protocol [9]. For example, a USB keyboard that hides all malicious processing cycles from the target network endpoint to which it is attached by communicating with the target network endpoint using unintended USB channels. Once sensitive data is exhilarated from the target network endpoint to the HTH, the HTH can process the data and decide what to do with it: store it to memory for later physical retrieval of the HTH or possibly exhilarate it to the internet wirelessly or using the compromised network endpoint as a pivot. A common Trojan is passive for the most time span an altered device is in use, but the activation can cause a fatal damage. If a Trojan is activated the functionality can be changed, the device can be destroyed or disabled, and it can leak confidential information or tear down [11]. the security and safety. Trojans are stealthy, that means the precondition for activation is a very rare event. Traditional testing techniques are not sufficient. A manufacturing fault happens at a random position while malicious changes are well placed to avoid detection.

III. DETECTING HARDWARE TROJANS

.3.1 Physical Inspection

First, the molding coat is cut to reveal the circuitry. Then, the engineer repeatedly scans the surface while grinding the layers of the chip [13-14]. There are several operations to scan the circuitry. Typical visual inspection methods are: scanning optical microscopy (SOM),scanning electron microscopy (SEM), pico-second imaging circuit analysis (PICA), voltage contrast imaging (VCI), light induced voltage alteration (LIVA) or charge induced voltage alteration (CIVA).

3.2functional Testing

This detection method stimulates the input ports of a chip and monitors the output to detect manufacturing faults. If the logic values of the output do not match the genuine pattern, then a defect or a Trojan could be found.

.3.3 Built-In-Self-Test

Built-in self-test (BIST) or Design-for-test (DFT) is additional functionality within the chip used to verify functionality of the chip. BIST and DFT are implemented as additional circuitry (logic in the c hand these techniques are used to detect manufacturing errors, but could possibly be used to detect unintended (malicious) logic on the chip [10]. Depending upon the purpose of the BIST, it could possibly be used to detect the presence of unintended (malicious) logic, but this would be highly dependent upon the BIST functionality itself. BRAIST functionality often exists to perform at-speed (high speed) verification where it is not possible to use scan chains or other low-speed DFT capabilities. It is more likely that DFT would be appropriate to recognize unintended logic. A genuine chip generates a familiar signature, but a defect or altered chip displays an unknown signature [12]. The signature can be any number of data outputs from the chip: an entire scan chain or intermediate data result. Most modern chips will fuse or disable (through hardware configuration) the ability for chip to perform BIST or DFT outside of a manufacturing environment; this is important because DFT or BIST could, itself, be used in a subversive attack on the chip [15].

3.4 Side Channel Analyses

Every device that is electrically active emits different signals like magnetic and electric fields. Those signals that are caused by the electric activity can be analyzed to gain information about the state and the data which the device processes. Advanced methods to measure this side-effects have been developed and they are very sensitive (side-channel attack). Hence, it is possible to detect tightly coupled Trojans via measurement of these analog signals. The measured values can be used as a signature for the analyzed device. It is also common that a set of measured values is evaluated to avoid measurement errors or other inaccuracies.

IV. HARDWARE TROJAN TAXONOMY AND DETECTION

The detailed taxonomy showing physical, activation, and action characteristics of Trojans is shown in the fig.1. ICs are becoming increasingly vulnerable to malicious activities and alterations. These vulnerabilities have raised serious concerns regarding possible threats to military systems, financial infrastructures, transportation security, and household appliances. An adversary can introduce a Trojan designed to disable or destroy a system at some future time, or the Trojan could leak confidential information and secret keys covertly to the adversary Trojans can be implemented as hardware modifications to ASICs, commercial-off-the-shelf (COTS) parts, microprocessors, microcontrollers, network processors, or digital-signal processors (DSPs).They can also be implemented as firmware modifications to, and for example, FPGA bit streams.

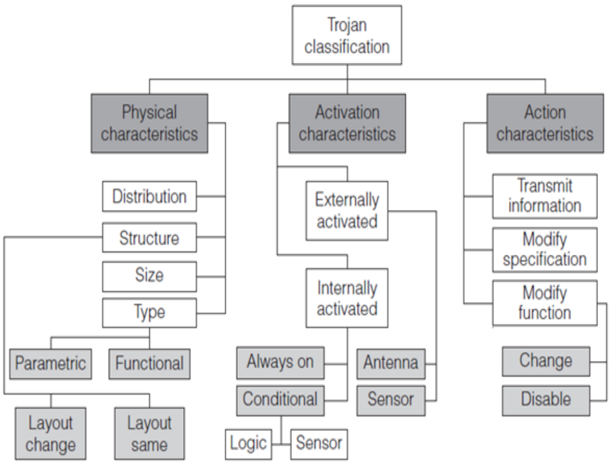

Fig.1 Detailed taxonomy showing physical, activation, and action characteristics of Trojans.

They can also be implemented as firmware modifications to, and for example, FPGA bit streams. These concern shave been documented in recent reports from the US Defense Science Board task force,1 the US Senate,2 IEEE Spectrum,3 and Semiconductor Equipment Materials International.

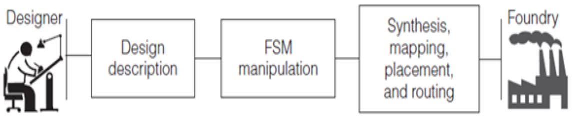

Fig.2 Insertion of an HTH during the design process of an IP core

Fig.2 shows an abstract view of the design process. The Trojan designer composes the high-level design description to find the computation model of the circuit that a finite-state machine (FSM) can represent. An HTH can be inserted into the circuit by altering the FSM and embedding states into it. The modified FSM should have a trigger as an input and a driver hidden in the structure of the FSM. This FSM can be systematically hidden in the design by merging its states within the states of the original design’s FSM. Thus, the HTH would be inseparable (irremovable) from the original design’s functionality. A stealth communication, which uses the medium for legitimate communications, can serve as a covert channel to transfer confidential data from the working chips to the adversary.

This Trojan-embedding approach provides a low-level mechanism for bypassing higher-level authentication techniques.

V.SOC IMPLEMENTATION

5.1 TROJAN VIRUS DETECTION BLOCK DIAGRAM

The Block Diagram for Trojan Virus Detection
is shown in fig..3

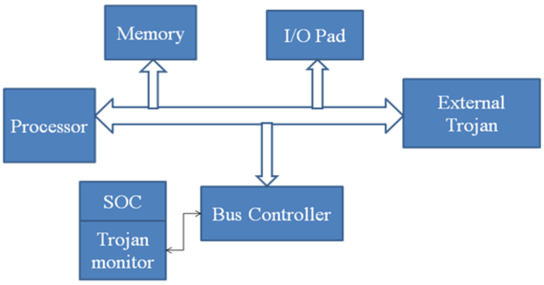

Fig.3 Block Diagram **of** Trojan virus detection block

5.2 MULTIPROCESSOR

The Block diagram for Multiprocessor is shown in the Fig.4

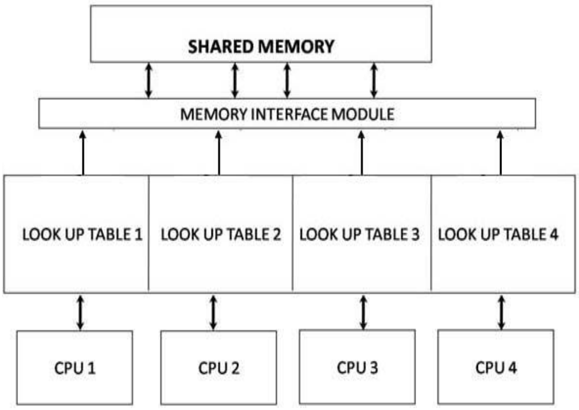

Fig.4 Network on chip (soc) based multiprocessor

A distributed-memory system (often called a multicomputer) consist of multiple independent processing nodes with local memory modules, connected by a general interconnection network and Global shared memory. A DSM system logically implements the shared-memory model on a physically distributed-memory system.The DSM system hides the remote communication mechanism from the application writer, preserving the programming ease and portability typical of shared-memory systems.

Read Only Memory (ROM) is memory whose stored data can only be read but cannot be re-written (altered). It is a device in which “permanent” binary information has been stored. ROMs are nonvolatile where stored data are not lost even when power is turned OFF.Like RAMS, a ROM has n address inputs and m outputs. This corresponds to 2^n memory words each of m storage bits for a total capacity of 2^n x m bits shown in fig 3.2.2.1Unlike RAMs, ROMs do not have data input lines, because they do not have a write operation.

10.15662/ijareeie.2015.0401072

ROMs are common to use in storing system-level programs that should be available at all times. The most common example is the PC system BIOS (Basic Input Output System), which is stored in a ROM called the system BIOS ROM.

The Parallel Port is the most commonly used port for interfacing homemade projects. This port will allow the input of up to 9 bits or the output of 12 bits at any one given time, thus requiring minimal external circuitry to implement many simpler tasks.The port is composed of 4 control lines, 5 status lines and 8 data lines. It's found commonly on the back of your PC as a D-Type 25 Pin female connector. There may also be a D-Type 25 pin male connector.

VI. SIMULATION RESULTS

The simulation results for Processor demonstrate that it is possible to significantly increase switching activity in Trojan circuits. Smaller Trojans may be fully activated and cause functional failures. Larger Trojans more contribute into side-channel signals and are detected as abnormality.

VII.CONCLUSION

A design of 16 bit Processor with Trojan affected environment is successfully designed using VHDL. The simulated results exhibits the differenttypes of error occurrences caused by Trojan injectionlike hang,reset,corrupt,etc. The simulated design will be modified to work under a real time criteria and results will be synthesized using Quartus -11 software.

REFERENCES

1. A novel sustained vector technique for the detection of hardware Trojans by .M. Banga and M. S. Hsiao
2. Security against hardware Trojan through a novel application of design obfuscation and by R. S. Chakraborty and S. Bhunia.
3. Sengottuvel P., Satishkumar S., Dinakaran D., "Optimization of multiple characteristics of EDM parameters based on desirability approach and fuzzy modeling", Procedia Engineering, ISSN : 1877-7058, 64() (2013) pp.1069-1078.
4. A region based approach for the identification of hardware Trojans byM. Banga and M. S. Hsiao.
5. Guided test generation for isolation and detection of embedded Trojans in ICs by M. Banga, M. Chandrasekar, L. Fang, and M. S. Hsiao.
6. Anbazhagan R., Satheesh B., Gopalakrishnan K., 'Mathematical modeling and simulation of modern cars in the role of stability analysis", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S5) (2013) pp.4633-4641.
7. P ower supply signal calibration techniques for improving detection resolution to hardware Trojans by R. Rad, X. Wang, J. Plusquellic, and M. Tehranipoor.
8. Muruganantham S., Srivastha P.K., Khanaa, "Object based middleware for grid computing", Journal of Computer Science, ISSN : 1552-6607, 6(3) (2010) pp.336-340.
9. Hardware Trojan detection and isolation using current integration and localized current analysis by X. Wang, H. Salmani, M. Tehranipoor, and J. Plusquellic.
10. Rajendran S., Muthupalani R.S., Ramanathan A., "Lack of RING finger domain (RFD) mutations of the c-Cbl gene in oral squamous cell carcinomas in Chennai, India", Asian Pacific Journal of Cancer Prevention, ISSN : 1513-7368, 14(2) (2013) pp.1073-1075.
11. Hardware Trojan Detection using Gate level characterization by M. Potkonjak, A. Nahapetian, M. Nelson, and T. Massey
12. Hardware Trojan detection using path delay fingerprint by Y. Jin.
13. Langeswaran K., Revathy R., Kumar S.G., Vijayaprakash S., Balasubramanian M.P., "Kaempferol ameliorates aflatoxin B1 (AFB1) induced hepatocellular carcinoma through modifying metabolizing enzymes, membrane bound ATPases and mitochondrial TCA cycle enzymes", Asian Pacific Journal of Tropical Biomedicine, ISSN : 2221-1691, 2(S3)(2012) pp.S1653-S1659.
14. Consistency-based characterization for IC Trojan detection by Y. Alkabani and F. Koushanfar.
15. Towards Trojan-free trusted ICs: Problem analysis and
16. detection scheme by F.Wolff, C. Papachristou, S. Bhunia, and R. S. Chakraborty
17. B Karthik, TVUK Kumar, MA Dorairangaswamy, E Logashanmugam, Removal of High Density Salt and Pepper Noise Through Modified Cascaded Filter, Middle East Journal of Scientific Research, 20(10),pp 1222-1228, 2014.
18. Daimiwal, Nivedita; Sundhararajan, M; Shriram, Revati; , Applications of fMRI for Brain MappingarXiv preprint arXiv:1301.0001, 2012.
19. Daimiwal, Nivedita; Sundhararajan, M; Shriram, Revati; , Respiratory rate, heart rate and continuous measurement of BP using PPGIEEE Communications and Signal Processing (ICCSP), 2014 International Conference on, PP 999-10022014.
20. Kamatchi, S; Sundhararajan, M; , Optimal Spectral Analysis for detection of sinusitis using Near-Infrared Spectroscopy (NIRS) .
21. Shriram, Revati; Sundhararajan, M; Daimiwal, Nivedita; , Human Brain Mapping based on COLD Signal Hemodynamic Response and Electrical NeuroimagingarXiv preprint arXiv:1307.4171, 2013
22. [21]Daimiwal, Nivedita; Sundhararajan, M; Shriram, Revati; , Comparative analysis of LDR and OPT 101 detectors in reflectance type PPG sensorIEEE Communications and Signal Processing (ICCSP), 2014 International Conference on, PP 1078-1081,2014