International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-4, November 2019

Design, Implementation and Detection of Hardware Trojans in Sequential systems

L.K.Hema, S.A.V. Satya Murty,Vijayan Sugumaran

Abstract*: For decades, digital systems have been designed based on assumptions that the underlying hardware, though not perfectly reliable, is free of malicious elements. The demand for IC's is greatly increasing due to tremendous technological development. Without appropriate resources the companies are hard pressed to produce trusted IC's. This is driving the companies into the 'fabless' trend predominant in semi-conductor industry, where the companies are depending on cheaper foundries for the IC fabrication instead of depending on their own resources. This growth brings with it a big rise in threat level in terms of Hardware Trojans that hits the manufacturing companies which make use of Integrated Circuits. This transcends many industries, including strategic organizations and telecommunication companies, mobile phones and computers, embedded systems used in domestic applications and health care equipment. These adversarial inclusions are generally triggered to do malicious modifications in the end user system by the intruder, which is difficult to detect in their quiescent state. This paper focuses on understanding Hardware Trojans, their implications and detection methodologies. It is extremely important for all industries and more so for defense organizations, who are involved in developing systems to protect the nation's boundaries.

***Keywords:** Hardware Trojans, Reverse Engineering, sequential, Side Channel Analysis, Trigger*

I. INTRODUCTION

Technological developments in the area of Electronic Systems, computers, communications and Internet have made dramatic changes in the way we design military systems, industrial process control systems, communication systems and the way we work, communicate and live. These developments have influenced even the common man. Thus, today's electronics systems, computers, networks and Internet are extensively used in every industry and organization. The usage includes Strategic operations that protect the country, industrial systems automation, strategic communications, office automation, ERP, Internet Banking, e-Tendering, e-Commerce etc. Even the strategic organizations use them for these applications and even more.

Manuscript published on November 30, 2019.
* Correspondence Author
Dr.L.K. Hema*, Dept. of ECE, Aarupadai Veedu Institute Of Technology, Vinayaka Mission's Research Foundation, chennai, India.
Dr. S.A.V. Satya Murty, Aarupadai Veedu Institute Of Technology, Vinayaka Mission's Research Foundation, chennai, India.
Dr. Vijayan Sugumaran, Department of Decision and Information Sciences School of Business Administration Oakland University, Rochester

Though these are positive developments, information security of these varied systems has become a very big concern. The number of hacking incidents is increasing alarmingly with time. The hackers are particularly targeting strategic organization's networks, banking systems, e-Commerce sites etc. for obvious intentions of stealing confidential data, illegal money transactions etc.
This is the only concern till about a decade back. The underlying hardware was considered safe. The essential hardware used for different applications are considered to be trusted. However, the adversaries may inject Hardware Trojans (HT), which could lead to severe dysfunctionality of electronic hardware that violates the fundamental assumption of the hardware root of trust.

II. HARDWARE TROJANS ATTACKS

A Hardware Trojan can be described as a malicious inclusion into an integrated circuit (IC) that will modify its anticipated function thereby leads to catastrophic effect in strategic applications. This can be a simple stuck at zero or struck at one Trojan to a complex modification. Trojan consists of two parts: Trigger and Payload. The Trigger part decides when the Trojan is to be active and when it should be dormant. The Payload part is the actual modification to a system which does the damage. Trojan is designed by keeping two aspects in mind: one is malicious intent which determines extent of damage to be caused and the other is how to evade being detected during standard testing. These adversarial inclusions are generally triggered to do malicious modifications at the end user side by the intruder which is difficult to detect in their quiescent state. Table 1 shows the reported Hardware Trojan attacks brought to light just a decade ago. These are the potent attacks on electronic hardware that has shaken the hardware root of trust. (ACM Trans., 2016).

Table 1. Reported Hardware Trojan Attacks

SNo	Incidence	Type of attack	Source
1	Failure of Syrian Radar	The Syrian Radar failed to detect the Israeli missile attack due to the COTS microprocessor being fabricated with hidden malicious inclusions.	IEEE spectrum, 2007

2	Insertion of Remote kill switches	An European IC fabricating company had introduced remote kill switches in their microprocessor which can be controlled remotely.	IEEE spectrum, 2007
3.	Counterfeit chips	40% of US Military supply Chain has counterfeit chips. A hidden 'back door' in a computer chip could allow cyber-criminals a way to override and control computer systems on Boeing 787s.	dailymail.co.uk, 30th May 2012
4	Intel IVY bridge incident	Done by Sabotaging the cryptographic capability of Intel processors including the latest Ivy Bridge which is the heart of most 2012 PCs.	The Tech Repor,2013
5	Tiny spying chip	Purportedly planted a tiny spying chip on widely distributed server motherboards. The report contends that more than 30 companies, including Apple and Amazon, as well as the U.S. defense department, may have been at risk of data leaks.	Bloomberg report
6	Dell warns of Hardware Trojan	Computer Manufacturer Dell warned that some of their server mother boards have been delivered to customers carrying an unwanted computer malware.	Homeland Security News wire 2010
7	Bogus computer Gear in Cisco Router	F.B.I reported that a Trojan horse is lurking in the circuitry of a computer or network router	The New York Times, 2008

The various industries which are affected by the Hardware Trojans are Military, Financial Infrastructures and Consumer Industries.

Types of Attacks

Integrated circuits are prone to various kinds of attacks and they are classified into four types depending on the mechanism according to which the attack has been carried out.

Attack by Hack: It is carried out by software execution namely viruses and malware. These are downloaded and installed unknowingly by the user via physical or wireless connection.

Attack by shack: A shack attack may be a low-budget equipment attack utilizing hardware that may be bought from a store like Radio Shack. In this situation, the intruders get the access of the integrated Circuits not directly but via network analyzers, pins etc.

Attack in Lab: The lab attack is more comprehensive and obtrusive. The attackers do the reverse engineering and get the sensitive design part of the IC. By attaching microscopic logic probes to Si metal Layers which introduces glitches into the circuit. Also by monitoring the EM radiations, temperature variation and power management they attack to get the cryptographic information.

Attack during Fab: It is the lowest level of attack where the HT's are inserted in the layout, net list of an IC during fabrication by untrusted vendors.

Based on the different types of attacks, we cannot suggest a single method, as such, that can observe diversified Hardware Trojan threats.

Attack Models

Hardware Trojans shall be inserted at various phases of design / fabrication by malicious intruders and are classified into i) IP core development ii) SoC development, iii) Fabrication. The various attack models proposed are Model A (Untrusted 3 PIP), Model B(Untrusted Fab), Model C (Untrusted SoC Developer), Model D (Untrusted COTS), Model E(, Model E (Untrusted design in supply chain except foundry), Model F (Untrusted outsources) and Model G (Untrusted System Integrator) and these model address about the targets of Hardware Trojans.

III. HARDWARE TROJAN CLASSIFICATION

The classification of hardware Trojan is based on the following attributes and is shown in Figure 1. (Tehranipoor et al. 2010).

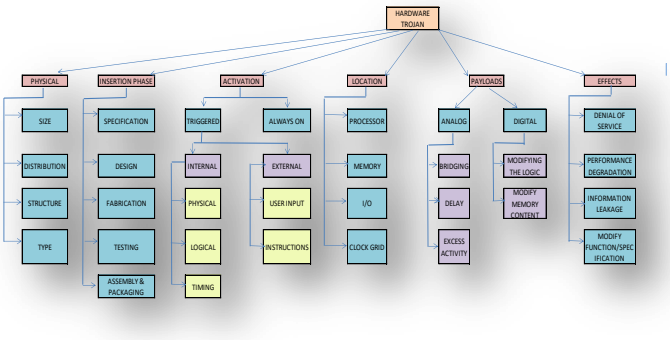


Figure 1. Hardware Trojan Classification

i. Insertion phase: This phase ranges from defining the hardware characteristics (i.e., design specifications) to physical IC placement (i.e., assembly) on a printed circuit board (PCB).
ii. Abstraction phase: This level spans from the physical dimensions and locations of the internal components in the circuit (i.e., physical level) to the final definitions of interconnects and communication protocols used in the IC (i.e., system level).
iii. Activation phase: It describes the means by which the Trojan is triggered viz. internal sequential counters and through input data streams.
iv. Effects phase: This ranges from change of functionality to Denial of Service.
v. Location phase: Targeting single component (e.g. System clock) to multiple complex components such as processors.
vi. Based on Payloads: Analog and Digital Trojan.

IV. COUNTER MEASURES FOR HARDWARE TROJAN

Hardware Trojans, as we know, are modifications done to a built-in circuit via an intruder to get right of entry to or manipulate records stored in the chip, tenacity to do denial of service or even ruin the chip based on the class of the Trojan inserted. It is very vital to take appropriate countermeasures for defending purchaser privacy, essential infrastructures, and key sources. Detection of hardware Trojan has been receiving widespread interest due to the increase in the number of attacks and the damage caused. It is essential to identify the hardware Trojans beforehand since they can't be removed after insertion, unlike the software Trojans which can be removed even after inserted in to the system. Also, with each new detection method being implemented, new Trojans that can overcome these detection strategies are also being introduced. Thus, continuous research and knowledge of the Hardware Trojans being used is essential. The detection approach to be used depends on the kind of Trojan and the section of insertion. While some techniques require an adaption in the hardware design process or extra circuitry, others do not require any change. Some techniques rely on non-stop monitoring of the machine in the course of runtime. Nowadays, IC's are manufactured from untrusted fabrication process since the vendors now prefer fabless processing and therefore it is necessary to ensure about the hardware security for the systems used for strategic application. Hardware Trojan Detection is becoming a challenging task due the following reasons:
(i) Many complicated IPs are used in the circuit, thus detecting miniature malicious intrusions in circuits are very difficult.
(ii) Devices and Circuits used presently are in nanometer size and Hardware Trojans detection by destructive testing is expensive and the process is also cumbersome.
(iii) Hardware Trojans' trigger circuits are designed to activate the payload when specific special conditions are met and hence, Trojan activation probability while conducting the tests is sporadic.
The counter measures for the malicious Hardware Trojan are classified into 3 types: HT Detection, Design for Trust and Split Manufacturing for Trust.

Hardware Trojan Detection

Detection is the first step in handling HT and corresponding preventive measures can be applied. Hardware Trojan Detection methods are depicted in Figure 2.

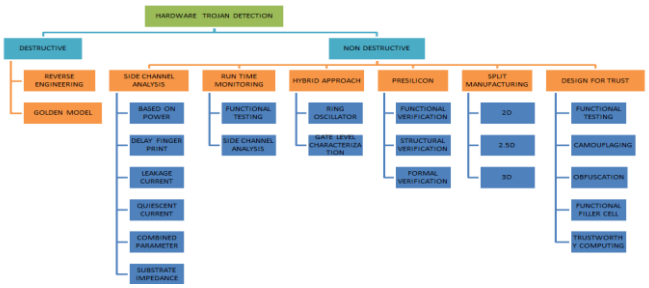


Figure 2.Hardware Trojan Detection methods

They are carried out during the design phase to validate IC designs or after the manufacturing stage (i.e., post silicon) to verify fabricated ICs. The types of Hardware Trojans testing are classified into i) Destructive Testing and ii) Nondestructive testing. (Bao et al. 2016).

V. PREVENTIVE APPROACHES OF HARDWARE TROJAN INSERTION

The most important distinction between the investigative technique and preventive approach is, in investigative Trojan detection method the ultimate goal is to determine whether any unspecified product is Trojan-free or not, while in a preventive technique, the objective is to discourage Hardware Trojan insertion into a specific product, which can be achieved either by making it very easy to detect Trojans in it or making it very difficult for certain untrusted parties to insert Trojans (Chakroborty et al. 2009). Figure 3. depicts the preventive measures of Hardware Trojan insertion.

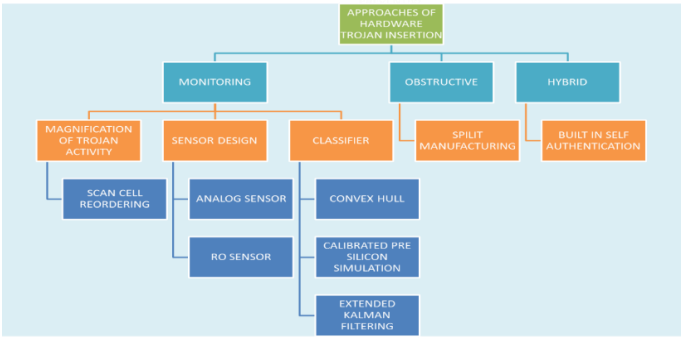


Figure 3. Preventive approaches of Hardware Trojan Insertion

The different approaches are: a) Monitoring approach- Detection of Trojan presence through monitoring is most commonly done through side-channel measurements impacted by Trojan activity.
b) Obstructive Approach- Instead of trying to activate the Trojans and capture their activity, the obstructive approach seeks to prevent their insertion altogether. The merits are obvious: If Trojans cannot be inserted, then there is no need to activate and/or detect a Trojan. As a corollary, golden chips/models, side-channel profiling, and accurate classification are not needed.

c) Hybrid Approach- The hybrid approach refers to techniques that consist of both monitoring and obstruction and therefore does not have the same strengths and weaknesses of either. The built-in self-authentication (BISA) technique is one such example.

VI. HARDWARE TROJAN BENCH MARKS

The Trojan benchmarks are coined with their physical, action and activation characteristics of Hardware Trojans. There are different types of Trojans available and no single detection technique will apply for the HT detection. So HT bench marks that describe the specific technique on particular design at a particular moment have to be developed. This leads to the analysis and design of different HT benchmarks that has gained focus of design and verification experts. The bench marks for each type of Trojan comes along with credentials that summarize the vital characteristics of trust bench mark namely probability of trigger for gate/layout level Trojans, input vectors (RTL/Gate Level), Path delay induced by the Trojan, Size of the Trojan and for some specific bench marks "golden Model" (Trojan free Version) which will enable in analyzing the trust bench marks in terms of various attack models described earlier.

VII. IMPLEMENTATION OF HARDWARE TROJANS AND DETECTION THROUGH FUNCTIONAL TESTING

In our research, we have designed four different circuits into which hardware Trojan is inserted in the design level/RTL level. They are briefly described below.

Countdown Circuit 1

Consider the launch of a missile. It has the final stage where countdown begins from a specific count and reaches 0. On reaching 0^{th} count, the missile is launched. The same idea is applied for the implementation of the countdown circuit. The circuit does the normal operation of counting from 9 to 0. On reaching the 0^{th} count, the LED is blinked resembling the launch of missile. The countdown circuit 1 is shown in Figure 4(a).

Design of the circuit: This circuit consists of certain number of stages, say, S0, S1and S2. It does its normal operation during stages S0 and S1. In stage S2, it deviates from its normal behavior. It counts from 9 to 0 but does not wait for 0^{th} count for blinking LED. It blinks the LED prior to 0^{th} count, say, 2nd count, indicating the launch of missile before the launch time. This forms the Trojan activation in the circuit design. The functional simulation output in Figure 4(b) shows both the normal behavior and Trojan inserted condition.

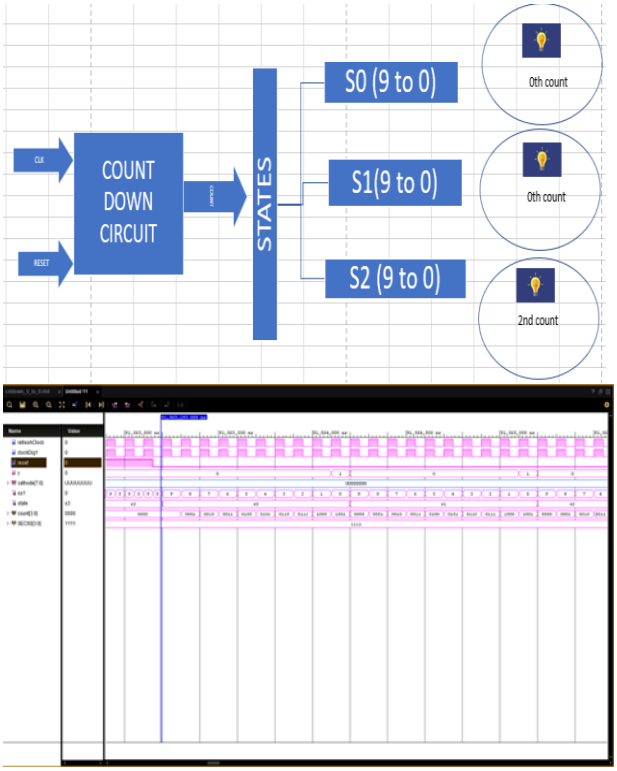


Figure 4(a). Countdown Circuit -1 Design
Figure 4(b). Functional Test-Simulation

Countdown Circuit 2

This is a countdown circuit implementing the idea of missile launch. The circuit has the normal operation of counting from 9 to 0. On 0^{th} count, it blinks the LED. Here, the Trojan activation takes a different turn. The normal function is to blink the LED on reaching the 0^{th} count. Here, Trojan activation is such that it will not make the LED to blink at all indicating a failed missile launch.

Design of the circuit: The circuit consists of three states of operation, say, S0, S1 and S2. The circuit is designed to perform its normal operation during the stages S0 and S1. In the stage S2, instead of blinking the LED at 0^{th} count, it doesn't blink the LED at all indicating the presence of hardware Trojan which causes the change in its normal behavior.

AES system

The AES system is a based on block cipher which will encrypt and decrypt the information for cyber security related applications. Encryption converts information to associate degree unintelligible type referred to as cipher-text. Decryption is the process of converting cipher text back to the actual information/plain text. The AES formula is capable of cryptological keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits. This process involves different steps applied consecutively over the input data blocks for specific number of times called rounds. The process for AES specifications consists of a number of different transformations applied consecutively over the data block bits, in a fixed number of iterations, called rounds. The number of iterations is decided by the key length used for encryption. The different transformations are: a)

Bytes Substitution Transformation, b) Shift Rows Transformation, c) Mixing of Columns Transformation, d) Addition of Round Key Transformation, and e) Key Schedule Generation. The number of rounds required for three different key lengths is as follows: AES-128: 10 Rounds, AES-192: 12 Rounds, AES-256: 14 Rounds.

Decryption process: This method is direct inverse of the encryption process. All the transformations namely key expansion, inverse Add Round Key, Inverse Shift Row, Inverse Sub bytes, Inverse Mix column are applied on the cipher text and finally original text will be obtained.

Implementation of AES: AES is coded in VHDL. The system is attributed with certain number of states such as S0, S1, S2 and S3. In the S0, S1 and S2 states, the circuit does normal encryption and decryption process. In S3 state, the system does not give desired result due to the insertion of hardware Trojan which is implemented by manipulating the **shift transformation** result in one of its rounds. The program is coded in VHDL language and simulated in Vivado 2018.2 version. The simulation output is shown in Figure 5.

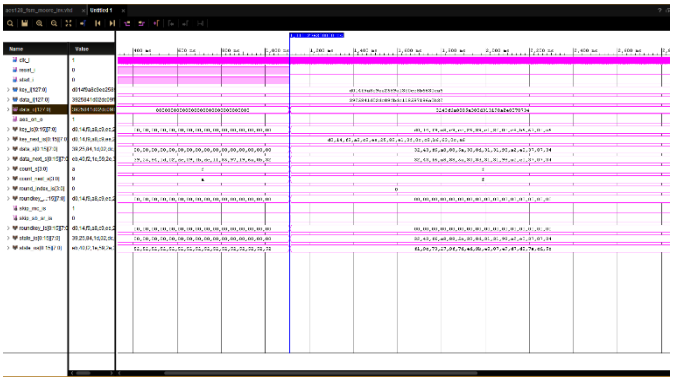
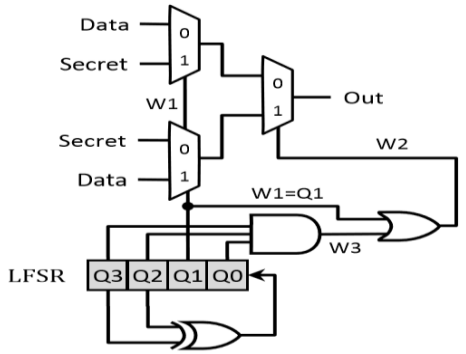


Figure 5. AES Decrypted output

Sequential circuit 3

The sequential circuit shown in Figure 6, is a LFSR based circuit that will output the data for normal operation. And during a specific clock cycle, the Trojan gets activated when the LFSR value is equal to 1101, which triggers the payload circuitry which is a combination of 3 Multiplexers. As soon as this condition is met the payload circuitry leaks the secret value instead of actual data. This is an example of trigger activated digital HTs which have digital payloads. The simulation output is shown in Figure 7. Consequently, in order to efficiently detect such HTs, one should know about the design parameters that are incorporated during the design of Hardware Trojan countermeasures



$Cycle$	$Q3$	$Q2$	$Q1$	$Q0$	$W1$	$W2$	$W3$
0	1	0	1	0	1	1	0
1	0	1	0	1	0	0	0
2	1	0	1	1	1	1	0
3	0	1	1	1	1	1	0
4	1	1	1	1	1	1	1
5	1	1	1	0	1	1	0
6	1	1	0	0	0	0	0
7	1	0	0	0	0	0	0
8	0	0	0	1	0	0	0
9	0	0	1	0	1	1	0
10	0	1	0	0	0	0	0
11	1	0	0	1	0	0	0
12	0	0	1	1	1	1	0
13	0	1	1	0	1	1	0
14	**1**	**1**	**0**	**1**	**0**	**1**	**1**

Figure 6. LFSR based circuit

.

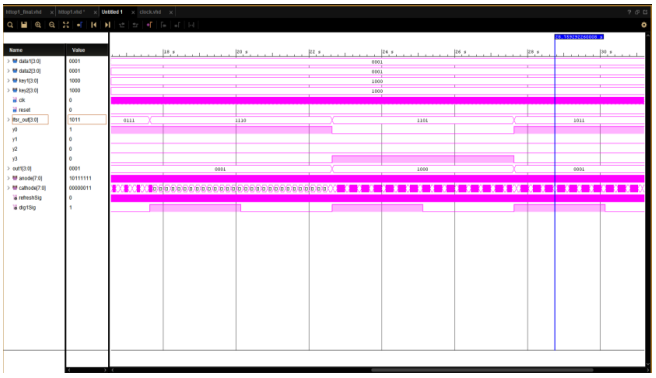


Figure 7. Functional Testing –Simulation output of Sequential circuit 3

VIII. CHALLENGES AHEAD AND PREVENTIVE APPROACHES

In the fast pace development of electronics industry, the necessity of IC's is incredible and vendors are moving towards 3PIP cores. Hence, the HT threat is also exponentially increasing and the consequent attacks lead the systems used in Strategic, Financial and consumer industries into catastrophe. Hence it is essential to device and develops new HT counter measures. They are,

Veritrust: It is a novel HT verification technique for hardware Trust. VeriTrust automatically identifies the probable HT trigger inputs by examining verification corners (Jie Zhang et al. 2015).

Hardware Trojan protection by logic encryption: This technique is based on the assumption that the intruder will attach a Trojan on signals having low controllability within a circuit.

The aim is to prevent the HT attacker from manipulating the actual low controllability signal by virtually modifying the probability of each signal to be either 0 or 1.

Hardware Trojan detection by rapid SEM imaging & machine learning: Machine learning algorithms are used to classify unique features of the golden model IC Layout and SEM images of an IC under verification. The descriptors are compared with one another and if there exists any restrained changes on the active region, a flag can be raised indicating the presence of malicious component. This SEM imaging and machine learning based Trojan scanner is more reliable than functional testing and fast enough as compared to reverse engineering techniques.

This scanner focuses on the real physical structure of the IC to detect the HT's inserted by the adversaries. The Trojan scanner carries out the detection in four phases namely: Preparation of the Sample, Rapid SEM imaging, Image Preprocessing, Feature clustering using K-Means algorithm and SVM, Detecting Gate level changes- via Golden chip Layout & SEM image (Courbon et al. 2015).

***Hardware Trojan detection by ring oscillator network with supervised machine learning technique*:** Ring oscillator networks are generally used to detect the Hardware Trojans by apprehending the difference in power consumption. In this traditional method the probability of Trojan detection shall be affected by the measurement noise and process variation (Zhang M et al. 2016). However, the process variation and measurement noise are the major obstacles to detect hardware Trojan with high accuracy. The proposed technique uses supervised machine learning algorithms and the required classifiers for optimization reveals that the accuracy has been improved with less False Positive Rate.

IX. CONCLUSION

Building a clear understanding of Hardware Trojans and developing powerful barriers requires a structure that classifies similar Trojans together to undertake a precise investigation of their qualities. Identifying the Trojans, applying appropriate counter measures and adopting preventive mechanisms would then be possible for every Trojan class alongside benchmarks. In our research we have implemented 4 different types of Hardware Trojans in sequential circuits and their presence is detected through functional testing. The Trojans implemented are malicious intrusions at the RTL level that resemble the malicious component inclusion in strategic applications that result in the failure of missile launch, leakage of cryptographic keys, denial of Service etc. The future challenges ahead in the domain of hardware Trojans are: handling more complex attacks at different stages of IC supply chain – thus necessitating more Automatic Vulnerability Tests, developing new trust metrics and benchmarks for different hardware abstraction levels, Golden-free trust verification problem against diverse trust issues, and HT attacks in Nano scale devices.

REFERENCES

1. Bao, C., Forte, D., and Srivastava, A. (2016). On Reverse Engineering-Based Hardware Trojan Detection. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 35(1), 49–57. https://doi.org/10.1109/TCAD.2015.2488495.
2. Chakraborty, R. S., Narasimhan, S., and Bhunia, S. (2009), Hardware Trojan: Threats and emerging solutions. Proceedings - IEEE International High-Level Design Validation and Test Workshop, HLDVT, (December), 166–171. https://doi.org/10.1109/HLDVT.2009.5340158.
3. Courbon .F, P. Loubet-Moundi, J. J. A. Fournier and A. Tria, "SEMBA: A SEM based acquisition technique for fast invasive Hardware Trojan detection," *2015 European Conference on Circuit Theory and Design (ECCTD)*, Trondheim, 2015, pp. 1-4. doi: 10.1109/ECCTD.2015.7300097.
4. Hardware Trojans: Lessons learned after one decade of research. (2016). ACM Transactions on Design Automation of Electronic Systems, 22(1). https://doi.org/10.1145/2906147.
5. Jie Zhang, Feng Yuan, Linxiao Wei, Yannan Liu and Qiang Xu. (2015). VeriTrust: Verification for Hardware Trust. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 34(7), 1148–1161. https://doi.org/10.1109/tcad.2015.2422836.
6. Tehranipoor, M., & Koushanfar, F. (2010). A survey of hardware Trojan taxonomy and detection. IEEE Design and Test of Computers, 27(1), 10–25. https://doi.org/10.1109/MDT.2010.7.
7. Zhang. X and M. Tehranipoor, "RON: An on-chip ring oscillator network for hardware Trojan detection," *2011 Design, Automation & Test in Europe*, Grenoble, 2011, pp. 1-6.doi: 10.1109/DATE.2011.5763260.
8. L.K.Hema et al," Wireless Sensor Networks' emergence and Growth-A survey"m International Journal of Computational Engineering Research (IJCER) ISSN: 2250-3005,Page No217-224.

AUTHORS PROFILE

L.K.Hema received her B.E Degree in Electrical and Electronics Engineering from Madurai Kamaraj University, Tamilnadu, in 1990, M.S Degree in Education Management from Alagappa University in the year 2007 and M. Tech Degree in VLSI Design from Sathyabama University in 2009. She has acquired her Doctorate Degree from Manonmaniam SundaranarUniversity.Since 1991 she has been working as Faculty in the Departments of Computer Science and Engineering, Electronics and Communication Engineering. Her research interests include Wireless Sensor Networks, VLSI Design, Hardware Security and Embedded systems. At present she is working as Professor and Head of the Department at AVIT and engaged in various Government funded projects. She is the life member of ISTE since 2009 and member in IEEE. MAIL ID: hemalk@avit.ac.in, hemjith2005@gmail.com

Dr. S.A.V Satya Murty is currently working as Director (Engineering & Technology Research) in Vinayaka Mission's Research Foundation (A Deemed to be University). Prior to joining VMRF, Dr. Satya Murty worked as Distinguished Scientist & Director of Indira Gandhi Centre of Atomic Research, Kalpakkam, the second largest R&D institute of Department of Atomic Energy, Government of India. Prior to that he held various senior Positions in IGCAR and has an excellent R&D career. Subsequent to his superannuation, he held Raja Ramanna Fellowship for two years.Dr. Satya Murty had a distinguished academic career. He did his B.Tech from Jawaharlal Nehru Technological University and was awarded Gold Medal for getting University First Rank. Subsequently he did one year Orientation Course in Nuclear Science & Technology at the training school of Bhabha Atomic Research Centre and was awarded Homi Bhabha Award for getting First Rank. He did his Ph.D from Homi Bhabha National Institute.He has more than 200 Publications in peer reviewed Journals and international & national conferences, Four book chapters, many design reports etc. He is the Editor of Two International Journals and one national journal.

Vijayan sugumaran is Professor of Management Information Systems and Chair of the Decision and Information Sciences department at Oakland University. Over the years he taught courses at the Graduate and Undergraduate level in Object-Oriented Systems Development, C++, Java, Javascript, Database Management Systems and Data Warehouses, Advanced Databases and Big Data Management, Systems Analysis and Design, Electronic Commerce, and Introduction to MIS. His research interests are in the areas of Big Data Analytics, Business Intelligence, Ontologies and Semantic Web, Intelligent Agent and Multi-Agent Systems, Component Based Software Development, Knowledge-Based Systems, and Data & Information Modeling. My most recent publications have appeared in Information Systems Research, ACM Transactions on Database Systems, IEEE Transactions on Engineering Management, IEEE software, Communications of the ACM, Healthcare Management Science, Data and Knowledge Engineering, The DATABASE for Advances in Information Systems, Information Systems Journal, and Journal of Information Systems and E-Business Management.He is the editor-in-chief of the International Journal of Intelligent Information Technologies and also serve on the editorial board of eight other journals.