ELEKTROTEHNIŠKI VESTNIK 84(1-2): 7-16, 2017
REVIEW SCIENTIFIC PAPER

# Malicious Hardware Detection and Design for Trust: an Analysis

**Sree Ranjani R , Nirmala Devi M**

*Department of Electronics and Communication Engineering, Amrita School of Engineering, Coimbatore, Amrita Vishwa Vidyapeetham, Amrita University, India.*
*E-mail: r_sreeranjani@cb.amrita.edu, m_nirmala@cb.amrita.edu*

**Abstract.** Hardware security is an emerging topic in integrated-circuit (IC) industries. Research in the domain of the hardware security is at a full swing and many schemes to enhance the security are being explored. The hardware Trojan (HT) design and its various detection techniques to ensure the trust in design are the most sought for schemes. The analysis of the reported techniques explores the major threat in the IC industries known as hardware Trojans and their countermeasures. Moreover, it clearly depicts the emerging trend in the hardware security with a direction indicating the future scope.

**Keywords:** Hardware security, Intellectual property, Hardware trojan, Trojan detection, Design for Security.

**Analiza in odkrivanje zlonamerne strojne opreme in načrtovanje z upoštevanjem zaupanja**

Zahteva po varnosti strojne opreme se čedalje bolj uveljavlja pri izdelovalcih integriranih vezij. Raziskave na področju varnosti strojne opreme so v polnem teku in raziskovalci analizirajo različne varnostne in zaščitne mehanizme pred zlonamerno strojno opremo (trojanska vezja), vgrajeno v integrirana vezja. V prispevku analiziramo najpogostejše nevarnosti zaradi vgrajenih trojanskih vezij in mogoče nasprotne ukrepe. V prispevku opišemo tudi zdajšnje smernice na področju varnosti strojne opreme in usmeritve za naprej.

## 1 INTRODUCTION

Secured hardware is necessary to upgrade the performance, reliability and efficiency of any system. Globalization of the IC design flow is the main reason for hardware vulnerabilities. The fabless industries have to depend on the untrustworthy fabrication units where the attacker can easily access the implementation of IC at any stage in the original IC design. Some untrusted IC fabrication company may illegally overbuild ICs and sell them in the market or an attacker in a fabrication unit may add a malicious circuit (hardware Trojan) to the original design [1]. It is reported that a hardware attack causes a loss of $4 billion annually to the semiconductor industry [2]. These hardware-related security issues directly spoil the efficiency of the architectures where hardware plays a major role in implementation such as cryptographic applications [3].

Various threats and hardware Trojans are proposed and their deterring methods are analysed in [4]. Hardware security includes detection and diagnosis of the hardware Trojans and design for secured hardware. Literature mainly focuses on the post-silicon phase to enhance the security [3-11] and the pre-silicon circuit protection against hardware Trojans is discussed in [12 & 13]. The security verification is carried out in the hardware description language (HDL) as a formal verification approach in software [14 & 15]. Availability of golden-chips used as a reference to detect the malicious activity of the chip is a big challenge to the researchers. Since none of the chips are trusted to be Trojan-free, Trojan-detection methods without having a golden-chip as a reference is the need of the hour. This survey considers hardware-Trojan taxonomy and gives a summary on various Trojan-detection methodologies. The rest of the paper is organized as follows. Section II elaborates on the hardware-Trojan detection and diagnosis methodologies. Section III describes the design-for-security schemes. Section IV draws conclusions of the survey.

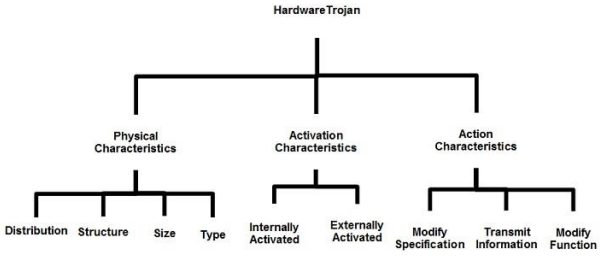


Figure 1. Trojan classification.

Hardware Trojans are added by the intruder in order to hinder the original design or to pilfer the secret information running on the chip. Many types of trojans have been designed by the researchers to evaluate the existing Trojan-detection techniques, as in [6], [16 &17]. Wang et al. developed a detailed hardware-Trojan taxonomy in [16]. Fig. 1 shows an abstract

*Received 28 November 2016*
*Accepted 27 February 2017*

classification of Trojans with their physical, activation and action characteristics as a major concern.

Further, Alkabani et al. [17] categorized hardware-Trojan-horses (HTHs) into an internal trigger, storage and hardware-Trojan driver. Hardware-Trojan-horses are inserted into ICs by a schematic approach of pre-synthesis manipulation to the design structure. Thus the Trojan-design engineers compose a high-level design description of the Trojan to embed it into the original design finite-state machine (FSM). The modified FSM with a hidden driver in its structure should be triggered by the input. Thus a trojan FSMs are injected into the original FSM design by merging their states and they are inextricable from the functionality of the original design. In order to steal the information from the working chip, the adversary will monitor the legitimate communication and use it as a media to transfer the confidential information. This Trojan-embedding method will bypass the high-level authentication techniques, so that their presence remains stealthy.

These stealthy hardware Trojans are hard to detect with conventional detection methods and the countermeasures against these Trojans are broadly classified into two categories, such as detection and diagnosis of Trojans and design for security.

## 2 HT Detection and Diagnosis Methodologies

Detection and diagnosis of the HT process can be broadly categorized into destructive and non-destructive approaches. Some approaches will continuously monitor the system during its run-time, while others verify the chips integrity after the production. The HT detection and diagnosis schemes categories are shown in Fig. 2.

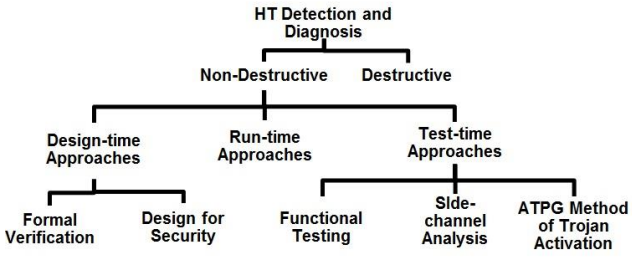


Figure 2. HT Detection and Diagnosis Schemes

### *2.1 Non-Destructive Approach to Trojan Detection*

The non-destructive method of the HT detection will ensure the presence of a trojan by examining the characteristic behavior of the chip. The prominent techniques to verify the integrity of the chip without destroying it include *Design-time, Test-time and Run-time approaches.*

#### *2.1.1 Design-time Approaches*

The design-time approach is a pre-silicon method of the Trojan detection and it detects the intellectual property (IP) threats. The adversary will add an additional design module to the original design (IP) without the knowledge of the trusted designer and these Trojans are not easy to detect during a verification test.

A formal verification is a process of property checking used to detect the presence of a Trojan by analysing the IP properties with golden-reference IPs. Banga et al. in [18] located malicious insertions in a third-party intellectual property (3PIP) with a four-step approach. In the first step, the functional vectors are used to remove the easy-to-detect signals and an N-detect full-scan automatic test-pattern generation (ATPG) tool is used in the second step to identify the functionally hard to excite signals. In the third step, the suspected signals are cross-checked by equivalence checking and eventually a region-isolation step helps to locate a Trojan-associated gate from a cluster of untestable gates in the circuit. The author experimentally proved that the proposed methodology distinguishes a tampered 3PIP from an authentic one and the region with a Trojan is identified effectively. However, the Trojans causing malfunctions when they are triggered alone can be detected by this approach.

Jin et al. [19] proposed an information-flow tracking approach by means of a proof carrying code method for the data-secrecy protection. The IP vendors generate proofs for the properties of secret data and add those properties to the circuit in a formal language, then supplied to the IP consumer. The IP consumer confirms the secured data properties of the circuit with a formal property checker and at the same time the HDL codes are converted into a formal logic. Then they are loaded to formal theorems as parameters. The IP consumer will receive both the RTL and proof codes along with the secret tags and the formal property checker will check the design. Thus the formal verification approaches enhance the security of the IP core by checking the IP properties. But the adversary with a good design knowledge will induce a malicious circuit as such formal verification tests fail to detect those hard to detect Trojans.

Though the design-for-security scheme comes under the classification of the design-time approaches, to thoroughly discuss the DfS scheme, it is catogarized under Section 3.

#### *2.1.2 Run-time Approaches*

The test-time approaches fail to detect the Trojans which are triggered after many clock cycles. The run-time approaches are used to detect a Trojan, throughout the IC life time by adding some modules like sensors to monitor the activity of the chip continuously. If there exists any variation in the behavior/state of the chip from the expected golden behavior, then an additional module will indicate the user. Thus the malicious

behavior is monitored in the run-time approach of the Trojan detection.

A run-time execution monitoring in both the hardware and software approach was proposed in [33]. An external hardware module is added to CPU in order to monitor its functionality. This work targets of the denial of service (DoS) attacks and some privilege escalation attacks. In [34], Hicks proposed a hybrid approach by combining a design-time component with a run-time monitoring known as Bluechip. The unused circuitry in the chip is identified by the design verification tests and they are replaced with an exception logic during the run-time. Thus the proposed method provides a detour for the malicious Trojans.

Bao et al. [35] proposed three approaches with thermal sensors to monitor the power/thermal profiles. In the first approach, the information from the thermal sensor is compared with the hypothesis testing to make a decision. In the second approach, the Kalman filter (KF) is used to exploit the correlation between the sensors and the thermal profile. The leakage power of the system is incorporated and simultaneously KF is applied to track the IC thermal profile in the third approach. This online-monitoring approach detects the Trojan that consumes less power (<1.54%) compared to the Trojan-free design.

Kim et al. [36] proposed an online, post-deployment functional verification approach to detect run-time hardware attacks. Two different SoC designs emulated in an FPGA-based test-bed are functionally verified by a dynamic function verification (DFV). The proposed anti-Trojan DFV functions are evaluated with several hardware attacks. The misbehavior of each IP module allows for a successful detection. Thus the run-time hardware attacks are easily detected by the online-monitoring DFV techniques. However, the extra logic used for online monitoring will result in an area and power overhead of the design.

Thus the run-time monitoring approach of the Trojan detection will check the design periodically with the parameters of the golden chip as a reference circuit. But to obtain a Trojan-free golden chip, the literature suggests reverse-engineering (RE)-based destructive approaches. This is to make sure that the chip is entirely Trojan-free, so that the side-channel parameters extracted from it can be referred to test ICs of the same family.

### *2.1.3 Test-time Approaches*

The test-time approaches are post-manufacturing approaches most widely used in the literature to detect malicious circuits in addition to the common IC tests. They include two types of testing, 1) functional testing and 2) side-channel fingerprinting.

#### *2.1.3.1 Functional Testing*

The Trojans which change the functionality of ICs are detected by logical verification approaches also known as functional testing approaches. In this test-time approach, a set of input vectors is applied to CUT and their corresponding outputs are examined. If the output obtained differs from the expected one, then the presence of Trojan is proven. But mostly Trojans will not alter the functionality of the design, as they are stealthy until triggered. The disadvantage of the functional testing is that the most complex circuits have hundreds of I/Os and testing all combinations of the input patterns is not possible. Schemes of the functional testing are discussed in literatures [9] & [16].

Chakraborty et al. [9] presented an ATPG scheme called MERO (Multiple Excitation of Rare Occurrence) in which rare nodes are activated simultaneously. The threshold of each node is measured and the node which has a rare value of the threshold is selected and activated. Thus the probability of the Trojans getting triggered is maximized and the Trojans are detected easily by logical testing. This method has effectively increased the sensitivity of the side-channel methods of the Trojan detection by monitoring the Trojan impact on the current or power signature. However, the test vectors generated are only to activate the triggering conditions and ignore to notice that the triggered Trojan has changed the functionality of the primary output.

Wang et al. modified the standard ATPG as a Trojan-detection approach [16]. A digital stimulus is applied to the chips and their corresponding outputs are monitored. This method detects the parametric Trojans injected to the existing logic of the chip by changing the design rules. Saha et al. [21] improved the ATPG technique of the Trojan detection by using a genetic algorithm and Boolean satisfiability problem. The payload nodes are triggered by the proposed fault-simulation-based framework, then a set of test vectors is applied to the triggered payload. This increases the ability to detect a malicious behaviour at the rare logic nodes of the circuit. The authors claim that their method achieves a higher detection coverage of HTH than the previously proposed ATPG-based Trojan-detection techniques.

#### *2.1.3.2 Side-channel Fingerprinting*

Side-channel-analysis (SCA) is another approach widely used to detect HTs [28]. The presence of a Trojan may affect the design characteristics like performance degradation, power characteristic variations or reliability reduction of the chip. This will affect either the power or the delay characteristics of each gate and wire in the infected chip. The power-based side-channel signal analysis will detect stealthy Trojans by providing visibility of the activities of the ICs internal structure. Even small changes in the circuit are sensitively detected by delay tests. So the presence of a Trojan along the affected path will be detected by the timing-based SCA technique. This approach will effectively differentiate the effect of Trojans from process variations. The SC measurement of an infected chip is compared with the golden-circuit (HT-free

circuit) and their difference guarantees the presence of a Trojan. Many different SCA-based Trojan-detection methods are discussed in literature [22-25].

Hardware-Trojan detection using a side-channel parametric information was discussed by Agrawal et al. in [22]. Random test patterns are given as an input to CUT and their corresponding power measurements are obtained as the power signature of golden IC (Trojan-free IC). The measured data includes the circuit power consumption and noise and process variations. A set of input patterns is given to a small number of ICs and they are reverse-engineered to assure that they are Trojan-free. Thus the reference signature is obtained from the golden-chip for a certain pair of the input patterns. Then a power measurement for IC under authentication (IUA) is carried out for the same input patterns. If the power signature of IUA differs from the power signature of the reference IC, then the presence of a Trojan in IUA is confirmed. However, if the Trojans are small in size, the process variation will mask their effect and they may not be detected by the power-signature-based SCA.

Alkabani et al. [25] proposed a non-destructive measurement of the IC quiescent current with a metric called consistency. Systems of equations are formed from measured parameters at the gate-level and they are mapped to each other. Thus the authors look for patterns of convergence to develop the Trojan detection with a gate-level estimation and consistency checking in the signal integrity identifies the location of a Trojan in the design. However, the gate leakage current due to Trojan might be masked by the effect of the noise and process variation. In [10], Potkonjak et al. utilize a linear formulation of a gate-level characterization (GLC) to detect Trojans. Timing and static-power analyses are carried out and their measurements are converted into equations using linear programming (LP) and singular-value decomposition. Then the highest rank is obtained from the LP matrix and the gates which are inconsistenct with their original characteristics are detected. The Trojan-free circuit characteristic needs to be studied and tested several times. This approach of gate-level characterization will provide a high controllability among the gates and hence static-power measurements and IDDQ testing have a high accuracy. Karunakaran et al. [26] proposed detection of combinational Trojans using GLC based on leakage-power measurements. The power consumed by the Trojans when they are triggered is measured for each gate and the leakage-power equations obtained are solved using an LP solver. This method of Trojan detection requires a golden-chip as a reference.

Maneesh et al. [27] measured the power signature of the circuit under test (CUT) at different time windows for the applied set of input vectors. A Trojan is detected if there exists some inconsistency in the measured power signature. It is a golden-chip-free, self-referencing approach by measuring the power signature at different time intervals. This overcomes the effect of process variation, during side-channel fingerprinting of Trojan detection and diagnosis approach.

Li et al. proposed a delay-based analysis for the Trojan detection using a physical unclonable function (PUF) [28]. Register-to-register path delays are measured with the help of sweeping-clock-delay measurements. When the path delays extend beyond the threshold level of the process variation, Trojans are detected. However, the effect of the temperature may cause a path delay and this effect might be detected as a Trojan. The authors introduced an on-time temperature monitoring with a ring oscillator to overcome this problem. The operating temperature is measured by a ring oscillator, as its switching frequency is temperature-dependent and the effective response is calculated from the observed temperature and the delay signature. This is an effective Trojan-detection method even though there is an area constraint while embedding the ring oscillator.

Jin et al. [29] proposed a fingerprint-based path-delay analysis of the chip. A chip may contain different path delays and each path delay may represent one of the characteristics of the entire chip. Path-delay fingerprints are generated as a result of timing measurements. Even the smallest Trojans are detected in the path view. The entire process is as follows:

1. The path-delay information of the sample chips is collected by applying a high-coverage input pattern. These sample chips are reverse-engineered to ensure that they are Trojan-free.
2. The fingerprints are generated from the path-delay measurements and they are mapped to a lower-dimension space.
3. The same test patterns are applied to all other fabricated chips and their path-delays information are compared to the Trojan-free samples fingerprints.

In this method, the process variation is analyzed statistically, so that the presence of a small Trojan can be detected beyond the threshold level of the process variation. But analyzing all paths is not practically possible, since large circuits include millions of paths [22].

Thus the side-channel fingerprinting schemes will detect the hardware Trojans effectively even when they are stealthy. However, sometimes the effect of the noise and process variation will have its impact on the measured side-channel parameters, these may be incorrectly detected as a Trojan by the SCA techniques.

#### *2.1.3.3 Triggering the Trojan Activation*

The Trojan activations are triggered by the applied test vectors during the test-time. The idea is when a stealthy Trojan is triggered it consumes a more dynamic power and this helps to identify the presence of Trojan. The region-free Trojan activation and region-aware Trojan activation are the existing approaches in the Trojan

detection. These methods do not completely rely on the regions but they activate the Trojan by triggering.

Jha et al. [30] discussed the randomization-based probabilistic Trojan-detection approach. A unique probabilistic signature is constructed by applying an input pattern based on the specific probability of each circuit. The authors applied the input patterns to IC under authentication (IUA) and their outputs are compared with a genuine-circuits output. The difference in the outputs will indicate the presence of a Trojan. Only by applying the patterns based on the specific probability in a manufactured IC, the Trojan detection is possible. Banga et al. [23] proposed a two-stage test-generation approach that magnifies the power-waveform difference between a genuine design and IUA. In the first step, i.e. *circuit partitioning*, the entire circuit is partitioned into smaller circuits called regions. The Trojans are detected by increasing the in-region switching activity, other than the out-region switching activity. Based on the structural connectivity, the flip-flops are classified into groups. The function of the switching activity is calculated by:

$$F = \max (in_{\text{region-activity}} - out_{\text{region-activity}}) \qquad (1)$$

Activity magnification is the second step in which the test pattern that magnifies the activity of the specific regions is selected as an input vector. It magnifies the distinction between the genuine and the Trojan-infected chips. Thus the difference in the switching activities will expose the presence of Trojan. The main drawback in the region-based approach is that it will detect a Trojan only if the value of F is above the process variation.

Banga et al. [8] magnified the Trojan activation by toggle minimization. This is achieved by applying the same input patterns for different clock cycles. The state elements determine the circuit activity of the design, whereas, the overall switching activity is minimized and the Trojan location is specified at those regions. The differential-power profile plot information is used to locate the Trojan-infected region. The vector pairs which produce a high differential power are considered as starting points. Each time, a vector pair toggles the gate that shows the differential power greater than the differential-power threshold. The Trojan-count and non-Trojan count are analysed for each gate and the ratio of the Trojan-count and non-Trojan count gives the gate weight. A huge value of the gate weight indicates the presence of a Trojan in the circuit. Thus the high-activity, medium-activity and low-activity Trojans are detected by this method. Since the type of the Trojan is unknown, both the region-free and region-aware approach are required to detect the Trojan. If the Trojan circuit gets the input from any part of the circuit, then the region-aware method will detect the Trojan effectively. If the Trojan circuits are triggered randomly, then the probability of the Trojan detection will be increased by the region-free method.

Du et al. [31] introduced a self-referencing approach with a vector-generating algorithm to make the detection independent. The transient-current signature of one region is compared with that of the other region. The effect of the process noise is nullified by utilizing a correlation in the process variation between the regions. The Trojan effect on the supply current is maximized by the proposed region-based vector-generation method, in which CUT is divided into sub-segments called regions. The authors select the input patterns that maximize the activity of the in-region other than of other regions. Thus the proposed method is scalable to both the design size and process variation.

In [32], Narasimhan et al. discussed a self-referencing approach in which the current signatures measured at different time windows are compared to eliminate the noise due to process variation. This method provides a high-sensitivity Trojan detection without referring to any golden-chip instances. The authors measure temporal variations in the transient-current signature of Trojans to segregate the Trojan effect from the noise and process variation.

However, these test-time approaches will detect the Trojans triggered during testing and they fail to detect the Trojans activated due to aging of IC.

### *2.2 Destructive Approaches*

Verifying the chip design by an optical method is carried out by analyzing the chip layer by layer. Thus the chip is destroyed while examining each layer and each chip is to be tested individually. A practical limitation of this analysis is the cost and requirement of a specialized equipment. Hence the destructive approach of HT detection may be applied to those ICs to confirm the presence of suspicious Trojans or the designer doubts the foundry is untrusted.

Reverse-engineering is a process where an IC is tampered layer by layer and internal structures, connections, etc., are analyzed in order to assure that the design is Trojan-free. The cost and skill required for reverse-engineering are high and it is not easy to test all ICs, since once the ICs are reverse-engineered, they cannot be used again. Bao et al. in [37] proposed the Trojan detection by the RE approach. They used a K-means clustering technique to distinguish a suspicious structure in the ICs. The authors experimentally compared the simulation results of the SVM-based approach and K-means clustering approaches and the results are discussed. The main advantage of RE-based Trojan-detection approach using K-means clustering is that it does not require any golden chip as a reference and it is efficient in the storage space. Unfortunately, the chip tested under RE may not be used further even if it is Trojan-free. Table 1 describes the summary of Trojan detection schemes in literature.

Table 1. Summary of the Trojan detection schemes

| Paper | Test Modality | Trojan Type | Detection Method | Referring to Golden-chip | Benchmarks used |
|---|---|---|---|---|---|
| Wolff et al. [5] (2008) | Functional | 2-input gates activated by Trojans | Frequency analysis for rate triggers | Yes | ISCAS'85 |
| R.S. Chakraborty et al. [9] (2009) | Functional | Combinational Trojan : 2 input xor gate sequential Trojan: Counter: 3-bit | Statistical approach | Yes | ISCAS'85 and ISCAS'89 |
| Potkonjak et al. [10] (2009) | Static power and Delay (GLC) | 1 gate | Static power and circuit switching activity | Yes | ISCAS'85 |
| S. Saha et al. [21] (2015) | Genetic Algorithm (GA) based Automatic Test Pattern Generation (ATPG) | Combinational Trojan : 2 input xor gate sequential Trojan: Counter: 3-bit | Boolean satisfiability | Yes | ISCAS'85 & ISCAS'89 |
| Agrawal et al. [22] (2007) | Transient Power | Counter : 16- bit Comparators: 3, 8-bit | Kullback-Leibler (KL) distance | Yes | 256-bit Rivest, shamir, and Adleman (rsa) |
| P.K. Maneesh et al. [27] (2015) | Gate Level Characterization (GLC) | Combinational Trojan | Self-referencing power signature analysis | No | ISCAS'85 |
| Jin et al. [29] (2008) | Delay | Comparators: 2, 4-bit | Path-delay analysis | Yes | Data Encryption Standard (DES) core |
| Narasimhan et al. [32] (2011) | Current-signature Analysis | Sequential Trojan: Counter: 3-bit | Side-channel signature analysis | No | AES cipher circuit, 32-bit pipelined IEU and 32-bit DLX processor |
| S. Jha et al. [30] (2008) | Functional | Extra logic randomly added | Probabilistic signature of a Boolean circuit | Yes | ISCAS'85 |
| Du et al. [31] (2010) | Transient Current | Combinational Trojan : 2 input xor gate and 2 input xnor gate | Maximizing the region activity | Yes | 32-bit DLX processor core |
| Bao et al. [37] (2016) | Reverse Engineering | Parametric Trojans | K-means clustering approach | No | ISCAS'89 and ITC benchmarks |

## 3 DESIGN-FOR-SECURITY (DFS)

The DFS approaches increase the observability and controllability of rare nodes in ICs, such that the rare triggering conditions of a malicious circuit are altered. The vulnerabilities in the VLSI design can be prevented by techniques like logic encryption, IC camouflaging, split manufacturing and Trojan activation. These DFS techniques are arbitrarily applied to the design structure to provide the required security level. Classification of the DFS schemes is shown in Fig. 3.

### *3.1 Logic Encryption*

Chakraborty et al. [38] proposed a HARdware Protection through Obfuscation of the Net list (HARPOON), i.e. an SoC design methodology to improve the Obfuscation technique. In this method, the hardware IPs are protected by obfuscation of the netlist followed by its authentication process. The circuit undergoes the normal mode of operation only upon applying a valid key at the primary inputs. A maximal obfuscation at a minimal design overhead is achieved by a theoretical analysis of the level of obfuscation. From the proposed obfuscation technique, the design flow for SoCs with a gate-level security is obtained. However, the proposed obfuscation scheme has the design area overhead under a delay constraint.

J.V.Rajendran et al. [40] addressed the obfuscation techniques at the gate-level of the design flow. In their proposed method, the obfuscation technique is made stronger by increasing the number of the key gates (key size) to deceive the adversary. The key gates are inserted randomly to the original design, such that the

keys are concurrently mutable. Hence, the attacker can easily decipher the obfuscation netlist with the number of keys and sensitize the key values at the output. To make it harder, the defender inserts the key gates by using an interference graph, by maximizing the number of the non-mutable edges in the graph. In this proposed technique, for the large size keys (key size> 100) the attacker may take several years to determine the key value. These techniques protect the functionality of IC from a reverse-engineering threat. However, an attacker with an expertise in the IC testing techniques will easily subvert the logic obfuscation technique and insert a malicious circuit to the design.

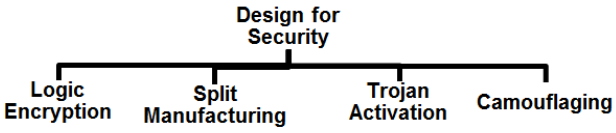


Figure 3. Design for security schemes classification

J. A. Roy et al. [41] considered the IC piracy in the defense industry as a major challenge and proposed a public-key-cryptography (PKC)-based logic-encryption technique in order to elevate a combinational chip-locking system and a protocol to activate the chip. However, in this method, each chip of the same wafer will have its own locking keys, thus increasing the design complexity.

S. Dupuis et al. [42] proposed a hardware logic-encryption technique by reducing the number of the rare logic values in the circuit to protect IC from illegal overproduction and hardware Trojan insertion. The number of the low-controllable nodes is minimized without changing the functionality of the design. Accordingly, unauthorized overproduction is prevented but the proposed technique will incur an area and delay overhead.

### *3.2 Split Manufacturing*

Jarvis [43] proposed split manufacturing, so that an adversary in the foundry will be discomfit to access the entire chip design. In this technique, the entire layout of the chip is split-off in two types of layers: the front-end-of-line (FEOL) layers (they include transistors and lower metal layers) and the back-end-of-line (BEOL) layers (they include higher metal layers). These two types of layers are fabricated in two different foundries by hiding each other. At postfabrication, the two split-off wafers are aligned, unified and tested. Since the adversary in the foundry may not get the complete details of the split design, inserting a hardware Trojan is not possible. However, the attacker in FEOL may bypass the security of split manufacturing by exploiting the heuristics used in physical design tools like floor planning, placement and routing tools.

J.V.Rajendran et al. [44] developed a fault-analysis-based protection against the FEOL attacks in split manufacturing. The authors introduced the IC testing principles like fault excitation, fault propagation and fault masking to improve the security of split manufacturing by using swapping partition pins at the FEOL layers. However, the authors swapped only a small set of pins to achieve a 50% metric of the Hamming distance, since the pin-swapping technique will increase the wire-length and noise and reduce the signal integrity of the design. Thus the split-manufacturing techniques enhance the security level of the design to some extent.

### *3.3 Trojan Activation*

The dormant Trojans are to be activated by an external trigger and this can be achieved by increasing the switching activity within the circuit. The authors added some module to the original design to increase the Trojan activation [20], [47]. Salmani et al. [6], [20] introduced a dummy-scanned flip-flop at rare triggering nodes, aiming at decreasing the transition time. This approach increases the nets transition probability beyond the threshold. Thus the Trojan detection is improved by reducing the Trojan-activation time. J.V.Rajendran et al. [47] reconfigured the circuit paths into ring oscillators (Ros) by adding some extra logic to the circuit. Then the frequency of Ros is monitored. Any change in the frequency of Ros will be detected as a Trojan. Thus the Trojans are activated by additional design modules to enhance the detection process. However, the frequency of RO may vary due to the temperature and this variation may be wrongly detected as a Trojan sometime. These methods of DFS support the test-time Trojan-detection approaches to detect Trojans easily, either by triggering the rare nodes or by increasing the Trojan-activation time.

### *3.4 Camouflaging*

Camouflaging is a layout-level technique in which an adversary is obstructed from extracting an original gate-level netlist by imaging different layers. In [45], dummy contacts are added to the original design irrespective of their functionality enabling the adversary to extract a netlist with dummy contacts that differ from the original netlist. Reverse-engineering-based attacks are prevented by this approach since the functionality of the camouflaged gates will not be retrieved by the attacker. J.V.Rajendran et al. [46] selected the camouflaged gates such that the functionality of the extracted netlist is completely different from the original netlist. The authors evaluated the defense technique on an Open-sparc T1 microprocessor and found that reverse engineering becomes more complicated for the camouflaged designs.

3.5 **Table 2. A list of security schemes design**

| DFS Schemes | Paper | Methodology | Protection against | Benchmarks used |
|---|---|---|---|---|
| ***Obfuscation*** | R.S.Chakraborty et al. [38] (2009) | Inserting a simple finite-state machine | Hardware IP protection | ISCAS'89 |
| | R.S.Chakraborty et al. [39] (2009) | Modifying the state-transition function | Hardware IP protection | ISCAS'89 |
| | J.V.Rajendran et al. [40] (2012) | Inserting key gates | Reverse-engineering, overbuilt ICs, HT | ISCAS'85 |
| ***Logic Encryption*** | J. A. Roy et al. [41] (2008) | Randomly inserting XOR gates | IP piracy | ISCAS'85 |
| | S.Dupuis et al. [42] (2014) | Adding an external key | Illegal overproduction | 128 bits AES Cipher |
| ***Split Manufacturing*** | Jarvis et al. [43] (2007) | The entire layout of the chip is split into two layers | Reverse-engineering, illegal overproduction | All Semiconductor die |
| | J.V.Rajendran et al. [44] (2013) | Fault-analysis-based protection | FEOL attacks | ISCAS'85 |
| ***Trojan Activation*** | Salmani et al. [20] (2012) | Dummy-scanned flip-flops insertion | To generate transition in functional Trojans | ISCAS'89 |
| | J.V.Rajendran et al. [47] (2011) | The circuit path is reconfigured into ring oscillators | Stealthy Trojans | ISCAS'85 |
| ***Camouflaging*** | Chow et al. [45] (2007) | Adding dummy contacts | Reverse-engineering | All Semiconductor ICs |
| | J.V.Rajendran et al. [46] (2013) | Functionality of camouflaged gates | Reverse-engineering | Open-sparc T1 microprocessor |

However, the area, power and delay overhead due to the camouflaged standard cell is more than 5% of a normal standard cell due to the unused transistors of the dummy contacts. Table 2 shows a list of security-schemes designs in literature.

## 4 CONCLUSIONS

A survey is given of the hardware-security research including design-for-security. The non-destructive approaches like the design-time approach, test-time approach and run-time approach are most widely used as the chip tested destructively may not be used even if it is Trojan-free. Among the non-destructive approaches, the test-time approach is more resilient as the other two approaches will have an area overhead by the added extra logic. If the attacker tampers a Trojan in the added Trojan-detection module, then the design-time and run-time approaches will provide a false positive result. Hence, to increase the trustworthiness of the end users, the design should carry a proof throughout the design flow and check the design at every stage of the design flow. The run-time approach of the Trojan detection is required to provide a trustworthy design to the end user and the designer. The survey shows the direction to enhance the security level of the hardware with fundamental solutions against the hardware threats.

## Acknowledgement

This work is funded by the Defence Research and Development Organization (DRDO), New Delhi, "ERIP/ER/1503187/M/01/1582".

## References

[1] U. O. Defense, "Defense science board task force on high performance microchip supply," Washington, DC, pp. 2005–02, 2005.

[2] L. L. Harada, "Semiconductor technology and us national security," DTIC Document, Tech. Rep., 2010.

[3] Preneel, Bart, and Tsuyoshi Takagi, eds. *Cryptographic Hardware and Embedded Systems--CHES 2011: 13th International Workshop, Nara, Japan, September 28--October 1, 2011, Proceedings*. Vol. 6917. Springer, 2011.

[4] Chakraborty, Rajat Subhra, Seetharam Narasimhan, and Swarup Bhunia. "Hardware Trojan: Threats and emerging solutions." In *High Level Design Validation and Test Workshop, 2009. HLDVT 2009. IEEE International*, pp. 166-171. IEEE, 2009.

[5] Wolff, Francis, Chris Papachristou, Swarup Bhunia, and Rajat S. Chakraborty. "Towards Trojan-free trusted ICs: Problem analysis and detection scheme." In *Proceedings of the conference on Design, automation and test in Europe*, pp. 1362-1365. ACM, 2008.

[6] Salmani, Hassan, Mohammad Tehranipoor, and Jim 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*, pp. 66-73. IEEE, 2009.

[7] Bhunia, Swarup, Miron Abramovici, Dakshi Agrawal, Paul Bradley, Michael S. Hsiao, Jim Plusquellic, and Mohammad

Tehranipoor. "Protection Against Hardware Trojan Attacks: Towards a Comprehensive Solution." *IEEE Design & Test* 30, no. 3 (2013): 6-17.

[8] Banga, Mainak, and Michael S. Hsiao. "A novel sustained vector technique for the detection of hardware Trojans." In *2009 22nd International Conference on VLSI Design*, pp. 327-332. IEEE, 2009.

[9] Chakraborty, Rajat Subhra, Francis Wolff, Somnath Paul, Christos Papachristou, and Swarup Bhunia. "MERO: A statistical approach for hardware Trojan detection." In *Cryptographic Hardware and Embedded Systems-CHES 2009*, pp. 396-410. Springer Berlin Heidelberg, 2009.

[10] Potkonjak, Miodrag, Ani Nahapetian, Michael Nelson, and Tammara Massey. "Hardware Trojan horse detection using gate-level characterization." In*Design Automation Conference, 2009. DAC'09. 46th ACM/IEEE*, pp. 688-693. IEEE, 2009.

[11] Sinanoglu, Ozgur, Naghmeh Karimi, Jeyavijayan Rajendran, Ramesh Karri, Yier Jin, Ke Huang, and Yiorgos Makris. "Reconciling the IC test and security dichotomy." In *2013 18th IEEE European Test Symposium (ETS)*, pp. 1-6. IEEE, 2013.

[12] Jin, Yier, Nathan Kupp, and Yiorgos Makris. "DFTT: Design for Trojan test." In *Electronics, Circuits, and Systems (ICECS), 2010 17th IEEE International Conference on*, pp. 1168-1171. IEEE, 2010.

[13] Drzevitzky, Stephanie, Uwe Kastens, and Marco Platzner. "Proof-Carrying Hardware: Towards Runtime Verification of Reconfigurable Modules." In*ReConFig*, pp. 189-194. 2009.

[14] Love, Eric, Yier Jin, and Yiorgos Makris. "Proof-carrying hardware intellectual property: A pathway to trusted module acquisition." *IEEE Transactions on Information Forensics and Security* 7, no. 1 (2012): 25-40.

[15] Jin, Yier, and Yiorgos Makris. "A proof-carrying based framework for trusted microprocessor IP." In *2013 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, pp. 824-829. IEEE, 2013.

[16] Wang, Xiaoxiao, Mohammad Tehranipoor, and Jim Plusquellic. "Detecting malicious inclusions in secure hardware: Challenges and solutions." In*Hardware-Oriented Security and Trust, 2008. HOST 2008. IEEE International Workshop on*, pp. 15-19. IEEE, 2008.

[17] Alkabani, Yousra, and Farinaz Koushanfar. "Designer's hardware Trojan horse." In *Hardware-Oriented Security and Trust, 2008. HOST 2008. IEEE International Workshop On*, pp. 82-83. IEEE, 2008.

[18] Banga, Mainak, and Michael S. Hsiao. "Trusted RTL: Trojan detection methodology in pre-silicon designs." In *Hardware-Oriented Security and Trust (HOST), 2010 IEEE International Symposium on*, pp. 56-59. IEEE, 2010.

[19] Jin, Yier, and Yiorgos Makris. "Proof carrying-based information flow tracking for data secrecy protection and hardware trust." In *2012 IEEE 30th VLSI Test Symposium (VTS)*, pp. 252-257. IEEE, 2012.

[20] Salmani, Hassan, Mohammad Tehranipoor, and Jim Plusquellic. "A novel technique for improving hardware Trojan detection and reducing Trojan activation time." *IEEE Transactions on Very Large*.

[21] Saha, Sayandeep, Rajat Subhra Chakraborty, Srinivasa Shashank Nuthakki, and Debdeep Mukhopadhyay. "Improved test pattern generation for hardware Trojan detection using genetic algorithm and Boolean satisfiability." In *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 577-596. Springer Berlin Heidelberg, 2015.

[22] Agrawal, Dakshi, Selcuk Baktir, Deniz Karakoyunlu, Pankaj Rohatgi, and Berk Sunar. "Trojan detection using IC fingerprinting." In *2007 IEEE Symposium on Security and Privacy (SP'07)*, pp. 296-310. IEEE, 2007.

[23] Banga, Mainak, and Michael S. Hsiao. "A region based approach for the identification of hardware Trojans." In *Hardware-Oriented Security and Trust, 2008. HOST 2008. IEEE International Workshop on*, pp. 40-47. IEEE, 2008.

[24] Narasimhan, Seetharam, Rajat Subhra Chakraborty, Dongdong Du, Somnath Paul, Francis G. Wolff, Christos A. Papachristou, Kaushik Roy, and Swarup Bhunia. "Multiple-Parameter Side-Channel Analysis: A Non-invasive Hardware Trojan Detection Approach." In *HOST*, pp. 13-18. 2010.

[25] Alkabani, Yousra, and Farinaz Koushanfar. "Consistency-based characterization for IC Trojan detection." In *Proceedings of the 2009 International Conference on Computer-Aided Design*, pp. 123-127. ACM, 2009.

[26] Karunakaran, Dinesh Kumar, and N. Mohankumar. "Malicious combinational hardware Trojan detection by gate level characterization in 90nm technology." In *Computing, Communication and Networking Technologies (ICCCNT), 2014 International Conference on*, pp. 1-7. IEEE, 2014.

[27] Maneesh, P. K., and M. Nirmala Devi. "Power based Self-Referencing Scheme for Hardware Trojan Detection and Diagnosis." *Indian Journal of Science and Technology* 8, no. 24 (2015): 1.

[28] Li, Jie, and John 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*, pp. 8-14. IEEE, 2008.

[29] Jin, Yier, and Yiorgos Makris. "Hardware Trojan detection using path delay fingerprint." In *Hardware-Oriented Security and Trust, 2008. HOST 2008. IEEE International Workshop on*, pp. 51-57. IEEE, 2008.

[30] Jha, Susmit, and Sumit Kumar Jha. "Randomization based probabilistic approach to detect Trojan circuits." In *High Assurance Systems Engineering Symposium, 2008. HASE 2008. 11th IEEE*, pp. 117-124. IEEE, 2008.

[31] Du, Dongdong, Seetharam Narasimhan, Rajat Subhra Chakraborty, and Swarup Bhunia. "Self-referencing: a scalable side-channel approach for hardware Trojan detection." In *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 173-187. Springer Berlin Heidelberg, 2010.

[32] Narasimhan, Seetharam, Xinmu Wang, Dongdong Du, Rajat Subhra Chakraborty, and Swarup Bhunia. "TeSR: A robust temporal self-referencing approach for hardware Trojan detection." In *Hardware-Oriented Security and Trust (HOST), 2011 IEEE International Symposium on*, pp. 71-74. IEEE, 2011.

[33] Bloom, Gedare, Bhagirath Narahari, and Rahul Simha. "OS support for detecting Trojan circuit attacks." In *Hardware-Oriented Security and Trust, 2009. HOST'09. IEEE International Workshop on*, pp. 100-103. IEEE, 2009.

[34] Hicks, Matthew, Murph Finnicum, Samuel T. King, Milo MK Martin, and Jonathan M. Smith. "Overcoming an Untrusted Computing Base: Detecting and Removing Malicious Hardware Automatically." In *IEEE Symposium on Security and Privacy*, pp. 159-172. 2010.

[35] Bao, Chongxi, Domenic Forte, and Ankur Srivastava. "Temperature tracking: toward robust run-time detection of hardware Trojans." *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 34, no. 10 (2015): 1577-1585.

[36] Kim, Lok-Won, and John D. Villasenor. "Dynamic Function Verification for System on Chip Security against Hardware-Based Attacks." *IEEE Transactions on Reliability* 64, no. 4 (2015): 1229-1242.

[37] Bao, Chongxi, Domenic Forte, and Ankur Srivastava. "On reverse engineering-based hardware Trojan detection." *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 35, no. 1 (2016): 49-57.

[38] Chakraborty, Rajat Subhra, and Swarup Bhunia. "HARPOON: an obfuscation-based SoC design methodology for hardware protection." *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*28, no. 10 (2009): 1493-1502.

[39] Chakraborty, Rajat Subhra, and Swarup Bhunia. "Security against hardware Trojan through a novel application of design obfuscation." In *Proceedings of the 2009 International Conference on Computer-Aided Design*, pp. 113-116. ACM, 2009.

[40] Rajendran, Jeyavijayan, Youngok Pino, Ozgur Sinanoglu, and Ramesh Karri. "Security analysis of logic obfuscation." In *Proceedings of the 49th Annual Design Automation Conference*, pp. 83-89. ACM, 2012.

[41] Roy, Jarrod A., Farinaz Koushanfar, and Igor L. Markov. "EPIC: Ending piracy of integrated circuits." In *Proceedings of the conference on Design, automation and test in Europe*, pp. 1069-1074. ACM, 2008.

[42] Dupuis, Sophie, Papa-Sidi Ba, Giorgio Di Natale, Marie-Lise Flottes, and Bruno Rouzeyre. "A novel hardware logic encryption technique for thwarting illegal overproduction and Hardware Trojans." In *2014 IEEE 20th International On-Line Testing Symposium (IOLTS)*, pp. 49-54. IEEE, 2014.

[43] Jarvis, Richard Wayne, and Michael G. McIntyre. "Split manufacturing method for advanced semiconductor circuits." U.S. Patent 7,195,931, issued March 27, 2007.

[44] Rajendran, Jeyavijayan JV, Ozgur Sinanoglu, and Ramesh Karri. "Is split manufacturing secure?." In *Proceedings of the Conference on Design, Automation and Test in Europe*, pp. 1259-1264. EDA Consortium, 2013.

[45] Chow, Lap-Wai, James P. Baukus, and William M. Clark Jr. "Integrated circuits protected against reverse engineering and method for fabricating the same using an apparent metal contact line terminating on field oxide," U.S. Patent 7,294,935, Nov.13, 2007.

[46] Rajendran, Jeyavijayan, Michael Sam, Ozgur Sinanoglu, and Ramesh Karri. "Security analysis of integrated circuit camouflaging." In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pp. 709-720. ACM, 2013.

[47] Rajendran, Jeyavijayan, Vinayaka Jyothi, Ozgur Sinanoglu, and Ramesh Karri. "Design and analysis of ring oscillator based Design-for-Trust technique." In *29th VLSI Test Symposium*, pp. 105-110.

**Sree Ranjani Rajendran** is currently pursuing her Ph.D. in the Department of Electronics & Communication Engineering, Amrita School of Engineering, Ettimadai, India and is working on a project sponsored by Defense Research & Development Organization (DRDO), Delhi, India. Her research interests include hardware Trojan detection and diagnosis in integrated circuits and trusted hardware design. She received her M.E degree in VLSI Design from Anna University, Chennai. She is a student member of IEEE.

**Nirmala Devi M** is a professor in the department of Electronics and Communication Engineering at Amrita Vishwa Vidyapeetham, Coimbatore, India. Her research interests include VLSI Design and Testing, Computational Intelligence, Hardware Security and Trust, Evolvable Hardware and RF CMOS System Design. She has published some 55 papers in the International Journals and Conferences in her field of expertise. She has served as a reviewer for refereed international conferences and international journals which include the following; Springer Journal of the Institution of Engineers (India): Series B, Inderscience Int. Journal of Information and Communication Technology. She is the recipient of the following awards: Marquis Who's Who in the World - 2011 and 2000 Outstanding Intellectuals of the 21st Century - 2011 - International Biographical Center, Cambridge, U.K. She has received a financial grant for the research proposal from the Defence Research & Development Organization, Delhi, India.