Reduction Of Hardware Trojan Effect Using
Multipath Authentication

P. Bosebabu, K. Siva Nagaraju, B. Chanikya, P. Ritish Kumar

Abstract: with increase of Integrated Circuit (IC) manufacturing foundries and fabrication units, security of an IC gains its importance. The manufacturing of IC is having many stages like designing, assembling, packaging, etc. Hardware Trojans can be implantable at any of these stages by the foundries or third-party vendors. Hardware Trojan is a malicious, undesired, intentional, modification of an electronic circuit or design, resulting leakage of data or incorrect behaviour of an electronic device. The Cryptographic algorithms play an important role in information security and protection of data from unauthorised usage. The proposed AES crypto processor model is having a authentication monitoring which will detect hardware Trojan triggering, alerts the user and takes necessary actions for retrieving original data. With help of proposed system, the reduction of effect of hardware Trojan can be achievable.

Keywords: Hardware Trojan, Cryptography, IC security, AES.

1. INTRODUCTION

In recent years, the usage of semiconductor devices has rapidly increased. Integrated Circuit (IC) has become the foremost part of every stream like military, government, commercialization, etc. Chip manufacturing cycle involves Specification, Architectural design, Functional and Logical design, Circuit design, Physical design, Fabrication, Packaging and Testing. Due to long supply chain, the manufacturing of an IC at one place was difficult and demands a large capital investment. So, fabrication of an IC is done at different places and monitoring such long process, the products are likely to be modified or inserted a malicious circuit into the design by the attackers [1-3]. Hardware Trojans [HTs] are malicious modification or insertion of harmful circuit into existing design. HTs can be implanted in security weaker parts of IC to disturb the original functionality of the circuit. Hardware Trojans can leak the secure information (Data leaks) or disturb the regular flow of the circuit (behaviour modifiers) or destroy the device or system’s hardware or degrade the operation (reliability Impacts) [5]. HTs are small in size and activated by rare events. As the foot print for a Trojan may be very small, it becomes hard to verify or test for Trojan in circuit. Especially when there is no Trojan free reference available to compare against. Several methods are proposed to detect HTs, still it become an issue in IC security. Cryptography is used for protect data from attempt theft, theft or unauthorised use of data. Cryptographic chips are used for protecting Military secrets, Business Data, and other high security fields, requires most secured chips [4]. Therefore, in this paper, the proposed AES Crypto processor circuit having an authentication of data to detect HTs and takes corrective action against Trojans. The rest of the paper is organized as follows. The section II deals with survey of Hardware trojans, Detection methods, prevention technics, and AES Crypto processor. In section III, the paper deals with our proposed model. In section IV, results are analysed in detail. Finally, conclusion and future scope of the work.

2. RELATED WORK

A. Hardware Trojan

Hardware Trojan consist of two parts, trigger and payload. Trigger is an activation condition or event that triggers the payload in active state. Payload is an activity that executed whenever Trojan is activated or triggered. There are two types of HTs, one is always-on and another one is condition based [8]. Trojans are activated internally or externally. For internally activation of trigger, it observes the certain sequence of signals to occur and satisfied the triggering condition and the other possibility is Trojan activated after every particular time interval by a counter logic. Externally activated trigger takes activation signals from the outside of the IC [2].

The HTs are also classified in another way based on triggering are:

1. Analog Trojans
2. Digital Trojans

The Analog Trojans are activated by on-chip sensors using physical parameters like temperature, delay or device aging effect. Analog Trojans also activated by the incoming voltages to the Chip. Digital Trojans are triggered by some Boolean functions and edge signals from clock or internal signals. In terms of payload the Trojans are classified as Analog, Digital and Other. Analog payloads disturb the circuit in terms of power and delay concerns. Digital payloads can perform unwanted function or introduce some memory content, i.e., data modification. Other type of payloads are the side-channel attack which leak the information through thermal radiation or serial data port interface and the another one is denial-of-service attack which causes circuit function is unavailable.[3][12][13].

B. Trojan Detection Methods

Several Hardware Trojan detection methods are proposed and some are discussed here. Reverse Engineering of an IC is destructive method used for Trojan detection by performing depackage, delayering, imaging of each layer of the circuit to get circuit information and analyse that information for identification of Hardware Trojans in the chip. [4][10]. For more complex designs it takes more time and cost effective, so it is not an effective and advisable method.[9]. Built-in self-test (BIST), method provides on chip test pattern generators and response analysers. The testing of chip is performed by itself.
By using BIST method detection of Trojans which are activated by large rare conditions is difficult, test pattern generators generates only small set of test patterns [2]. Several types of methods to detect HTs are proposed based on Golden IC model. Golden IC model is an IC or simulation model for design without having any Trojans, it taken as ideal reference for comparison with circuits under test. Some methods based on golden model are proposed requiring only golden circuits, golden net list results etc. Scanned based method, scan the target design for number of gates, design structure, block areas and compare with Trojan free design parameters for Trojan detection. As the Trojans with smaller sizes are cause very little changes in gates, area so it is difficult to HTs in scan tests using conventional methods [8]. Logical testing method is low cost detection technic for Trojan detection. In this method, a set of testing vectors are given as input to a circuit, the produced outputs are compared with the estimated output values for Trojan detection. The random test signals are generated using Automatic Test Pattern Generators (ATPG). This is best suited for smaller circuits and it cannot be applicable for complex designs with more I/O. An optimal expand algorithm was proposed to effectively detect the HTs by generating test patterns to trigger the HTs [4]. Similarly, Hardware Trojan Catcher (HaTCh) algorithm was proposed for HTs detection by Syed kamran haider [18].

Insertion of Hardware Trojans in the design cause changes in physical properties of the design like current (both static and transient), power consumption, path delay and electromagnetic field characteristics. Analysis of these parameters for Trojan Identification using Golden IC is known as Side Channel Analysis. Hardware Trojans implanted in the design causes extra leakage currents. The impact of Trojan on leakage current is small and difficult to analysis. The entire design is partitioned into smaller regions and analysed, the leakage current variations for Trojans detection [12]. Distance discrimination method is proposed for HTs detection by observing power consumption. In this method the Trojan circuit power and Trojan free circuit power was compared with distance between the two values for the detection of Hardware Trojan. Euclidean Distance and Mahalanobis Distance discriminations are discussed in [8] for detection of Hardware Trojan. Euclidean distance method is effectively detects Trojan than the Mahalanobis Distance discrimination method. In path delay analysis timing parameters of the circuit is observed for Trojan detection. Each component in the design introduce some path delay, for larger path delay designs identification of small delay changes added by Trojan is difficult. For effective identification using delay parameter design is verified by segmentation. Hardware Trojans are also detected using IC fingerprint techniques. These techniques uses signal processing techniques like Kerhunen-Loeve expansion for calibration of noise and power trace signals for identification of Trojans. In fingerprinting technology electromagnetic emissions are also monitored for Trojan detection. The EM emissions from with and without Trojan devices are little dissimilar. By using these analysis very small Trojans are also detectable in the size of 0.1% to 0.01% of the total circuit area [6]. Fuqiang Chen and Qiang Liu proposed a method to detect the single triggered Hardware Trojans based on the structural characteristics of the HTs. They extracted several structural templates from the gate-level netlists, they proposed a scoring algorithm to count the number gates in the circuit part and matched with the templates for Trojan detection. [7]. Further the analysis was done on the structural features of the combinational Hardware Trojans and sequential Hardware Trojans. The scoring discrimination algorithm used for effective detection of Trojans with less runtime and low failure rate. [16]. With increase of attacker's ability, there is chance of sudden attacks at run-time. The machine learning techniques are used for detection of real-time attacks or dynamic attacks. The real time online machine learning algorithm is used for protecting many core designs. The algorithm updates the design data after every data transfer using feedback mechanism, different algorithms used for detection, those are Support Vector Machines (SVM), K-Nearest Neighbours (K-NN) and Modified Balanced Window algorithm (MBW) etc., Modified Balanced Window algorithm has higher accuracy for detection compared to SVM and K-NN algorithms. [19]. Hardware Trojans are also detected using Deep learning technique in the gate-level netlists. By observing the controllability and transition probability characteristics of the circuit nodes, which differentiate the healthy node and effected node. The Trojans effected nodes exhibits large inter cluster distance compared to ideal one, with help of this the group of effected nodes and unaffected nodes are identified using k-means clustering [20].

C. Trojan Prevention Methods

After the Trojan detection, necessary actions should be taken for effective use of Trojan effected system. Some Trojan diagnosis methods are proposed for exact identification of Trojans locations and type of the Trojans. The Precautionary methods are used to prevent the effect of Trojan are discussed below. Most of the Trojans are inserted in the empty areas of the designs. The Trojans are in inactive state for all the time, those are activated in rare situations and rest of the time design will work as the user desired. So, in order to prevent the Trojan insertion it is better to reduce the unused area of the chip. For this, some layout filling methods are proposed like Built-in self-Authentication (BISA) techniques are proposed to prevent Trojans insertion. In this method the empty area of the design are filled with dummy logical circuits which will not disturb the main functionality of the circuit. These dummy logical circuits forms a BISA circuit. If any modifications of these logics with Trojans insertion, the BISA circuit will produce an indication signal during authentication of the circuit. [12]. By reduction of the unused pins in the FPGA design was proposed to prevent of Trojans [1]. In this, the unused pins of the board is identified and the pins are connected with dummy functional logics, the information is encrypted by using Advanced Standard Encryption (AES) with 128 bit symmetrical key. So, the information is only accessed by the authorised user only. By using this method the improved throughput and greater security to the system are achievable. Obfuscation methods are proposed for Trojans prevention. Obfuscation means hiding the information of the original design by transformation of the design into another form which is difficult to understand. Logic obfuscation is a transform that modify the original circuit information into new circuit which works as original design and does not reveal any sophisticated information about circuit. In block box obfuscation circuit will gives as obfuscated black box which do not leak any information except input and output signals information of the circuit. In combinational obfuscation method, the design information is hide with randomly inserting gates like XOR, XNOR or multiplexer circuits and this information is hidden in the memory of the device or by using
cryptographic methods. For sequential obfuscation, the design state machines are modifying by adding an additional states and transform into the new state machine. [12]. Chakraborty and Bhunia proposes a method to protect the hardware IP with Netlist obfuscation. In this technique modification of IP core structure and functionality of system by changing gate level netlist and also incorporates authentication features in the design. This method brings the active participation of the different developers of the design cycle. It modifies the gate level netlist of IP core in pre synthesized state and resynthesized for achieving maximum level of obfuscation. Authentication feature insertion of the design will provide security to the design in every design phase against Trojans insertion or any malicious modifications to the circuit design. [17]. Hardware isolation based technique provides secure environment against data leakage Trojans. Hardware isolation is achieved by isolating the secret data area using bus-level hardware isolation techniques provided by secure processors like ARM TrustZone. In this, there are two different memory areas are maintained for normal data and secure data, secrete information is processed and transferred to secure environment. If any attempts made to leak the secure information it will monitor the delay times for data transmission and blocks the secure data leakage. [11]. Alford Crouch, Eve Hunter and Peter L. Levin presented a tool called Trojan Emulation and Exploration Environment. This tool is used for verification and approval of the design. The tool has the data base of the different types of Trojan details, this tool is used in the pre-manufacturing stage as well as post manufacturing stage to provide security for the design before adverse effects occur. [5]. Split manufacturing process is one of the most effective method for the Trojan prevention. In split manufacturing the fabrication steps of the IC is performed at different trusted agencies and combined after checking the individual production house outcomes. In this process front end process steps and back end process steps are separated. The front end process steps are performed by the most trusted agencies and back end process steps are performed by less trusted or general agencies. The interconnection information is not shared for prevention of Trojan insertion. This will take much time to produce final product but provides more trustworthiness on the final product. [9].

D. AES Crypto Processor
The Advanced Encryption Standard (AES) is most popular and used across worldwide as encryption algorithm for data security. AES is a symmetric key algorithm from Rijndael family developed by Vincent Rijmen and Joan Daemen and established by U.S. National Institute of Standards and Technology (NIST) in 2001. Symmetric algorithm means, it uses same key for both encryption and decryption. It is proposed to replace the encryption algorithm Data Encryption Standard (DES), which has small key length and more vulnerable to attacks. AES provides stronger encryption and faster in execution. AES encryption and decryption involves series of interlinked operations for N number of rounds with slight change in last, first round of encryption and decryption respectively. The number of rounds (N) is depends on the key length. AES ciphers uses block size of 128 bits, but three different key lengths: 128, 192 and 256 bits. The number of rounds performed for 128 bit key is 10, for 192 bit key is 12 and for 256 bit key is 14. AES performs all its operations by considering the data as bytes, the data should be arranged in symmetrical matrix form. The encryption and decryption process of the AES is shown as a flow chart in fig.1.

![Flow diagram of AES Crypto Processor: a) Encryption b) Decryption](image)

In encipher the plain text is initially undergone for add round key operation, then N rounds of encryption is performed. Each round comprises four transformations except last round, it has three transformations. The different transformations involved in the encryption process are Sub bytes, Shift rows, Mix columns and Add round key. Mix columns is not there in last round. Sub bytes: In this each byte is substituted with new byte from the fixed table S-box given in design. The S-box values are given by the results of two transformations, a multiplicative inverse of GF (2^8) with irreducible polynomial m(x) and an affine mapping over GF (2). [21]. Shift rows: In this transformation each byte in a row of the matrix shifted left (rotational shift) based on row index. For first row no shift occur, second row one position shifted, third row two positions shifted and so on. Mix columns: This produces new matrix by every column of the matrix. Each column of the matrix is replaced by new column by performing mathematical transformations. This Transformation is not performed in the last round. Add round key: The matrix is considered as 128 bit data and a new 128 bit data is produced by performing bitwise Exclusive-OR (XOR) operation with 128 bit round key. For each round a new round key is generated by key manipulator from the input key. The output of last round is cipher text. In decryption process the same transformations are performed in reverse manner in reverse order to the encryption rounds. The flow graph of the decryption is shown in fig.1.b.

3. PROPOSED MODEL
In proposed model, an authentication system for input data verification was proposed. The proposed model block diagram is shown in fig.2.
In proposed model there are two paths, main path and parallel path. Trojans are inserted in free area (alongside of data path) and are activated in rare conditions based on triggering signal (input data) to modify the data to produce miclenious results. The authentication system comprises of both comparator and switching network. Any modifications happened to the data by the Trojans is observed by the comparator, which compares the main path data with entered input data through the parallel path. The output of the comparator gives as status signal for the intimation of Trojan detection and drives the control input of the switching circuit. The changes of main path data is observed, the comparator generates negative signal to the switch control for data change. The switch circuit terminates main path signals and connects parallel path signals to AES cipher, so the original results are achieved even though Trojan is activated. The proposed model performs both Trojan detection and prevention mechanisms. Our proposed model is designed and simulated using LabVIEW tool. The results are discussed in the upcoming section.

4. RESULTS & DISCUSSION
In this section we present simulation results of our proposed method as set of LabVIEW front panel pictures. In this we compared the results of Trojan free circuit, Trojan effected circuit and our proposed circuit.

The plaintext "loyola college" and 128 bit symmetric key are applied as inputs to encipher, the encrypted output is show in fig.3.a. The cipher text is decrypted by taking cipher text and the same key used for encryption as inputs. We get plain text as decryption output. The decryption results are show in fig.3.b.
The encryption and decryption results of our proposed model is shown in fig.5. The results in fig.5 are similar to Trojan free results in fig.3. Our proposed model will give the correct data even in the Trojan effected condition and Trojan detection is also performed and gives that information as status signal. In fig.5.a status output is produce by our proposed system in order to indicate the status of the Trojan detection. Status is a two bit binary output and what status indicates is given in table I.

**TABLE I: Status Information**

<table>
<thead>
<tr>
<th>Status bits</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>There is no activation of Trojan</td>
</tr>
<tr>
<td>01</td>
<td>Trojan attacks on input data</td>
</tr>
<tr>
<td>10</td>
<td>Trojan attacks on input key</td>
</tr>
<tr>
<td>11</td>
<td>Trojan attacks both input data and key</td>
</tr>
</tbody>
</table>

5. CONCLUSION

In this paper, we proposed a method to Hardware Trojan detection and prevention using Multipath Authentication. Our proposed method is implemented in an AES crypto processor using LabVIEW simulation tool and successful in detecting and preventing the effect of Hardware Trojan.

ACKNOWLEDGEMENT

The authors of this paper would like to thank Department of Electronics and Communication Engineering and Management of Andhra Loyola Institute of Engineering and Technology for their valuable suggestions and support.
Hardware Trojans”.IEEE Access, 4, 2721-2731.June1, 2016.


