A Side Channel Based Power Analysis Technique for Hardware Trojan Detection using Statistical Learning Approach

Roshni Shende
Department of Electronics and Telecommunication
Sardar Patel Institute of Technology
Andheri(W), Mumbai, India.
roshni24shende@gmail.com

Dayanand D. Ambawade
Department of Electronics and Telecommunication
Sardar Patel Institute of Technology
Andheri(W), Mumbai, India.
dd_ambawade@spit.ac.in

***Abstract*—Hardware Trojan (HT) is an intentional and the undesired modification of the integrated circuit (IC) and major security issue for the semiconductor industry. HT alters the normal working of IC, can leak the secret information or may damage the IC permanently. Due to the small size of the devices on IC, detection of trojan is very difficult by normal testing methods. In this paper, a side channel based trojan detection technique using power analysis is used to detect the trojan infected IC. Here a trust-hub test bench circuit is used to validate trojan detection technique in which the Trojan is inserted on AES-128 bit crypto core. The trojan detection is improved by analyzing the power of IC without trojan (Golden model) and IC with trojan (Trojan model) and by comparing the mean of power traces of both the IC. Statistical data analysis is performed and statistical parameters of power are calculated which are then used as feature vectors. These feature vectors are reduced by using Principal Component Analysis (PCA) algorithm and then classified using Linear Discriminant Analysis (LDA) which discriminates between the Golden and Trojan model and detects the trojan infected IC from the IC under test with 100% accuracy.**

***Index Terms*—Hardware Trojan, Hardware Trojan Horse, power analysis, side channel analysis, PCA, LDA.**

I. Introduction

In 21st century due to the rapid development in technology, innovative and imaginative engineering expanded the electronics domain into wireless networking applications such as satellite, GPS, radio, mobile etc. All these devices continue to invent in speed, efficiency, accuracy, complexity and also change in cost. For lower cost and due to unavailability of manufacturing resources and technology, manufacturers has started production overseas, which means that the electronic devices are manufactured in other countries. This makes all these devices vulnerable to attacks from potential competitors or enemies. The attacker may insert the malicious circuit into hardware design causing it to appear as it is operating as expected. But however, in reality the device may leak the secret information or may cause DOS and several attacks on IC. This kind of Trojan is build in devices and can be activated by predefined condition. The hardware Trojan can be inserted in the IC circuit at various stages of IC design. Since electronics has its vast applications in various domains such as military, transportation, banking, government organizations, etc. Hardware trojan attacks on such domains is very dangerous and can cause hazardous effects on the whole country. Due to this, research in this field is evolving rapidly.

The rest of the paper is divided as follows : Section II gives the detail information about the Trojan and its detection techniques. Section III discusses the related work in this field. The methodology for Hardware Trojan detection is explained in section IV. Section V gives experimental setup and results. And it is concluded in section VI and Section VII gives the future scope.

II. Background

Hardware Trojan is the pernicious circuit inserted inside a chip which does not harm the chip until it gets triggered by predefined internal or external condition. Y. Alkabani et al. in [2] give the components of HTH (Hardware Trojan Horse). Fig. 1 shows that the HTH is divided into three parts which is trigger, storage and driver. The trigger activates the Trojan and the action to be taken after activation of HTH is stored in storage. The driver part implements the stored action.

Fig. 1: Components of HTH

The detailed taxonomy of HTH is explained by X.Wang et al. in [3] which divides the HTH in to 3 categories according to its characteristics which are Physical, Action and Activation characteristics. The physical characteristics give the shape, size and type of Trojan. Activation characteristics give the trigger mechanism, whether it is internally or externally triggered and the action characteristics explains the action to be taken when the Trojan is activated.

978-1-4673-8975-4/16/$31.00 ©2016 IEEE

R.S Chakraborty, S. Narasimha et al. in [4] gives the broad classification of Trojan detection techniques which is shown in Fig. 2. According to [4] the Trojan detection techniques are mainly classified into Destructive and Nondestructive. Destructive method of HT completely destroy the IC. In such technique the IC is reverse engineered for Trojan detection, which is a tedious process, hence these techniques are less useful. The non destructive method is classified into invasive and noninvasive. In invasive method the IC design is changed or modified for Trojan detection and in noninvasive method the Trojan is detected at run time or test time without changing the IC design. The test time approach for Trojan detection is further classified into two parts which are Side channel analysis and Logic testing method. In side channel analysis side channel signals such as power, path delay, electromagnetic radiation, etc. of the Golden IC and Trojan infected IC is compared and any deviation from the stored value of side channel parameters detects the presence of Trojan in the IC under test. In logic testing method different possible inputs are given to the circuit and outputs are tested. Any change in the output value detects the presence of trojan.

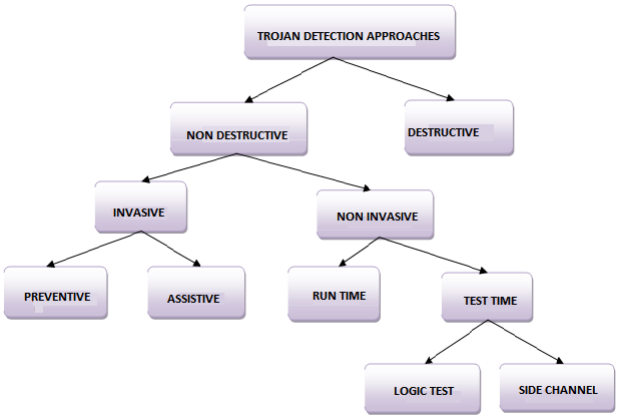

Fig. 2: Hardware Trojan Detection Approaches[4]

III. RELATED WORK

In this emerging technological world HT has become a major security threat. Hence, researchers are paying more and more attention towards the detection of such trojans. For evaluation of various Trojan detection techniques, many types of Trojan models are designed by the researchers Y. Jin et al. in [5]. The presence of the perciniois circuit in the IC affects the side channel parameter, hence these parameters can be examined closely for trojan detection. Y. Jin, Y. Makris in [6] proposed a path delay fingerprinting technique in which path delay measurements of Trojan infected IC are compared to golden IC as the hardware trojan present at the IC changes the path delay of IC. In [7] Li-Wei Wang Hong-Wie Luo proposed Trojan detection by analyzing the power of IC and the author uses data processing algorithm which is able to detect Trojan in the presence of large noise. The authors in [6] [7] does not consider the effect of process variations on trojan detection and hence Trojan detection is not 100% . The process variations are the random and unexpected variations in length, thickness, width, etc. of the IC during fabrication, which causes a measurable change in the output parameters and in small circuits of nanometer range consideration of the effects of process variation is most significant. Trojan detection in the presence of process variations is possible in [8] which is proposed by Narasimhan et al. in which effect of process variations on trojan detection is evicted by considering the relation and then giving the comparison between three parameters transient current, quiescent current, frequency of golden and trojan IC which improves the Trojan detection in the presence of large process variations. In [9] X-T. Ngo et al. proposed a trojan detection method by considering the effect of intradie process variations during Trojan detection and they also explain a Trojan detection method by measuring and analyzing electromagnetic radiations. Chunhua He et al. [10] gives trojan detection technique by combining the advantages of both logic test method and side channel analysis test together, which improves the Trojan detection sensitivity when Trojan size is small. N. Gunti and K. Lingasubramanian et al.[11] uses sleep transistors to detect the distributed small trojan across the IC which divides the IC into a number of parts so that only single part of IC remains active at a time so as to reduce the leakage power from the IC. This method improves the trojan detection by adding extra overhead due to sleep transistors.

IV. METHODOLOGY

A. A side channel based power analysis technique for hardware Trojan detection

The presence of extra circuitry in the IC circuit changes the side channel parameter such as the power of the IC. Thus the power dissipated by the IC can be analyzed to detect the presence of hardware Trojan in the circuit. The IC without trojan circuit is the Golden IC and the trojan infected IC is the Trojan IC. The total power dissipated in a device is obtained by adding two components of power: dynamic power when the device is switching, and static power when the device is at steady state[7].

The total power dissipated is given by following equations:

$$\mathrm{P}_{total} = P_{dynamic} + P_{static} \quad [7]$$
$$p_{total} = ((1/2).C.V_{dd}^2 + Q_{se}.V_{dd}).f.N + V_{dd}.I_{leak} \quad [7]$$

B. Hardware Trojan model description

In this paper, we are analyzing power of IC for trojan detection hence the trojan circuit which makes the IC to dissipate excess power than normal is used here for experimentation. Following description gives the explanation of the trojan model used in our experiment. The Trojan model from trust-hub site is used as a test bench for validation of Trojan detection technique. Trojan circuit is inserted in AES-128 bit crypto core at RTL (register transfer level) design level which is the Trojan infected IC. The Trojan is triggered internally and once

triggered the Trojan circuits leaks the secret key from the AES core. The leakage circuit here is 16 bit shift register which leaks the secret key when its input is high. Due to this, the circuit experiences more dynamic power consumption than the original circuit without Trojan. [1][12].

C. HT Detection

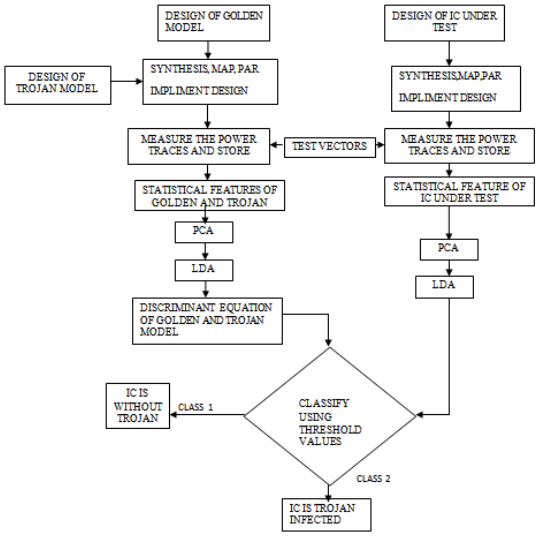

Fig. 3: Hardware Trojan Detection Using Power Analysis

Fig. 3 shows the flow chart of hardware Trojan detection using power analysis. The code for Golden and trojan model is synthesized and implemented on spartan-6 FPGA kit.

1.Data Generation:
Power analysis is done by giving different input vectors to the Golden and Trojan model. 256 test vectors are generated and these test vectors are given as input vectors to both Golden and Trojan IC and power is measured for each corresponding input vector for both the IC. Here supervised machine learning algorithm is used to detect trojan infected IC from the IC under test. In this paper measurement of power for 256 input vectors is taken 3 times for each Golden and Trojan IC. Out of 3 measurements we have used 2 measurements for training sequences and 1 measurement for test sequence.
2.Feature Extraction:
Statistical Data Analysis is performed on training sequences of power measurements and statistical parameters of power are calculated and the parameters are mean, variance, root mean square value, median, histogram. PCA algorithm is used to reduce the parameters to remove excess of overload and to avoid redundancy. The parameters are converted to feature vectors by reducing parameters to 60% of its value by using PCA.
PCA: Principle Component Analysis algorithm is used to reduce the number of variables in the data without changing the original value of data when the data is redundant i.e when the variables of data are correlated with one another PCA is used to convert correlated variables into uncorrelated variables. The dimension of the data is reduced by rejecting the unnecessary part from the data.
3.Data Classification:
After data reduction Linear Discriminant Analysis is performed on feature vectors which differentiates between the Golden and Trojan IC. LDA is a data processing algorithm which differentiates between two classes by maximizing separation between them.
4.Testing:
The statistical analysis is performed on testing sequences and parameters are reduced by PCA. Now LDA is performed on the reduced data which directly identifies the IC whether it is trojan infected or trojan free. Trojan detection is done by comparing the stored values of feature vectors of golden and trojan model with the feature vectors of IC under test.

V. Experimental Setup

The code for both golden and Trojan infected IC is synthesized using Xilinx ISE 14.7 tool and implemented on Xilinx Spartan-6 XC6SLX45 FPGA Board. We have used AES-128 bit crypto core as the golden IC and the Trojan model given in [1][12] is inserted in the AES-128 bit crypto core and used as Trojan IC. Power measurements for both Golden and Trojan IC are obtained using power analysis EDA Tools. Statistical analysis is performed on the measured value of power.

VI. Result and Performance Analysis

Table I shows the device utilization of Golden and Trojan IC.

TABLE I: Device Utilization of Golden and Trojan IC

Resources	Golden IC	Trojen IC
No. of slice registers	5259/54576-9%	4583/54576-8%
No. of slice LUT's	9590/27288-35%	8611/27288-31%
Number used as Memory	14/6408-1%	14/6408-1%
Bounded IOB's	17/218-7%	17/218-7%

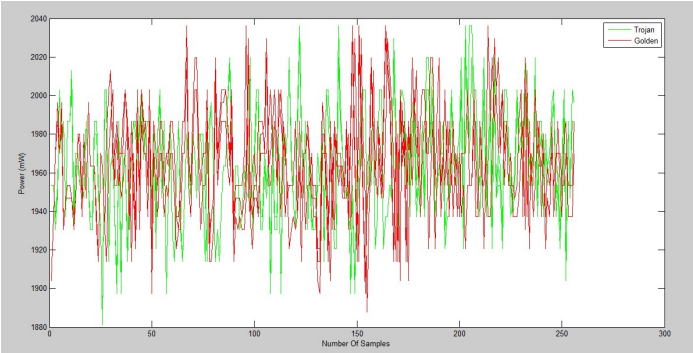

Fig. 4: Power Traces of Golden and Trojan IC for 3 measurements each

Fig. 4 and Fig. 5 shows the plots for the power traces of golden and Trojan model. The graphs are plotted between the power and sample points. The sample points are the input

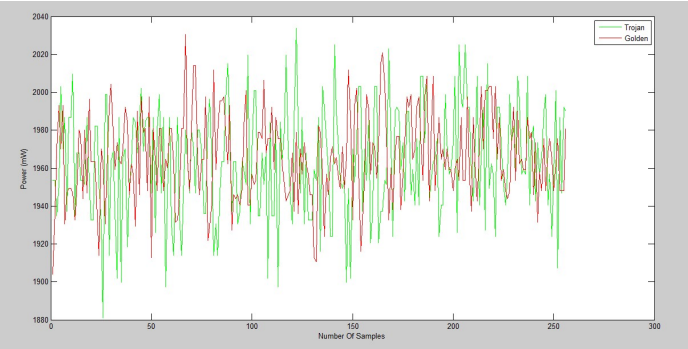

Fig. 5: Mean Power Traces of Golden and Trojan IC

vectors to the IC. Power trace of golden model is plotted in green color and that of Trojan model is plotted in red color. Fig. 4 gives the power traces for 3 measurements each of golden and Trojan IC with same input vector. The difference between power traces of Golden and Trojan IC is clearly visible in Fig. 5 in which the mean of power measurements is plotted and it can be seen that the Trojan IC dissipates more power than the golden IC. And also the power variation of Trojan IC is greater than the golden IC for different input vectors. Statistical analysis is performed on training and testing sequences and results shows that after 60% reduction (from 5 to 3 feature vectors) of parameters LDA accurately (100%) classifies the difference between Trojan infected and IC without trojan.

VII. Conclusion

In this paper, we discussed the side channel based Trojan detection approach using power analysis. Here we have used the FPGA environment for our experimentation. Power measurements of both the Golden and Trojan IC are analyzed and two graphs are plotted which shows that the difference between the power traces of golden and Trojan infected IC is clearly visible in the mean power plot than the normal plot. And the Trojan IC dissipates more power than the golden IC and also the power variation of Trojan IC about mean zero value is more than the golden IC. Statistical analysis is performed on measured power data of Golden and Trojan IC and the results shows that the proposed model classifies between the trojan IC and IC without trojan with 100% accuracy.

VIII. Future scope

For our future work we will make some improvements in our Trojan detection technique. We will take more number of measurements for different input vectors. Also in this paper the test is performed on a single IC. In our future work we will perform our tests on a number of IC's to enhance the trojan detection sensitivity.

Acknowledgment

The author would like to thank Sardar Patel Institute of Technology, India for providing the necessary facilities for carrying out this work.

References

[1] https://www.trust-hub.org
[2] Y. Alkabani, F. Koushanfar, "Extended Abstract: Designers Hardware Trojan Horse", *IEEE International Workshop Hardware-Oriented Security and Trust (HOST08), IEEE CS Press* 2008, pp. 82-83.
[3] X. Wang, H. Salmani, M. Tehranipoore, J. Plusquellic "Hardware Trojan Detection and Isolation Using Current Integration and Localized Current Analysis", *IEEE International Symp. Defect and Fault Tolerance of VLSI Systems (DFT 08), IEEE CS Press*, pp. 87-95,2008.
[4] R.S. Chakraborty, S. Narasimhan, and S. Bhunia, "Hardware trojan: threats and emerging solutions", *IEEE International Workshop Hardware-Oriented Security and Trust (HOST 09)*, pp. 166-171, 2009.
[5] Y. Jin, N. Kupp, Y. Makris, "Experiences in Hardware Trojan Design and Implementation", *IEEE International Workshop Hardware-Oriented Security and Trust (HOST 09)*, pp. 50-57, 2009.
[6] Y. Jin, Y. Makris, "Hardware trojan detection using path delay fingerprint", *IEEE International Hardware-Oriented Security and Trust (HOST 08)*, pp. 51-57, 2008.
[7] Li-Wei Wang, Hong-Wei Luo, "A Power Analysis Based Approach to Detect Trojan Circuits", IEEE 2011.
[8] Narasimhan ,Chakraborty ,S.Paul et al. "Hardware Trojan Detection by Multiple- Parameter Side-Channel Analysis", *Computers, IEEE Transactions on 62.11 (2013)*: 2183-2195
[9] X-T. Ngo, I. Exurville, S. Bhasin, J-L. Danger, S. Guilley, Z. Najm2, J-B. Rigaud3 and B. Robisson." Hardware Trojan Detection by Delay and Electromagnetic Measurements", *Design, Automation Test in Europe Conference Exhibition (DATE)*, pp.782-787,2015.
[10] Chunhua He, Bo Hou, Liwei Wang, Yunfei En, Shaofeng Xie, "A Novel Hardware Trojan Detection Method Based on Side-Channel Analysis and PCA Algorithm", *International Conference on Reliability, Maintainability and Safety (ICRMS)*, pp. 1043-1046 ,2014
[11] N. Gunti, K. Lingasubramanian, "Efficient Static Power Based Side Channel Analysis for Hardware Trojan Detection Using Controllable Sleep Transistors", *IEEE Southeast Conference* 2015, April 9 - 12, 2015 - Fort Lauderdale, Florida.
[12] L. Lin, M. Kasper, T. Gneysu, C. Paar and W. Burleson,"Trojan SideChannels: Lightweight Hardware Trojans through SideChannel Engineering", *11th International Workshop Cryptographic Hardware and Embedded Systems (CHES)*, pp.382395, 2009.