International Journal of Electrical and Computer Engineering (IJECE)
Vol. 9, No. 5, October 2019, pp. 4035~4043
ISSN: 2088-8708, DOI: 10.11591/ijece.v9i5.pp4035-4043

A compressive sensing algorithm for hardware trojan detection

M. Priyatharishini, M. Nirmala Devi
Department of Electronics and Communication Engineering, Amrita School of Engineering, Coimbatore, Amrita Vishwa Vidyapeetham, India

Article Info

Article history:

Received Jul 12, 2018
Revised Apr 17, 2019
Accepted Apr 28, 2019

Keywords:

Compressive sensing
Hardware security
Hardware trojan
Self referencing
Test generation

ABSTRACT

Traditionally many fabless companies outsource the fabrication of IC design to the foundries, which may not be trusted always. In order to ensure trusted IC's it is more significant to develop an efficient technique that detects the presence of hardware Trojan. This malicious insertion causes the logic variation in the nets or leaks some sensitive information from the chip, which reduces the reliability of the system. The conventional testing algorithm for generating test vectors reduces the detection sensitivity due to high process variations. In this work, we present a compressive sensing approach, which can significantly generate optimal test patterns compared to the ATPG vectors. This approach maximizes the probability of Trojan circuit activation, with a high level of Trojan detection rate. The side channel analysis such as power signatures are measured at different time stamps to isolate the Trojan effects. The effect of process noise is minimized by this power profile comparison approach, which provides high detection sensitivity for varying Trojan size and eliminates the requirement of golden chip. The proposed test generation approach is validated on ISCAS benchmark circuits, which achieves Trojan detection coverage on an average of 88.6% reduction in test length when compared to random pattern.

Corresponding Author:

M. Priyatharishini,
Department of Electronics and Communication Engineering,
Amrita School of Engineering, Coimbatore,
Amrita Vishwa Vidyapeetham, India.
Email:m_priyatharishini@cb.amrita.edu

1. INTRODUCTION

The presumption of fabricated ICs not being subjected to any trade off in security was present for a long time. To lower the fabrication costs, third party fabrication industries are involved in the production of SoC (System on Chip). Some of these foundries may act as an adversary and might insert malicious circuitry into the chips during the fabrication process.These additional modules are efficiently designed such that they evade detection during post manufacturing tests and are deployed in field application. The malicious IP-Cores apart from corrupting the functionality of the SoC may cause consequences in the fields which require extreme information security such as defence, medicine and communication. To reduce the vulnerability of the SoC, hardware security and Trojan detection are incorporated to safeguard and protect the sensitive designs.

Hardware security involves the major research areas such as detection and diagnosis of hardware Trojans along with design of secured hardware. Classification of Hardware Trojans and various threats are analyzed in [1]. The lack of availability of golden chips as a reference circuit is the main challenge for the researchers to detect the Trojan. The Hardware Trojan has been classified [2] into three different types as an internal trigger, storage and Hardware Trojan driver. Wang et al. developed an elaborate hardware Trojan taxonomy in [3] which categorized the Trojans into physical, activation and action characteristics. In [4] the activation mechanism is further categorized into digital and analog Trojans. The impact of digital Trojan may

affect the logic values of the specified internal node or it may also alter the stored content in the memory unit. The performance, power and noise margins are the parameter which gets affected due to the analog payload Trojan. In-order to secure the vulnerable system, the researchers mainly focuses on activation mechanism of Trojan circuit. The activation mechanism includes transition probability based Trojan triggering [5], in which the node selection technique for the Trojan insertion is proposed for detection process. To ensure the presence of Trojan module using conventional testing approach triggers the internal nodes and propagation of logic variations in the nets due to Trojan effects to the payload must be enhanced. The problem of detecting the Trojan module using conventional test vector approach is a challenging task for extracting Trojan triggering vectors by taking fault masking logic into consideration. In addition, the internal nodes and Trojan triggers are dependent factors, which indicates instead of conventional testing, a compressive sensing approach for sparse test pattern generation for triggering the Trojans are formulated in a feasible manner.

In the proposed work, an optimal test pattern generation technique using compressive sensing approach has been attempted to aid in the detection of hardware Trojan.The proposed compressive sensing approach is performed on the input patterns to provide optimal test patterns that can distinguish a Trojan infected chip from a golden chip. This approach is performed to extract the Trojan triggering test vectors thet are rare and is also sparse. Thus by attempting the proposed compressive sensing approach, the sparsity of the test vectors is achieved and can effectively determine the revealing test patterns from the large pool of test vector space. This approach generates compact test set, which minimizes the time complexity for testing, while maximizing the probability of Trojan detection coverage. The transition probability algorithm is formulated to extract the significant internal nodes in the net-list for insertion of Trojan module. The main insight of measuring the power profile in our work is to classify the IC is Trojan free if the power signature is constant and Trojan infected if it has some anomaly at different time instances. Simulation results shows that the proposed compressive sensing approach is effectively used for detecting both combinational as well as sequential Trojans.

The rest of the paper is organized as follows: Section 2 describes the state-of-the-art techniques for hardware Trojan detection schemes and challenges based on compressive sensing techniques. The Proposed compressive sensing based test set approach for detection Trojan module is presented in Section 3. The Simulation results for various ISCAS benchmark circuit with detailed observations is described in Section 4. At the end, Section 5 concludes the paper.

2. BACKGROUND

Hardware Trojans are embedded into the original finite state machine by the Trojan design engineers by composing a high level design description of the Trojan. Thus a Trojan FSM is injected by merging their states with the original design and is indistinguishable from the functionality of the golden chip. This method of Trojan insertion will hide the presence of Trojan and is hard to detect by the conventional authentication techniques. The countermeasures against these Trojans are classified into two types such as detection and design for trust.

2.1. Detection

The hardware Trojan detection is developed in the hardware security community and are broadly categorised into destructive and non- destructive [4] as shown in the Figure 1. The destructive approach is analysed to verify the chip design by an optical method. Thus the chip is examined layer by layer in this method and each chip is to be tested individually. Hence this approach is applicable only for the IC's which is fabricated under untrusted foundry. The requirement of specialized equipment and the cost are the major limitations of this analysis. The non-destructive approach is analysed by considering the characteristic behaviour of the chip and the presence of Trojan is identified by mapping with the examined profile. This method of hardware Trojan is further classified into three types such as design time approach, run time approach and test time approach.

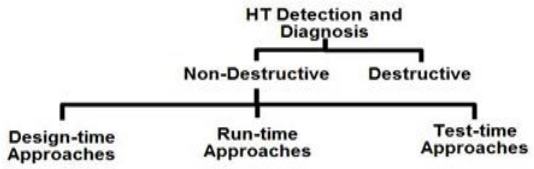


Figure 1. Classification of Hardware Trojan detection [4]

2.1.1. Design approach

A pre-silicon method of hardware Trojan detection is employed in this approach, which detects the threats associated with intellectual property (IP). A hardware Trojan module is inserted to the design of golden IP without the designer's knowledge and these Trojans behaviour will be hidden during normal verification test. The design time approach is further divided into formal verification and design for security. The process of property checking is a formal verification, in which the IP properties of the design under test are analysed with the original reference IP. In paper [6] proposed a method for diagnosis which locates the malicious module in the third party IP. The isolation of infected third party IP from the authentic one is experimentally proved in this method and the location of Trojan module is also effectively identified only when the Trojan are triggered. Hardware Trojans internal and external activation delivers the character of Trojan module and its various types of activation mechanism are listed in [7]. The triggering input of the Trojan circuit is independent from the original circuit and it is represented as always on Trojan.

2.1.2. Runtime approach

The run time approaches are used to detect to detect the Trojan by inserting a sensor module to the original chip and the activity of the IC's are continuously monitored. The variation in the characteristics of the chip under test from the expected reference characteristics will indicate the presence of malicious module. A hybrid method of run time is proposed [8], which combines a design time component with the run time monitoring such as blue chip. An on-line monitoring approach of hardware Trojan detection is proposed in [9], which mainly focuses on original functionality of the circuit and detects any variation from the expected logic values at the suspected internal nodes. A Two rail checker module are developed and inserted in the system to monitor the logic malfunction in its vicinity.

2.1.3. Test time approach

The presence of malicious module is detected in test time approach during post manufacturing process. The test time approaches are classified into two types such as functional testing approach and side channel analysis. The presence of Trojan changes the functionality of the design is detected using logic verification known as functional testing approach [10]. The main drawback of this method is that the Trojan inserted will not alter the functionality of the circuit until it is triggered. Compressive sensing technique is an emerging methodology which is related with the functional testing approach [11].

2.2. Design for trust

The design for security techniques is applicable for designing the structure in-order to enhance the level of security in hardware. The design for security is classified such as logic encryption, IC camouflaging, split manufacturing and Trojan activation. In paper [12], proposed a design methodology in which the IP's are protected by obfuscating the original net-list. In this technique, the normal mode of operation is possible only when the valid key is provided to the key gates where the delay and area are the main constrains. S. Dupuis, et al., [13, 14] proposed an encryption algorithm which minimises the number of rare occurrence values of the internal node. In this logic encryption technique, the probability of all the internal nodes is computed in-order to identify the low controllability nodes. The proposed method overcomes the above specified drawbacks and also protects the IC's from illegal over production. A several key technologies associated with network security are proposed in paper [15], which satisfies the computational security aspect in electronic voting, data mining and other fields. The split manufacturing [16] technique is applicable in layout level in which the original design is split into two layers and it is fabricated under different foundries. The adversary cannot access the complete details of the split design and hence the inserting a Hardware Trojan is not possible in this technique.

3. PROPOSED METHODOLOGY

The main goal of the proposed methodology is to generate the test patterns that can excite the Trojan triggering nodes more effectively. The Probability distribution of each net in the circuit under test is calculated in order to determine the extra Trojan gate in the IC. The Hardware Trojan detection using proposed methodology is shown in Figure 2.

3.1. Reduced Test set Generation using CS

Algorithm 1 describes the major steps in the proposed generation of optimal test vectors for Trojan detection. The gate level net-list is considered as the input file for the conventional ATPG tool. The test vectors obtained from the ATPG are further compressed using proposed compressive sensing algorithm. The input signal to the compressive sensing algorithm must be sparse in any domain. The sparsity of the

signal is achieved by incorporating basis matrix ($\boldsymbol{\Psi}$) to the input, which converts the signal in one domain to another domain where it is sparse. Thus, the N number of test patterns generated from ATPG is further compressed into M number of test patterns (M<<N) after compressive sensing (CS). The result of the proposed CS pattern generation method is a optimal test set that identifies the presence of Trojan and also improves the test coverage for Trojans compared with original test patterns.

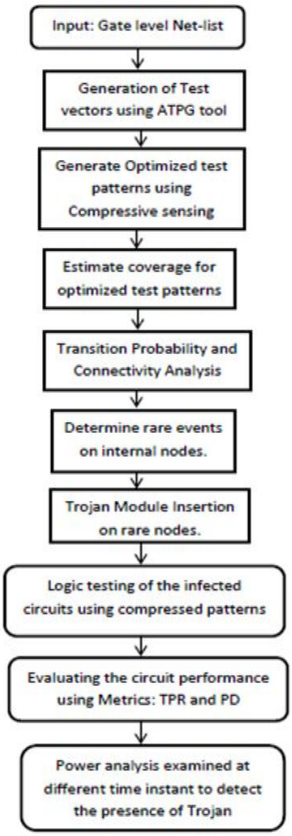


Figure 2. Proposed hardware Trojan detection flow

Algorithm 1. Generate reduced test set using compressive sensing for Trojan Detection

Input: Circuit Net-list, list of random patterns (T), constant(c), list of node (R).
Output: Reduced test patterns (Tc).

1. Read the circuit net- list.
2. for all random patterns in T do
3. Compute the sparsity parameter k
4. Compute M with c as constant values
5. $M \geq c * k * \log(T/k)$
6. Compute Minimal value of M<N.
7. Generate $\boldsymbol{\Phi}$ matrix € M x N.
8. for all bits in T do
9. Compute reduced setTc
10. Tc= $\boldsymbol{\Phi}$ matrix * T matrix
11. end for
12. end for

3.2. Node identification for Hardware Trojan insertion

Transition probability value plays a very significant analysis in inserting the Trojan module to the circuit. The internal nodes with low transition probability (TP) are more susceptible for triggering the Trojan and payload. It is also highly likely that an adversary might insert a Hardware Trojan (HT) in these low TP

nodes because of their low switching activities, which triggers the Trojan module in rare instances. The algorithm 2 provides the calculation for transition probability. The probability calculation for basic logic gates [5] is expressed as

$$OP(1) = IN1(1) * IN2(1)(1) \quad (1)$$

$$OP\ (0)\ =\ IN1(0)\ +\ IN2(0) - [IN1(0)\ *\ IN2(0)] \quad (2)$$

The Hardware Trojans such as combinational and 3 bit counter sequential modules are designed, which get activated at rare conditions and cause changes in the performance of the chosen benchmark circuits. Nodes with low Transition Probability (TP) and high connectivity are selected and the designed Hardware Trojan (HT) modules are inserted at these nodes for validation process.

Algorithm 2. Calculating Transition probability value for each net

Input: Circuit net-list, module list of the circuit.
Output: Transition probability (TP) values.
Step1: Scan the module list. xlsx file.
Step2: Extract the primary input (PI), output (PO) and the gates of the circuit.
Step3: Initialise the probability of primary inputs nets as 0.5.
Step4: Determine the net index.
Step5: If (net index = net index of PI) then
Step6: Store the TP values in an array
Step7: else
Step8: for each net in the net- list do
Step9: Find the type of gate and index values of input
Step10: Calculate the probability at the output net according to the gate type
Step11: Calculate the transition probability values for each net
Step12: Store nets transition probability in ascending order.
Step13: end for
Step14: end if

3.3. Logic testing

Logic testing is performed by comparing the logic values at the nodes in the golden circuit with that of the Trojan ICcircuit for all possible test patterns obtained from proposed algorithm. The Table 1 provides the comparison of the logic values for Trojan infected and golden circuit. A combinational type of Trojan is inserted in the low transition probability node and the logic variations in the nets are observed which indicates the presence of Trojan module.

Table 1. Comparison of output function in Logic Testing

Input Pattern	C17 Golden						C17 Trojan circuit					
	Internal Nodes				Primary output		Internal Nodes				Primary output	
	N6	N7	N8	N9	N10	N11	N6	N7	N8	N9	N10	N11
1	1	1	1	0	0	1	1	1	1	0	0	1
7	1	0	1	1	0	0	1	1	1	1	0	1
14	1	0	1	1	0	0	1	1	1	1	1	1

In-order to validate the efficiency of detection of Hardware Trojan using compressive sensing, metrics such as True Positive Rate (TPR) and Probability of detection (PD) [5] are applied to the circuit under test. In case of binary classification, the True positive (TR) value identifies the number of Trojan nets as malicious nets itself and the False negative (FN) values shows the number of Trojan nets identified as normal nets by mistake.

3.4. Power analysis

The compressed test set generated from the proposed algorithm are forced to the design under test at different time windows. A Synopsys prime time tool is used to determine the leakage power for every test vector. The hardware Trojan chosen for this analysis is a three bit counter and its impact will be noticed only during certain clock cycle. The observed power profile will vary for the Trojan IC at some time stamp whereas it is unaltered for the Trojan free IC. The variation of the power profile is mainly due to the application of certain test sets which activates the Trojan module. This method of side channel approach for detecting Trojan module does not requires any golden net list as reference circuit.

4. RESULTS AND DISCUSSION

The proposed methodology is validated using ISCAS 85 combinational benchmark circuits with combinational and sequential Trojan modules, which alters the functionality of the circuit. Table 2 lists the comparison of test vector reduction for ISCAS bench mark circuits for conventional ATPG patterns and proposed compressive sensing (CS) approach. It is observed that the proposed test set using CS achieves an average test length reduction of 88.6%, while maximizing the Trojan triggering rate. The run time for executing this algorithm is also computed.

Table 2. Test pattern reduction using CS algorithm

Bench mark circuits	No. of primary inputs	Possible Test vectors	Test vectors using ATPG (N)	Test vectors using CS (M)	Compression ratio (CR)	Processing Time (s)
C17	5	2^5	7 x 5	3 x 5	99.4	0.0182
C432	36	2^{36}	63 x 36	23 x 36	92.33	0.587
C499	41	2^{41}	56 x 41	19x41	93.66	0.79
C880	60	2^{60}	148 x 60	55 x 60	81.66	1.003
C1355	41	2^{41}	100 x 41	37 x 41	87.66	0.178
C3540	50	2^{50}	265 x 50	97 x 50	70.6	0.162
C6288	32	2^{32}	34 x 32	13 x 32	95.6	1.56

The Transition Probability (TP) values are evaluated for different bench mark circuits and low TP values along with the high connectivity nodes are also listed in the Table 3. The Low TP values are considered as potential nodes and these nodes are chosen by the attackers at the design site to introduce the Trojan gate for malicious intention. For the simulation of power profile some of the locations are considered for Trojan insertion and the results are validated for detection process.

Table 3. Target nodes identification using Transition Probability values

Bench mark circuits	Minimum TP values	Nodes with low TP value	High Connectivity nodes
C17	0.1875	N6,N7	N6,N7
C432	0.0836691	N259,N262,N263,N266,N269,N272, N278,N281,N284,N287,N288,N289, N290,N291,N292,N293,N294,N299, N300,N301,N302,N303,N304,N305, N306,N307	N295, N299, N300, N301, N302, N302, N308, N318.
C499	0.0585938	N382,N383,N384,N385 N378,N379,N380,N381	N289, N325, N312, N372, N378, N379.
C880	0.0000610314	N507, N508, N509, N510, N511, N512, N513, N514.	N752,N753,N754, N755,N756,N760,N761,N770
C1355	0.00727229	N996,N1001,N1006, N1011, N1016,N1021,N1026, N1031	N794, N797, N800, N803,N806,N812, N815,N996

The Comparison of the detection probability metrics such as True Positive Rate (TRP) and trigger coverage for the conventional test generation ATPG and the proposed compressive sensing approach is analyzed in Table 4. The Trojan is inserted at different nodes with low TP and it is observed that the test vector obtained by proposed CS approach is capable of determining the Trojan module more effectively during logic testing. It is also observed that reduced test pattern provides high trojan triggering coverage compared to ATPG patterns, which proves the CS approach has revealed the optimal test vectors for the triggering the Trojan module and improves the detection rate.

Table 5 lists the Probability of Detection (PD) rate for the ISCAS benchmark circuit. Key nodes with low TP values are selected for Trojan insertion and the results are validated. It is observed that for most of the pattern the detection probability is high, which indicates the effective test set generated by the proposed algorithm, while maximizing the Trojan detection rate.

The Figure 3 shows the Power signature for various ISCAS benchmark circuits. A sequential 3-bit counter is designed in order to observe the variation of power profile during specific clock pulse to validate the Trojan presence. The proposed CS test set is applied to circuit under test and the power profile is measured for different time stamps. It is observed that the value of the measured power overlaps for Trojan free circuit and for some set of test patterns it shows some variation in power for Trojan infected circuits. The proposed sparse test patterns triggers sequential Trojan and is reflected by non-overlapping of power profile which maximizes the probability of Trojan detection.

Table 4. Comparison of True Positive Rate metrics and trigger coverage

Bench mark circuits	Trojan Inserted Nodes	Proposed CS Algorithm patterns				ATPG Patterns			
		Trigger Coverage	True Positive	False Negative	TRP	Trigger Coverage	True Positive	False Negative	TRP
C17	7	66.66	2	1	0.667	28.57	2	5	0.285
	9	33.33	1	2	0.333	14.28	1	6	0.142
	7 ,9	100	2	1	0.667	42.85	2	5	0.285
C432	300	95.65	3	20	0.131	49.2	4	59	0.0634
	301	95.65	2	21	0.0869	44.44	2	61	0.0317
	300, 301	95.65	3	20	0.131	53.96	4	59	0.0634
C499	378	94.73	6	13	0.3157	83.92	8	48	0.143
	379	94.73	6	13	0.3157	82.14	8	48	0.143
	378, 379	100	6	13	0.3157	91.07	8	48	0.143
C880	507	94.54	51	4	0.927	39.18	57	91	0.385
	511	94.54	47	8	0.855	39.18	53	95	0.358
	507, 511	94.54	52	3	0.945	39.18	58	90	0.391
C1355	996	91.89	34	3	0.919	66	66	34	0.66
	1016	89.18	33	4	0.892	65	65	35	0.65
	996,1016	94.59	35	2	0.946	73	73	27	0.73

Table 5. Probability of Detection Metrics for Trojan detection

Bench mark circuits	Applied Test patterns using CS	No. of Trojans triggered	Output changes	Probability of detection
C17	1/3	1	yes	33.33%
	2/3	2	no	66.66%
C499	11/19	3	yes	100%
	7/19	2	yes	66.66%
	1/19	0	no	0%
C880	46/55	3	yes	100%
	4/55	2	yes	66.66%
	2/55	1	yes	33.33%
	3/55	0	no	0%
C3540	27/43	3	yes	100%
	16/43	2	yes	66.66%
C6288	8/13	3	yes	100%
	4/13	2	yes	66.66%

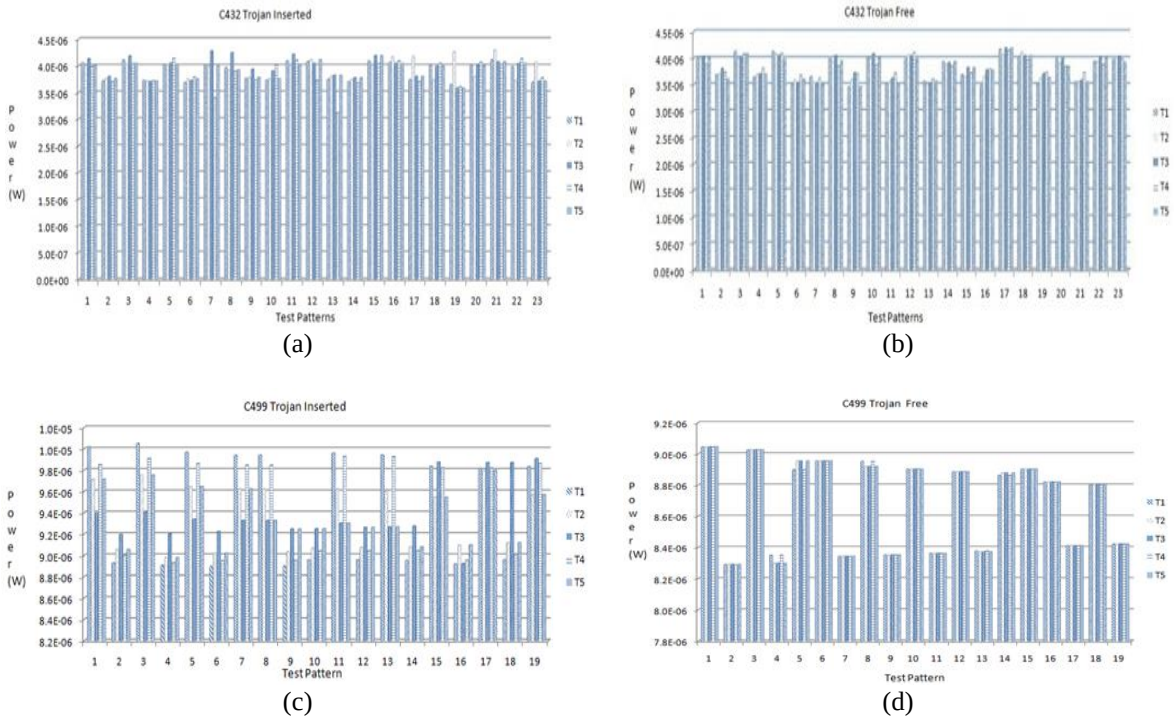
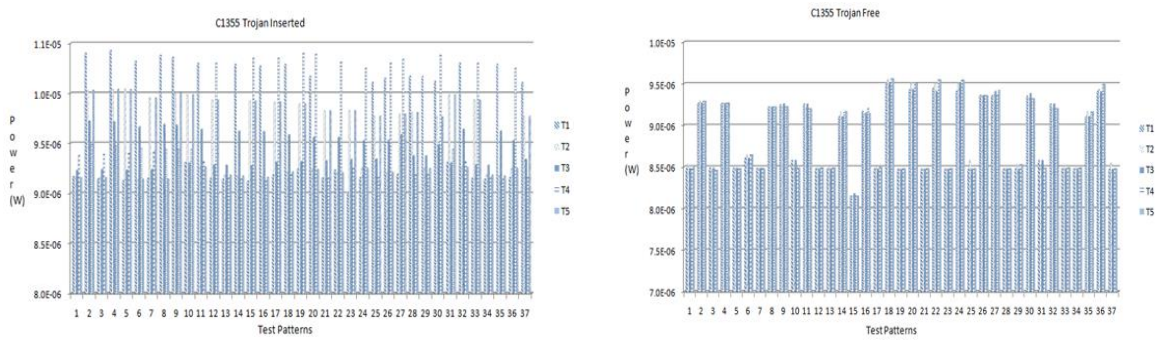


Figure 3. Measurement of power profile at different time windows
(a) C432 Trojan inserted circuit, (b) C432 circuit, (c) C499 Trojan inserted circuit, (d) C499 circuit



(e) (f)

Figure 3. Measurement of power profile at different time windows
(e) C1355 Trojan inserted circuit, (f) C1355 circuit

5. CONCLUSION

In this work a compressive sensing approach based on Trojan detection is presented, where the concept of sparsifying all possible input vectors is used to generate the revealing test vector which triggers the Trojan module. The simulation is done on ISCAS'85 bench mark circuit, which shows the proposed CS based test set generation approach which achieves about 88.6% reduction in test lenght over conventional test set. The detection of hardware Trojan is ensured by validating the probability of detection and trigger coverage metrics. The proposed detection approach improves the test quality by minimizing the test length and maximizing the triggering rate. He side channel parameter are analysed for the CS based test patterns at different time windows, which avoids the requirement of golden chip for detection process.

REFERENCES

[1] Chakraborty, et al., "Hardware Trojan: Threats and emerging solutions," *In High Level Design Validation and Test Workshop, 2009. HLDVT 2009. IEEE International*, pp. 166-171, 2009.
[2] Y. Alkabani and F. Koushanfar, "Designer's hardware Trojan horse," *In Hardware-Oriented Security and Trust, 2008. HOST 2008. IEEE International Workshop On*, pp. 82-83, 2008.
[3] X. Wang, et al., "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, 2008.
[4] M. Tehranipoor, "A Survey of Hardware Trojan Taxonomy and Detection," *IEEE Design, Test of Computers*, 2010.
[5] J. Popat and U. Mehta, "Transition probabilistic approach for detection and diagnosis hardware Trojan in combinati onal circuits," *IEEE*, 2016.
[6] M. Banga and M. 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, 2010.
[7] Karunagaran D. K. and N. Mohankumar, "Malicious Hardware Trojan Detection by Gate level minimization 90nm Technology," *5th International Conference on Computing Communication and Network Technology* (ICCCNT), 2014.
[8] M. Hicks, et al., "Overcoming an Untrusted Computing Base: Detecting and Removing Malicious Hardware Automatically," *In IEEE Symposium on Security and Privacy*, pp. 159-172. 2010.
[9] R. S. Chakraborty, et al., "A Flexible Online Checking Technique to Enchance Hardware Trojan Horse Detectability by Reliability Analysis," *IEEE Transactions on Emerging Topics in Computing*, 2017.
[10] Chakraborty, et al., "MERO: A statistical approach for hardware Trojan detection," *in Cryptographic Hardware and Embedded Systems-CHES 2009*, Springer Berlin Heidelberg, pp. 396-410, 2009.
[11] S. Foucart and H. Rauhut, "An Invitation to Compressive Sensing," *Applied and Numerical Harmonic Analysis*, pp. 1-39, 2013.
[12] Chakraborty, et al., "HARPOON: an obfuscation-based SoC design methodology for hardware protection," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol/issue: 28(10), pp. 1493-1502, 2009.
[13] S. Dupuis, et al., "A novel hardware logic encryption technique for thwarting illegal overproduction and Hardware Trojans," *2014 IEEE 20th International On-Line Testing Symposium (IOLTS)*, pp. 49-54, 2014.
[14] J. Sun, et al., "An Improved Public Key Encryption Algorithm Based on Chebyshev Polynomials," *TELKOMNIKA Indonesian Journal of Electrical Engineering*, vol/issue: 11(2), pp. 864-870, 2013.

[15] X. Guo, et al., "Key Technologies and Applications of Secure Multiparty Computation," *TELKOMNIKA Indonesian Journal of Electrical Engineering*, vol/issue: 11(7), pp. 3774-3779, 2013.
[16] R. W. Jarvis and M. G. McIntyre, "Split manufacturing method for advanced semiconductor circuits," *U.S. Patent* 7,195,931, Mar 2007

BIOGRAPHIES OF AUTHORS

M. Priyatharishini is an assistant professor in the department of Electronics and Communication Engineering at Amrita Vishwa Vidyapeetham, Coimbatore. She received the M.Tech. degree in Embedded system design from Amrita University, Coimbatore. She is working toward the PhD degree in the ECE Department, Amrita Vishwa Vidyapeetham, Coimbatore, India. Her research interests include hardware Trojan detection in integrated circuits, and trusted hardware design.

M. Nirmala Devi is a professor in the department of Electronics and Communication Engineering at Amrita Vishwa Vidyapeetham, Coimbatore, India. Her research interest includes VLSI Design and Testing, Computational Intelligence, Hardware Security and Trust, Evolvable Hardware and RF CMOS System Design. She has published around 55 papers in the International Journals and Conferences in her field of expertise. She has served as the 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, England. She has received the financial grant for the research proposal from Defence Research & Development Organization, Delhi, India.