Golden IC free Methodology for Hardware Trojan Detection using Symmetric Path Delays

Ramakrishna Vaikuntapu, Lava Bhargava, Vineet Sahula
Department of Electronics and Communication Engineering
Malaviya National Institute of Technology, Jaipur-302017, India
vramakrishna409@gmail.com, lavab@mnit.ac.in, sahula@ieee.org

***Abstract*—Hardware Trojans can be inserted by an adversary at any phase of IC manufacturing. In this paper, a methodology is proposed to detect Trojans inserted after design sign-off i.e the Trojan insertion occurs at layout level. In such attack models, golden IC are not always available in all cases, thus requiring golden IC free detection methodologies. This work exploits the concept of symmetric path delays to detect Trojans, considering the change in delays of symmetric pairs due to Trojan insertion. We propose detection metric (DM) of a suspect IC and compare the same with a detection threshold (DT) to decide whether IC under purview is Trojan free. Moreover, this method does not require any golden IC. Additionally, this method is robust enough against process variation effects. Simulation results establish that, a detection rate of 100% is achievable with maximum of 8% intra-die and 10% inter-die variation in both threshold voltage (V_{th}) and length (L), respectively.**

***Index Terms*—Hardware Trojan, Trojan detection, Path delay, Process variation, Hardware security.**

I. Introduction

The semiconductor IC manufacturing process involves many third-party design and fabrication houses whose trustworthiness is not known. Hardware Trojan (HT) is one threat to the security of ICs posed by such houses. Hardware Trojan can be defined as addition or deletion of few gates to the original design with a malicious intent by an adversary. The detailed taxonomy of hardware Trojans at various abstraction levels is presented in [1]. In general, Trojans are intelligently designed to be stealthy, such Trojans can not be detected by using conventional functional and structural testing techniques. Several detection methods are devised based on side channel analysis (SCA) i.e analyzing power, path delay etc [2-4]. In contrast to earlier approaches, proposed work is capable of detecting Trojan inserted ICs by exploiting the path delay parameter, though without requiring a golden IC. This paper's contribution lies in reducing the number of paths for delay measurement and covering the entire IC for detecting Trojans. Moreover, this method is able to detect unactivated Trojans, and eliminates the effort needed to activate Trojans.

II. Proposed Methodology

The delays of some paths out of all paths within an IC would be equal. We consider such paths as symmetric paths. All paths are segregated into different groups such that, paths within a group have equal delays. At least one pair of paths is selected from each group in a way the entire IC is covered. When the delays of such pairs are plotted on a two dimensional space they would follow a strait line as shown in Fig.1. The proposed methodology is shown in Fig.2. Assuming, N pairs have been selected out of all paths in such a way that these paths in a pair have nearly equal delays. Let $P_p^{(i)}$ represents the delay of p^{th} path in i^{th} pair. As a pair has only two paths in it, $p \in \{1,2\}$ and $i \in \{1,2...N\}$ as we have selected N pairs. If any hardware Trojan is inserted in the IC, it would affect the delay of at least one path which in turn leads to some deviation from the expected straight line as shown in Fig.1. Assuming inserted Trojan is affecting the delay of path 2 in pair j i.e $P_2^{(j)}$, then point ($P_1^{(j)}$,$P_2^{(j)}$) of pair j would deviate from the expected straight line as shown in Fig.1. We propose d_j to be distance between expected straight line and the point ($P_1^{(j)}$,$P_2^{(j)}$) can be calculated using (1).

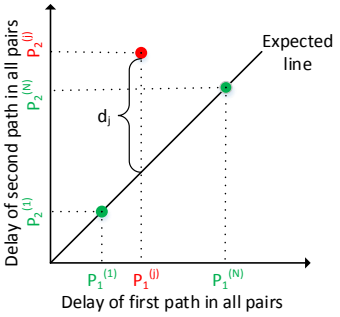

Fig. 1. Deviation from expected line due to Trojan insertion

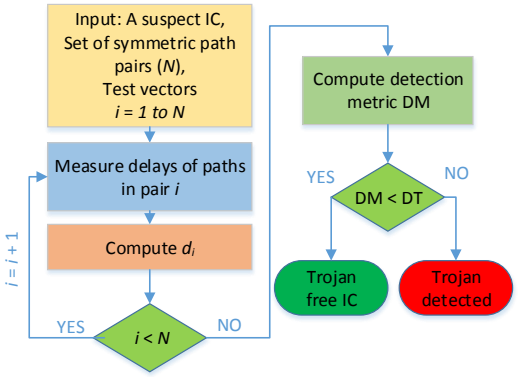

Fig. 2. Proposed Trojan detection methodology

$$d_j = \frac{1}{\sqrt{2}} \mid P_1^{(j)} - P_2^{(j)} \mid \quad (1)$$

978–1–5090–1422–4/16/$31.00 © 2016 IEEE

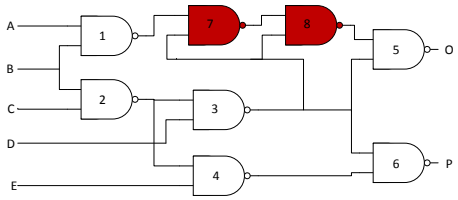

Fig. 3. Circuit with Trojan

Only the Trojan affected pairs would tend to deviate from the straight line. In practice, few unaffected pairs may deviate slightly from the straight line implying different delays caused due to process variations. Such deviation is only due to intra-die variations as the inter-die variations have equal effects on all the paths within a die. Thus, each pair corresponds to one distance hence, we get N distances i.e $d_i, i \in \{1, 2...N\}$. Using these distances, we propose to compute a detection metric (DM), utilizing the concept of mathematical expectation in [5], as illustrated in (2).

$$DM = \sum_{i=1}^{N} \frac{d_i}{\sqrt{(P_1^{(i)})^2 + (P_2^{(i)})^2}} \tag{2}$$

Ideally, the DM should be zero for a Trojan free IC but because of the process variations the delays may slightly deviate from the expected straight line. Thus, we need to find some cut-off value, which we call as detection threshold (DT). The DT is decided on basis of Monte-Carlo simulations in the presence of process variations. The DM of each suspect IC is compared with the DT to decide whether the IC is affected by any Trojan. i.e if $DM > DT$ Trojan is present in IC, else Trojan is not present/detected. When the delays of paths in a pair are affected equally by the Trojan as well as remaining pairs are not affected, then proposed methodology is incapable to detect such Trojans and designing such Trojans is very difficult and not practical.

III. Simulation Results

We consider ISCAS-85 c17 benchmark circuit. The test vectors to measure the delay of each path are generated by employing single-input-change method. We implemented c17 circuit in 22nm Predictive Technology Model (PTM) CMOS technology and used HSPICE for simulation. The delays of paths in selected pairs in the Trojan free circuit are shown in Table-I. The notation BO235 represents the path from B to O through the gates numbered 2,3,5. The DM of Trojan free circuit is calculated using the data in Table-I and Eq. (1) & (2) to be 0.0225. Further, we have included process variation models as shown in Table-II. We have generated 100 Trojan free ICs using Monte-Carlo simulations and calculated the DM of each IC. The circles in Fig.4 show the DM of 100 Trojan free ICs. Using this data we have decided a DT as 0.5 by observation. Further, a non-functional Trojan of size two gates has been inserted into the circuit as shown in Fig.3 and measured delays of paths in three pairs are shown in Table-I. The DM of Trojan inserted circuit without process variations

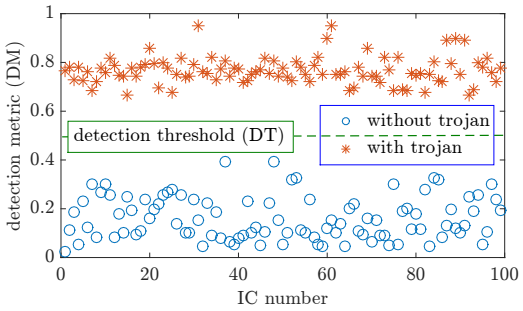

Fig. 4. Detection metric of 100 ICs with and without Trojan

TABLE I
DELAYS OF PATHS IN SELECTED PAIRS WITH AND WITHOUT TROJAN

Pair	Path	Path delay (psec)	
		with out Trojan	with Trojan
1	AO	10.8	23.4
	EP	10.8	10.8
2	BO235	18.7	28.5
	CP246	18.3	22.9
3	BO15	12.2	25.0
	DO	12.0	17.0

has been calculated as 0.7646. We have generated 100 Trojan inserted ICs and calculated the DM of each such IC. The stars in Fig.4 show the DM of 100 Trojan inserted ICs. As illustrated, the DM of all Trojan inserted ICs is above 0.5 in Fig.4.

TABLE II
PROCESS VARIATIONS CONSIDERED

Parameter/ Type	V_{th}	L	T_{ox}
Inter-die(3σ)	10%	10%	2%
Intra-die(3σ)	8%	8%	2%

IV. Conclusion

The proposed method can detect hardware Trojans without requiring a golden IC for reference and has been verified on a non-functional Trojan. This method employs a novel Detection Metric and is able to detect inserted Trojans by only measuring delays of few paths instead of all paths. The proposed methodology does not incur any design and hardware overhead. Further, we are in process of validating this method on larger benchmarks.

References

[1] M. Tehranipoor and F. Koushanfar, "A survey of hardware trojan taxonomy and detection," *IEEE Design and Test of Computers*, vol. 27, no. 1, pp. 10–25, 2010.

[2] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, and B. Sunar, "Trojan detection using IC Fingerprinting," in *Proceedings - IEEE Symposium on Security and Privacy*, 2007, pp. 296–310.

[3] Y. Yier, Jin and Makris, "Hardware Trojan Detection Using Path Delay Fingerprint," in *Proceedings of the 2008 IEEE International Workshop on Hardware-Oriented Security and Trust*, 2008, pp. 51–57.

[4] N. Gunti and K. Lingasubramanian, "Efficient Static Power Based Side Channel Analysis for Hardware Trojan Detection Using Controllable Sleep Transistors," in *SoutheastCon 2015*, 2015, pp. 1–6.

[5] Y. Zheng, S. Yang, and S. Bhunia, "SeMIA: Self-Similarity based IC Integrity Analysis," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 0070, no. 99, pp. 1–1, 2015.