ANP: A Self-Reference-Based Random Variation Aware Hardware Trojan Detection Method

Syful Islam, Michihiro Shintani, and Michiko Inoue
Nara Institute of Science and Technology, 8916-5 Takayama-cho, Ikoma 630-0192, Japan
{islam.syful.il4,shintani,kounoe}@is.naist.jp

***Abstract*—Obtaining high hardware Trojan (HT) detection sensitivity under large random process variation through side-channel parameter analysis is addressed in this paper. The impact of random variation on dynamic power per test pattern is first analyzed by establishing a Monte Carlo simulation environment. Based on the analysis, we propose a random process variation aware HT detection method ANP (Arbitrary neighboring test pattern pair comparison). The ANP is evaluated on ISCAS-89 benchmark circuits using both combinational and sequential HTs from Trust-Hub. Our experimental results show that the ANP achieves high (100%) detection sensitivity for some HTs with 0.3-0.4% HT-to-circuit ratio even in the presence of random process variation with 1-5% relative standard deviation for cell delays.**

***Index Terms*—Hardware Trojan (HT), Random process variation, Circuit partitioning, Self-referencing, Power-based side-channel analysis, HT Detectability.**

I. Introduction

Due to tremendous growth and recent outsourcing trends in the integrated circuit (IC) industries, malicious alternations like hardware Trojan (HT) have become a significant threat to IC security and reliability. Unfortunately, the detection of HT is very challenging for several reasons, such as nanometer IC feature sizes and system design complexity, etc. There exist several methods to detect HT. Among them, side channel analysis is one of the most promising technique, since it facilitates HT detection by reflecting partial activation effect of the HT circuits through the side-channel parameters.

However, the side-channel parameters deviate from their nominal values by process variations [1]. Process variation is classified into *inter-die systematic*, *intra-die systematic*, and *random* variations [2]. The recent increase in uncorrelated variability in ICs due to phenomena like random dopant fluctuation and line edge roughness causes random variations in threshold voltage which introduce the random delay variations in combinational logic circuits. Consequently, these uncorrelated delay variability produces transient behaviors which are referred to as glitches [3]. The increase in uncorrelated delay variability in circuit magnifies the variability of glitch activity and largely contributes to the variability of dynamic power. Thus, the dynamic power deviates from its nominal value which causes difficulty in identifying the HT effect through power-based side-channel analysis technique, and resulting in low detection sensitivity. Therefore, it is very essential to address random process variation in detecting HT.

In this paper, we present a method ANP (Arbitrary neighboring test pattern pair) to detect HT considering the random process variation. The major contributions of this work are summarized as follows:

- Establish a Monte Carlo simulation environment for analyzing dynamic power deviation due to random process variation.
- Propose the concept of arbitrary neighboring test patterns pair comparison for increasing the chance of HT detection in the presence of elevated random variation.
- Introduce the new HT detection condition through proper analysis on the effect of random process variation on dynamic power.
- The proposed ANP method achieves relatively high detectability for small size HTs with 0.3-0.4% HT-to-circuit ratios in the presence of random process variation. That drastically improves our previous methods [4]–[6].

The rest of the paper is organized as follows. Section II provides a brief description of the existing related works in detecting HTs. Section III describes the dynamic power variability analysis. Section IV describes the proposed random process variation aware ANP method. In section V, we discuss the evaluation of ANP method and compare its performance with our previous method EPN [5]. Finally, we present our conclusions in Section VI.

II. Related Work

There exist several methods based on side-channel parameters, such as delay, current, and power, to detect HTs. These methods can be broadly classified into two categories; golden IC dependent and golden IC free methods.

As a golden IC dependent method, the IC fingerprinting concept using several side-channel signals is introduced in [7], where a destructive analysis to validate a golden IC is supposed. In [8], [9], segmentation is done for the whole design by creating many small regions to detect HTs more effectively. Random test patterns are used in [8], while test patterns for transition delay faults are used to activate more cells in [9]. All the methods mentioned above are golden IC dependent, therefore they are highly affected by process variation noise since they are affected by inter-die variation, which is the most dominant variation source. Also, it is practically difficult to provide Trojan-free golden IC. This is another problem for golden IC dependent methods.

To overcome the challenge imposed by golden IC dependency, golden IC free HT detection methods are proposed [4]–[6], [10]. A structural self-similarity blocks based analysis

is presented in SeMIA [10]. This method partitions circuits by functionally similar blocks and activates two adjacent blocks to compare within the chip. The dynamic currents are compared between two identical structures and the deviation due to the HT attacks are observed. As blocks are functionally partitioned, this method depends on the structure of the circuit.

Self-referencing HT detection using clock tree based segmentation is proposed in [4]–[6], where segmentation is realized by gating clock buffer in a clock tree with a little area overhead. Since the method partitions a whole circuit into segments, it is a structure-independent golden IC free HT detection method. An inter-die variation aware self-referencing HT detection method EP is proposed in [4], and it is extended to handle intra-die systematic variation, called EPN (equal power test pattern pair in neighboring segments comparison), in [5]. In EPN, HT is detected if two test patterns with equal nominal power exhibit enough different powers in measurement. The method eliminates the effect of inter-die variation since two measured powers from the same chip are compared, and it diminishes the effect of intra-die variation since two measured power from neighboring regions are compared. However, it does not well address random variation. It is considered that random variation affects transistors randomly and it is canceled out if an adequate number of cells are activated.

Side-channel aware test generation methods are also investigated [11], [12]. Considering the stealthy nature of HT, these methods address to improve the relative activity of rarely triggered nodes to a whole circuit. Several statistical analyses are proposed for HT sensitivity.

To the best of our knowledge, none of the side-channel based HT methods properly address random variation. In this research, we start with an analysis of random variation effect on dynamic power variation and propose a random process variation aware HT detection method ANP (Arbitrary Neighboring test pattern Pair comparison).

III. Analysis of Dynamic Power Distribution

To address random process variation in HT detection, analysis of dynamic power variation due to random process variation is essential. The purpose of this analysis is to understand the variability of test patterns due to random variation. We analyze the test patterns used in EPN [5].

A. EPN

We briefly explain EPN used in our analysis. EPN partitions a circuit into segments based on a clock tree with two steps. In the first step, initial partitioning is obtained by assigning gating points to clock buffers, where each segment is realized by activating a part of clock buffers. In the second step, dynamic powers for segments are adjusted by FF shifting across segments to get more equal power test pattern pairs. In the test pattern generation part, transition delay fault test patterns set is adopted to toggle more cells.

In a detection phase, one segment (a group of FFs) is activated at a launch-capture cycle in a launch-on-capture test scheme. A set of cells activated at a launch-capture cycle is called *a region*, and a power consumed by the region is measured. HT is detected if test pattern pair (a test pattern includes information of associated segment) with equal nominal power from neighboring segments exhibit enough different measured powers. Fig. 1 shows an example of a pair of two test patterns t_i and t_j, where two regions R_i and R_j in neighboring segments are activated and their powers are compared.

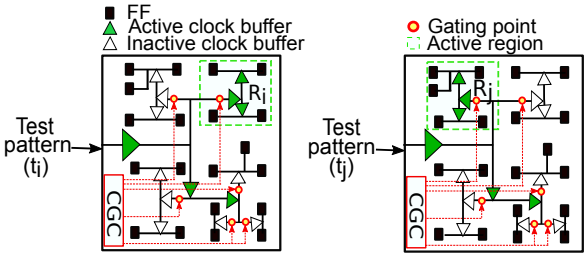


Fig. 1. HT detection using measured power difference.

TABLE I
Benchmark Circuits

Circuits	# of FFs	# of cells	area (μm^2)	# of segments	# of test patterns
s35932	1728	3133	101,543	10	433
s38417	1564	3455	94,562	10	1000
s38584	1172	3982	80,108	7	260

B. Analysis

We applied the clock-tree based circuit partitioning [5] to the ISCAS'89 benchmark circuits to obtain final segments. Afterward, Monte Carlo simulation and best-fit distribution finding are performed to analyze dynamic power. Table I shows the summary of the benchmark circuits and test patterns used in [5]. The circuits are synthesized using commercial logic synthesis and place-and-route tools with a 90 nm technology library.

Monte Carlo simulation on timing and power analysis is with test patterns for each circuit and variation case conducted using commercial power analyzer and Verilog simulator as shown in Fig. 2. Each simulation is performed by annotating additional delays with $n\%$ (n = 1, 2.5, and 5) relative standard deviation to the nominal delays for all the cells in a standard delay format (SDF) file. Simulation is repeated 1000 times for each circuit and variation case (a value of relative standard deviation) and 1000 dynamic power values are obtained for each test pattern and each simulation case.

To know the distributions of dynamic power values obtained from the Monte Carlo simulation, the Kolmogorov-Smirnov test is applied for 10 different distributions (normal, log-normal, alpha, beta, power log-normal, power normal, triangle, log Laplace, log gamma, Gumbel_r, etc.). Then, the best fit distribution is obtained based on the P-value.

Fig. 3 shows the distributions of dynamic powers for test pattern-21 and 22 in segment-1 of s35932. It is observed that two distributions follow normal and beta distributions, respectively with different deviations. Table II shows the overall results of the analysis using test pattern distribution count for all segments of the benchmark circuits. Different test patterns

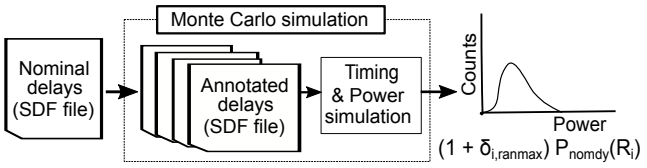
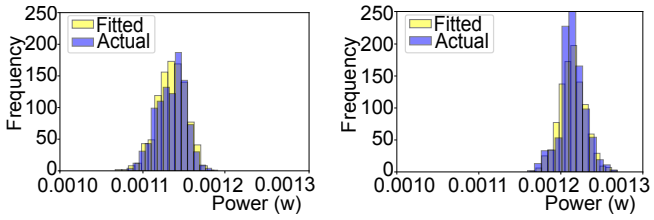


Fig. 2. Monte Carlo simulation process.



(a) Test pattern-21 (Normal) (b) Test pattern-22 (Beta)

Fig. 3. Distribution of test patterns for segment $S1$ of s35932 circuit.

are differently affected by random process variation, and we could not find any unified distribution to model dynamic power variation.

IV. Proposed ANP Method

Motivated by the analysis, we propose an HT detection method ANP to detect HT in the presence of random process variation. The proposed ANP compares all possible combinations of test patterns in neighboring segments. In addition, to derive the detection threshold, we again use Monte Carlo simulation that we developed for preliminary analysis in Section III.

A. Comparison of Arbitrary Test Pattern Pair

Comparison between the arbitrary test pattern pairs is useful in random variation since a comparison between a test pattern which is less affected by random variation and a test pattern which activates (a part of) HT has a higher chance of detection of the HT. Fig. 4 illustrates this concept.

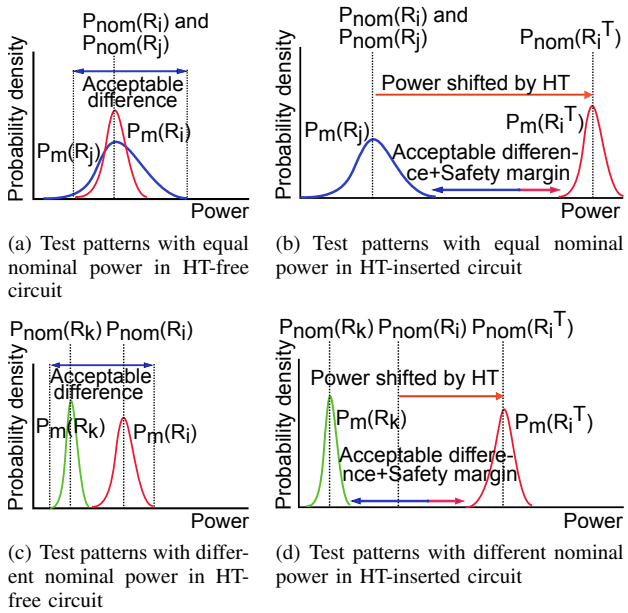
Let t_i, t_j, and t_k be test patterns applied in some neighboring segments and $P_m(R_i)$, $P_m(R_j)$ and, $P_m(R_k)$ be the corresponding measured powers, respectively. Here, t_i and t_j have equal nominal power values while t_k hasdifferent value. Also, the dynamic power variations for t_i, t_j, and t_k are medium, large, and small, respectively, as illustrated in Fig. 4(a) for t_i and t_j and Fig. 4(c) for t_i and t_k. Assume that a test pattern t_i activates an HT.

For the equal power pair t_i and t_j, their acceptable difference is also shown in Fig. 4(a). If HT shifts the power of t_i as shown in Fig. 4(b), we can detect HT by comparing measured power values. However, for the HT to be detected, a large power shift is required.

On the other hand, in case of a test pattern pair t_i and t_k, now t_k has a small variation with different nominal power. Their acceptable measured power difference shown in Fig. 4(c) is smaller compared to a pair of t_i and t_j. Hence to detect the HT, it is enough to shift power as shown in the Fig. 4(d).

TABLE II
Summary of test pattern distribution due to random variation

List of distributions	2.5% random variation			5% random variation		
	s35932	s38417	s38584	s35932	s38417	s38584
Normal	1152	3017	996	353	1646	610
Log normal	127	379	36	160	501	72
Beta	397	1294	197	1350	1799	354
Alpha	373	923	67	184	1146	89
Power log normal	599	1148	127	789	1514	182
Power normal	529	842	175	1106	932	220
Triangular	70	218	22	7	286	31
Log Laplace	0	0	0	0	0	0
Log gamma	690	1362	123	248	1175	151
Gumbel_r	393	817	77	133	1001	111



(a) Test patterns with equal nominal power in HT-free circuit

(b) Test patterns with equal nominal power in HT-inserted circuit

(c) Test patterns with different nominal power in HT-free circuit

(d) Test patterns with different nominal power in HT-inserted circuit

Fig. 4. The concept of ANP in random process variation perspective.

The above observation implies that the arbitrary test pattern pair comparison provides a higher possibility to detect smaller HT than the case where comparison is restricted among test patterns with equal nominal power values.

B. Method

For improving the HT detection sensitivity under large random process variation, we propose ANP enhances the probability of detecting small HT successfully. To develop the ANP method, we assume that the electronic design automation (EDA) flow is trusted but the fabrication of chip at the foundry is untrusted. The overview of the proposed ANP method is illustrated in Fig. 5. The ANP has two major parts; the design phase and the detection phase.

1) Design Phase: In the design phase, there are three parts; clock tree based circuit partitioning, test pattern generation and Monte Carlo simulation. For a given circuit with the layout information, a clock tree-based circuit partitioning and a test pattern generation are applied. In our method, we adopt only the first step of the clock-tree based partitioning [4] and we does not require FF shifting, since ANP compares the arbitrary test pattern pairs and does not need to unify dynamic powers

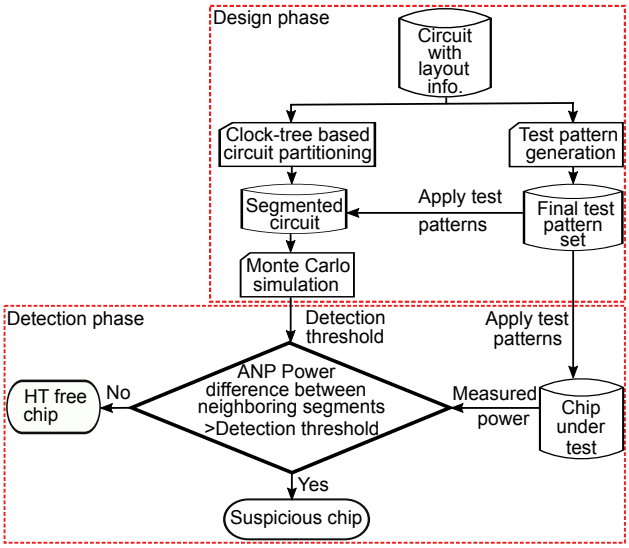


Fig. 5. Overview of ANP method.

among segments. Finally, Monte Carlo simulation is performed by applying the final test pattern set to the segmented circuit to obtain dynamic power deviation due to random variation with $n\%$ relative standard deviation for transistor delays. The detection threshold is derived by comparing test patterns arbitrarily in neighboring segments.

2) HT Detection Phase: In the detection phase, the test patterns are applied to the chip under test (CUT) to obtain the measured power per test pattern. Then, the measured power values from within two neighboring segments are compared, where we compare measured powers not only from two neighboring segments but also from the same segment. It is expected that the measured power difference for HT free circuit will be less than or equal to the acceptable difference imposed by process variations with some safety margin. We consider such value as a *detection threshold*. An HT in region R_i can be effectively detected if the measured power difference exceeds the detection threshold.

C. Detection Threshold

The test patterns comparison in two neighboring segments within the same chip diminishes the inter-die variation and intra-die systematic variation effects. while the random variation effect is independent of the region of a circuit. A mathematical analysis will help us appropriately account for inter-die variation, intra-die systematic, and random variation effects to accurately detect HT.

Consider two test patterns t_i, t_j are applied and the associated activated regions are R_i, R_j, respectively as shown in Fig. 1. Let $P_m(R_i)$ and $P_m(R_j)$ be the measured power of region R_i and R_j, respectively.

Let $P_{nom\_Dy}(R_i)$ and $P_{nom\_Dy}(R_j)$ denote the nominal dynamic power when activating region R_i and R_j, respectively. We assume the nominal value of leakage powers are equal and independent of the particular test pattern for whole circuit (C). Let us assume that the measured power $P_m(R_i)$ differs from its nominal power with factors of inter-die variation δ_{inter}, intra-die systematic variation $\delta_{i,intra\_sys}$, and random variation $\delta_{i,ran}$ for dynamic power and a factor of θ_{inter} for leakage power. Thus, the measured power for region R_i can be written as follows:

$$\begin{aligned} P_m(R_i) =& (1+\delta_{inter}+\delta_{i,intra\_sys}+\delta_{i,ran})P_{nom\_Dy}(R_i) \\ &+ (1+\theta_{inter})P_{nom\_leak}(C) \end{aligned}$$

The measured power difference can be derived as follows:

$$\begin{aligned} & P_m(R_i) - P_m(R_j) \\ &= (1+\delta_{inter}+\delta_{i,ran})P_{nom\_Dy}(R_i) \\ &\quad - (1+\delta_{inter}+\delta_{j,ran})P_{nom\_Dy}(R_j) \\ &\quad + \delta_{i,intra\_sys}P_{nom\_Dy}(R_i) - \delta_{j,intra\_sys}P_{nom\_Dy}(R_j) \end{aligned}$$

Now, let us define that the last term can be written as:

$$\begin{aligned} & (\delta_{i,intra\_sys}P_{nom\_Dy}(R_i) - \delta_{j,intra\_sys}P_{nom\_Dy}(R_j)) \\ &= \delta_{i,j,intra\_sys}Mean(P_{nom\_Dy}(R_i), P_{nom\_Dy}(R_j)), \end{aligned}$$

using a correlation factor of intra-die systematic variation. Here, $Mean()$ is a function to return a mean value. Hence for HT free circuit, the measured power difference will be derived as follows:

$$\begin{aligned} & P_m(R_i) - P_m(R_j) \\ &= (1+\delta_{i,ran})P_{nom\_Dy}(R_i) \\ &\quad - (1+\delta_{j,ran})P_{nom\_Dy}(R_j) \\ &\quad + \delta_{inter}(P_{nom\_Dy}(R_i) - P_{nom\_Dy}(R_j)) \\ &\quad + (\delta_{i,j,intra\_sys})Mean(P_{nom\_Dy}(R_i), P_{nom\_Dy}(R_j)) \end{aligned}$$

Let α_{inter} and $\alpha_{i,j,intra\_sys}$ denote the worst case deviation of δ_{inter} and $\delta_{i,j,intra\_sys}$, assumed $3\sigma_{inter}$ and $3\sigma_{i,j,intra\_sys}$ in this paper, where σ_{inter} and $\sigma_{i,j,intra\_sys}$ are the normal distributions of δ_{inter} and $\delta_{i,j,intra\_sys}$, respectively. We assume these distributions follow the normal distribution. On the other hand, from the analysis we found that dynamic power deviation due to random variation effect does not follow any specific distribution. Therefore, we obtain the worst case factors α_{i,ran_max} and α_{j,ran_min} for the maximum and minimum values of $\delta_{i,ran}$, respectively, from the Monte Carlo simulation. Let $P_{i,max}$ and $P_{i,min}$ denote the maximum and minimum dynamic powers of patterns t_i obtained from Monte Carlo simulation, respectively. The worst case factors are derived as follows:

$$\alpha_{i,ran\_max} = \frac{P_{i,max} - P_{nom\_Dy}(R_i)}{P_{nom\_Dy}(R_i)}$$

$$\alpha_{i,ran\_min} = \frac{P_{i,min} - P_{nom\_Dy}(R_i)}{P_{nom\_Dy}(R_i)}$$

If the measured power difference exceeds an acceptable difference, HT can be doubted. Finally, considering β as a safety margin, we derive the detection threshold $TH(i,j)$. Since we are comparing test pattern pair (t_i, t_j) in arbitrary level, one test pattern may have higher dynamic power than

TABLE III
HT-TO-CIRCUIT RATIO (%)

HT	circuit		
	s35932	s38417	s38584
T1	0.073	0.080	0.094
T2	0.341	0.368	0.429

another. Hence, the detection threshold will have two possible cases.

$$
\begin{aligned}
&Case\_1 : P_{nom\_Dy}(R_i) \geq P_{nom\_Dy}(R_j) \\
&P_m(R_i) - P_m(R_j) \\
&\quad + \beta Mean(P_{nom\_Dy}(R_i), P_{nom\_Dy}(R_j)) \\
&\leq (1 + \alpha_{i,ran\_max}) P_{nom\_Dy}(R_i) \\
&\quad - (1 + \alpha_{j,ran\_min}) P_{nom\_Dy}(R_j) \\
&\quad + \alpha_{inter}(P_{nom\_Dy}(R_i) - P_{nom\_Dy}(R_j)) \\
&\quad + (\alpha_{i,j,intra\_sys} + \beta) Mean(P_{nom\_Dy}(R_i), P_{nom\_Dy}(R_j)) \\
&= TH(i,j)
\end{aligned}
$$

$$
\begin{aligned}
&Case\_2 : P_{nom\_Dy}(R_i) \leq P_{nom\_Dy}(R_j) \\
&P_m(R_i) - P_m(R_j) \\
&\quad + \beta Mean(P_{nom\_Dy}(R_i), P_{nom\_Dy}(R_j)) \\
&\leq (1 + \alpha_{i,ran\_max}) P_{nom\_Dy}(R_i) \\
&\quad - (1 + \alpha_{j,ran\_min}) P_{nom\_Dy}(R_j) \\
&\quad - \alpha_{inter}(P_{nom\_Dy}(R_i) - P_{nom\_Dy}(R_j)) \\
&\quad + (\alpha_{i,j,intra\_sys} + \beta) Mean(P_{nom\_Dy}(R_i), P_{nom\_Dy}(R_j)) \\
&= TH(i,j)
\end{aligned}
$$

V. EXPERIMENTAL EVALUATION

Our proposed ANP is evaluated for the benchmark circuits shown in Table I. In our experiment, we utilize two HT T1 (s38417-T200) and T2 (s15850-T100) which are extracted from Trust-Hub [13], [14]. Here, T1 is a combinational HT that consists of 11 elements (4 NOR gates, 3 AND gates, and 8 OR gates) and T2 is a sequential HT which consists of 26 elements (23 AND gates, 2 D-FFs, and 1 inverter). Table III shows the HT-to-circuit ratios for these HTs.

The HTs are inserted in each segment of a circuit, that is, we inserted HT in s ways if the circuit has s segments. Let Sq-T1 and Sq-T2 denote the HTs inserted in segment Sq, respectively. Fig. 6 shows the HT insertion scenario in each segment of a circuit. The HT inputs are connected with signals that meet the rare trigger condition of the HT (e.g., if HT is triggered with input signals of 1, the HT is connected with signals with low 1-controllability.) We use SCOAP (Sandia controllability/observability analysis program) [15] value for this purpose. After inserting HT in each segment of a circuit, 100 sample circuits are created for Monte Carlo simulation for each of $n\%$ (1%, 2.5%, and 5%) relative standard deviation for cell delay. For the sake of fair comparison between EPN [5] and ANP, we use the same number of segments and the test pattern sets as shown in Table I.

We injected inter-die, intra-die systematic, and random variation for each sample circuit as follows, and obtained

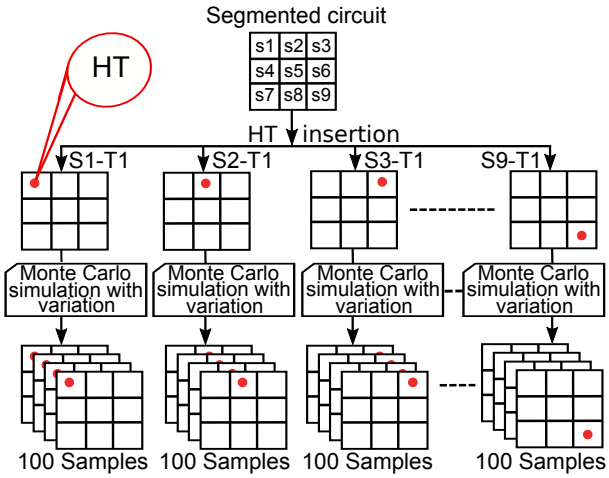


Fig. 6. HT insertion scenario in each segment of circuit.

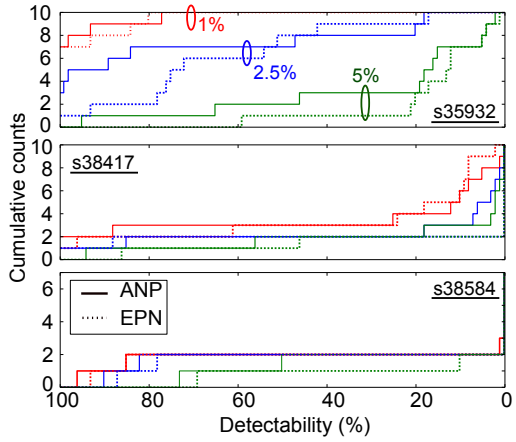
TABLE IV
CASE: ANP SHOWS HIGHER DETECTABILITY (%)

circuit	HT	1% random		2.5% random		5% random	
		EPN	ANP	EPN	ANP	EPN	ANP
s35932	S1-T2	100	100	78	99	12	16
	S3-T2	100	100	72	100	12	65
	S8-T2	100	100	75	100	13	95
s38417	S6-T2	2	25	0	18	0	18
	S10-T2	100	100	100	100	86	94
	S10-T1	33	100	0	3	0	0
s38584	S5-T2	80	85	78	82	10	50
	S7-T1	0	3	0	0	0	0

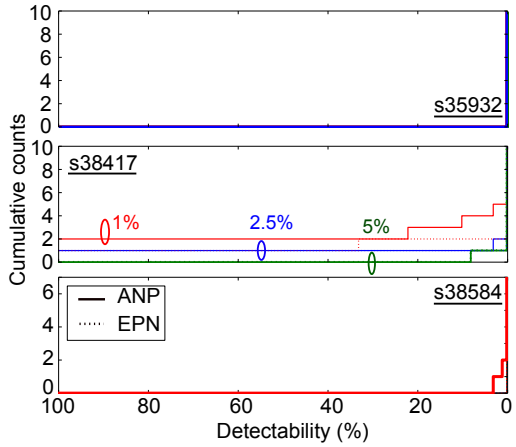
measured power values through logic and power simulation. We consider the inter-die relative standard delay deviation σ_{inter} as 5%. The standard deviation of intra-die correlated factor $\sigma_{i,j,intra\_sys}$ is set to 0.135% when selecting two patterns from neighboring segments, while it is set as 0% when selecting them from the same segment. In addition, a safety margin β is taken as 10%. The worst-case deviation factors due to random deviation are obtained by Monte Carlo simulation with 1,000 HT-free samples for each test pattern with $n\%$ (n=1, 2.5, and 5) relative standard deviation for cell delays. A detectability is evaluated as a ratio of the HT inserted circuits in which some measured power difference exceeds its detection threshold, that is, the HT is detected.

Table IV shows the cases where ANP achieves higher detectability than EPN. For some HTs (S3-T2 and S8-T2 in s35932, S5-T2 in s38584), ANP achieves relative high detectability for high random variation, while detectability drastically decreases as random variation increases in EPN. Table V shows the cases where ANP shows lower detectability, and EPN shows slightly higher detectability.

Finally, the comparisons of the HT detectability between the ANP and EPN for all the segments are given as shown in Fig. 7 for HTs T2 and T1, respectively. In the figure, the x-axis represents the HT detectability in reverse order, i.e., 100% to 0%, and the y-axis represents the cumulative counts of the detected HTs for three benchmark circuits (s35932, s38417,



(a) T2



(b) T1

Fig. 7. Detectability comparison between EPN and ANP method.

TABLE V
CASE: ANP SHOWS LOWER DETECTABILITY (%)

circuit	HT	1% random		2.5% random		5% random	
		EPN	ANP	EPN	ANP	EPN	ANP
s35932	S4-T2	80	77	51	18	4	2
	S10-T2	93	93	42	20	20	5
s38417	S8-T2	18	12	0	2	0	2
	S9-T2	24	10	0	0	0	0

s38584). For T2, ANP achieves high detectability for most segments at 1% relative standard deviation for random delays while EPN has lower detectability as random process variation increases. Though T1 has low detectability for both ANP and EPN, ANP can detect more HTs in some cases (s38417, 1% relative standard deviation for random delays).

VI. CONCLUSION

In this paper, we presented a self-referenced based random process variation aware HT detection technique through power-based side-channel analysis. We introduced a concept of arbitrary neighboring test pattern pair comparison and proposed an HT detection method ANP to enhance HT detection sensitivity in presence of elevated random variation. HT detection condition for arbitrary test pattern pair comparison was also developed in this paper. Finally, comparisons between ANP and the previous method EPN showed that our ANP can detect small size HT more effectively than EPN even in the presence of an elevated level of random process variation. It is noted that the proposed ANP slightly modifies the original circuit so that some of clock buffers can be gated. This is a different point from EPN, where the connection of FFs and clock tree is adjusted to enhance HT detectability. Since ANP does not change the original layout, it has minimal impact to the circuit performance.

ACKNOWLEDGEMENT

The research has been partly executed in response to support of KIOXIA Corporation (former Toshiba Memory Corporation).

REFERENCES

[1] S. Bhunia, M. S. Hsiao, M. Banga, and S. Narasimhan, "Hardware Trojan attacks: threat analysis and countermeasures," *Proc. of the IEEE*, vol. 102, no. 8, pp. 1229–1247, 2014.

[2] P. A. Stolk, F. P. Widdershoven, and D. B. M. Klaassen, "Modeling statistical dopant fluctuations in MOS transistors," *IEEE Trans. on Electron Devices*, vol. 45, no. 9, pp. 1960–1971, 1998.

[3] D. Kamel, C. Hocquet, F.-X. Standaert, D. Flandre, and D. Bol, "Glitch-induced within-die variations of dynamic energy in voltage-scaled nano-cmos circuits," in *Proc. of European Solid-State Circuits Conference*, 2010, pp. 518–521.

[4] F. S. Hossain, T. Yoneda, M. Inoue, and A. Orailoglu, "Detecting hardware Trojans without a golden ic through clock-tree defined circuit partitions," in *Proc. of IEEE European Test Symposium*, 2017, pp. 1–6.

[5] F. S. Hossain, T. Yoneda, M. Shintani, M. Inoue, and A. Orailoglu, "Intra-die-variation-aware side channel analysis for hardware Trojan detection," in *Proc. of IEEE Asian Test Symposium*, 2017, pp. 52–57.

[6] F. S. Hossain, M. Shintani, M. Inoue, and A. Orailoglu, "Variation-aware hardware Trojan detection through power side-channel," in *Proc. of IEEE International Test Conference*, 2018.

[7] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, and B. Sunar, "Trojan detection using IC fingerprinting," in *Proc. of IEEE Symposium on Security and Privacy*, 2007, pp. 296–310.

[8] M. Banga and M. S. Hsiao, "A region based approach for the identification of hardware Trojans," in *Proc. of IEEE International Symposium on Hardware Oriented Security and Trust*, 2008, pp. 40–47.

[9] F. S. Hossain, T. Yoneda, and M. Inoue, "An effective and sensitive scan segmentation technique for detecting hardware Trojan," *IEICE Trans. on Information and Systems*, vol. 100, no. 1, pp. 130–139, 2017.

[10] Y. Zheng, S. Yang, and S. Bhunia, "SeMIA: Self-similarity-based ic integrity analysis," *IEEE Trans. on Computer-Aided Design of Integrated Circuits and Systems*, vol. 35, no. 1, pp. 37–48, 2015.

[11] R. S. Chakraborty, F. Wolff, S. Paul, C. Papachristou, and S. Bhunia, "MERO: A statistical approach for hardware trojan detection," in *Proc. of Conference on Cryptographic Hardware and Embedded Systems*, 2009, pp. 396–410.

[12] Y. Huang, S. Bhunia, and P. Mishra, "MERS: statistical test generation for side-channel analysis based Trojan detection," in *Proc. of ACM Conference on Computer and Communications Security*, 2016, pp. 130–141.

[13] H. Salmani, M. Tehranipoor, and R. Karri, "On design vulnerability analysis and trust benchmarks development," in *Proc. of IEEE International Conference on Computer Design*, 2013, pp. 471–474.

[14] B. Shakya, T. He, H. Salmani, D. Forte, S. Bhunia, and M. Tehranipoor, "Benchmarking of hardware Trojans and maliciously affected circuits," *Journal of Hardware and Systems Security*, vol. 1, no. 1, pp. 85–102, 2017.

[15] L. H. Goldstein and E. L. Thigpen, "SCOAP: Sandia controllability/observability analysis program," in *Proc. of IEEE/ACM Design Automation Conference*, 1980, pp. 190–196.