Hindawi Publishing Corporation
VLSI Design
Volume 2014, Article ID 652187, 11 pages
http://dx.doi.org/10.1155/2014/652187

Research Article

Efficient Hardware Trojan Detection with Differential Cascade Voltage Switch Logic

Wafi Danesh, Jaya Dofe, and Qiaoyan Yu

Department of Electrical and Computer Engineering, University of New Hampshire, Durham, NH 03824, USA

Correspondence should be addressed to Qiaoyan Yu; qiaoyan.yu@unh.edu

Received 26 February 2014; Accepted 7 April 2014; Published 11 May 2014

Academic Editor: Chih-Cheng Lu

Offshore fabrication, assembling and packaging challenge chip security, as original chip designs may be tampered by malicious insertions, known as hardware Trojans (HTs). HT detection is imperative to guarantee the chip performance and safety. Existing HT detection methods have limited capability to detect small-scale HTs and are further challenged by the increased process variation. To increase HT detection sensitivity and reduce chip authorization time, we propose to exploit the inherent feature of differential cascade voltage switch logic (DCVSL) to detect HTs at runtime. In normal operation, a system implemented with DCVSL always produces complementary logic values in internal nets and final outputs. Noncomplementary values on inputs and internal nets in DCVSL systems potentially result in abnormal power behavior and even system failures. By examining special power characteristics of DCVSL systems upon HT insertion, we can detect HTs, even if the HT size is small. Simulation results show that the proposed method achieves up to 100% HT detection rate. The evaluation on ISCAS benchmark circuits shows that the proposed method obtains a HT detection rate in the range of 66% to 98%.

1. Introduction

The growing number of ICs manufactured offshore increases the threats to chip security [1–3]. Research has exposed an increase in existence of hardware Trojans (HTs), which are malicious additions or modifications to the circuit design that alter the original function. Malicious inclusions of hardware have the potential to degrade system performance, surreptitiously delete data, leave a backdoor for secret key leaking, or eventually destroy the chip [4, 5]. It is imperative to detect HTs.

HTs can be detected by destructive approaches such as the chemical mechanical polishing (CMP) method. The CMP approach detects HTs by analyzing pictures of the demetalized chips under an electron microscope [6]. In addition to being expensive, this type of technique is also time consuming (takes several months) and loses its efficiency when the transistor density increases. Nondestructive HT detection methods are broadly classified into two categories: logic testing and side-channel analysis (SCA) approaches [6]. Automatic test pattern generation (ATPG) approaches examine whether the measured outputs match the expected one for given inputs and work well for a functional unit with a small set of inputs, as the probability of rare events is relatively high. When the circuit complexity increases, the number of test vectors for ATPG will significantly increase to an unaffordable degree. The benefits relative to the testing efforts of ATPG become worse if the input nodes for the HT's trigger circuit are spread out throughout the system. The main challenge with logic testing approaches [7, 8] is the generation of stimulus for sequential HTs. Voltage inversion technique alternates supply voltage and ground grids in CMOS-based functional blocks to change the original logic function and thus increases the HT trigger probability [9]. Dummy flip-flops are inserted into the design to increase transition probability of particular paths and reduce Trojan activation time [10]. Alkabani [11] introduces the concept of creating dual circuits for a given design. By testing the dual with a few random input vectors, a HT inserted in the original design can be detected.

SCA approaches examine the anomalous behavior (resulting from HTs) in system parameters such as transient current, power, and path delay [12–15]. A multiple-parameter

side-channel analysis method and a platform are developed to reliably test, analyze, and detect a wide range of HTs for both combinational and sequential designs [14]. Recently, HT detection approaches rely on multiple-parameter side-channel analysis technique, which can be integrated with statistical logic testing in order to improve the detection of HTs with very small design area [16]. SCA-based methods [17, 18] achieve a high coverage and are effective for finding HTs that span a large area of a system. However, the sensitivity of SCA-based methods is challenged by the increasing process variation [16, 19]. False detection on small HTs can happen when process variation effects exceed the signal threshold (e.g., power) for side-channel analysis.

To address the challenge from process variation on HT detection, region-based approach [4] magnifies the region potentially affected by HTs and forces the remaining regions to be inactive. Postsilicon spatial thermal and power maps are simultaneously utilized in a multimodal characterization procedure to improve the HT detection sensitivity [13]. A unified framework combines different HT detection methods in a systematic analysis platform, which studies the impact of small HTs [20].

In this work, we propose a method to remove the need of golden design for comparison and detect small HTs at runtime. The difference with other side-channel analysis approaches is that our method focuses on enhancing the side-channel signals by using a logic family's inherent characteristics. We exploit the special characteristic of differential cascade voltage switch logic (DCVSL) to detect HTs. Trojan detection using DCVSL can be performed using the constant, abnormal power consumption peaks, or erroneous outputs. The method is inexpensive as there is no extra hardware overhead required in order to implement the HT detection platform. Simulation results show that the power consumption of a DCVSL system with a HT triggered is constantly three orders of magnitude higher than that of the system with inactive HTs. This unique, abnormal power consumption phenomenon complements existing power-based side-channel analysis methods.

The remainder of this work is organized as follows. In Section 2, we highlight the basis for abnormal power consumption in DCVSL and introduce the proposed HT detection method. In Section 3, we thoroughly evaluate the area, power, and HT detection rate of our method in full adders and ISCAS benchmark circuits. Conclusions and future work are provided in Section 4.

2. Proposed DCVSL-Based HT Detection Method

2.1. Method Overview. HT detection is typically carried out during test stages, when numerous test vectors are simultaneously applied to both the device under test (DUT) and a golden reference. As it is difficult to obtain a golden version, the behavioral model is often used as a reference. Because of the effects of process variation and imperfect device libraries for computer-aided design tools, a behavioral model based golden version is not precise enough to detect small and ultrasmall HTs. Moreover, due to the demand of short time-to-market, the verification and testing period has been reduced significantly. Although it is always desired, thorough testing is not economically feasible. It is imperative to develop a HT detection method that is not limited by the HT size and does not take very long time to perform chip testing and authorization.

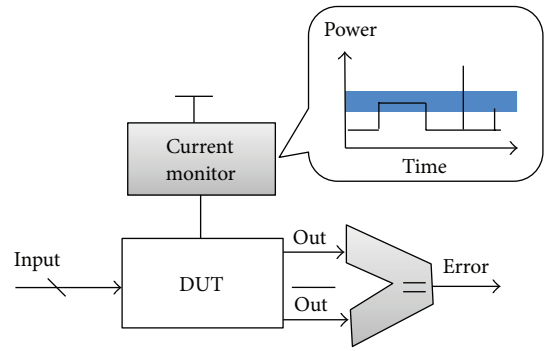

Figure 1: Proposed HT detection system.

We propose a HT detection method that allows users to detect potential HTs *at runtime* and *without a golden reference*. The proposed method exploits the abnormal instantaneous power for DUT to detect small HTs. Figure 1 shows the overview of the proposed method. Given a stable supply voltage, we examine the current through the current monitor for abnormal power behavior. A notable difference with offline power-based side-channel analysis methods is that we are not interested in a particular power value; instead, the current monitor detects the current (we can interpret it to power consumption) staying at a constant high value for a relatively long duration. As shown in Figure 1, the current monitor will trigger an alarm circuit, when the power value falls in and remains in the blue shadow region for a relatively long period. This duration is comparable with the duration of an input vector, rather than input rising and fall times. The triggered HT in the DUT causes the abnormal power period. We propose to implement DUTs with DCVSL, which always produces Out and Out bar, a pair of complementary outputs. Such complementary outputs will be used as inputs for next stage. In DCVSL, noncomplementary inputs (invalid inputs) result in short-circuit power remaining for a long period of time until the noncomplementary inputs disappear.The proposed method exploits this inherent feature of DCVSL to detect the presence of HTs.

Besides power detection, the proposed method further examines the complementary characteristic of the output pair, Out and Out bar. The noncomplementary output pair indicates a potential hardware Trojan insertion in the DUT. These noncomplementary outputs can be utilized for HT detection when no abnormal power values appear due to the HT being triggered.

The current monitor is connected with the DUT on a separate platform at the user end. If the current monitor is integrated on the same chip with the DUT, this potentially leaves an opportunity for an attacker to tamper or remove

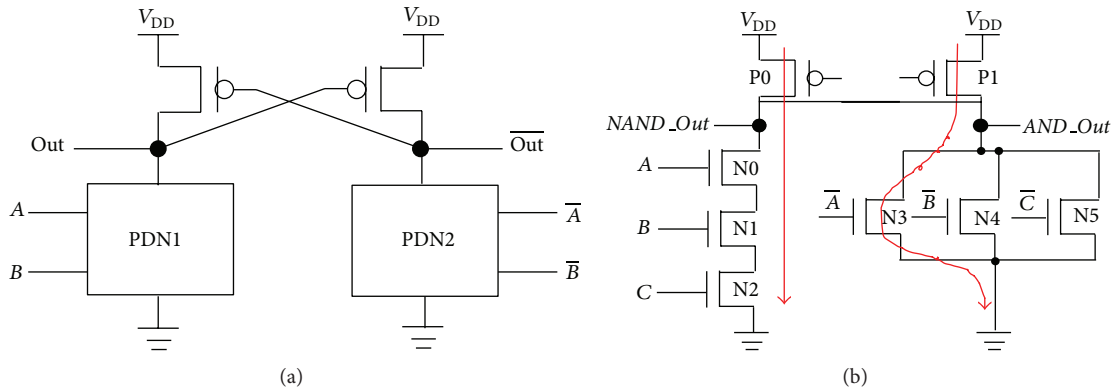

FIGURE 2: DCVSL logic gates. (a) General gate structure and (b) circuit schematic of NAND3-AND3. Current track highlighted in the figure is for noncomplementary inputs on A and $\overline{A}$.

the HT detection mechanism. A current sensor is needed to convert the transient current of the DUT and produce an analog voltage that is proportional to the measured DUT current. A programmed microcontroller can sample the analog voltage signal at specific intervals using interrupts. When the voltage value stays approximately constant for multiple interrupts, it indicates an abnormal short-circuit power due to a HT creating a short-circuit path from supply voltage V_{DD} to ground. The microcontroller can be further configured to set off an alarm or trigger a light-emitting diode to indicate HT detection to the user.

2.2. Short-Circuit Power-Based HT Detection

2.2.1. Unique Short-Circuit Power in DCVSL. Each DCVSL gate needs complementary inputs and produces complementary outputs [21], as shown in Figure 2(a). In normal operation, short-circuit power consumption of DCVSL gate is close to that of CMOS logic gate, as the time period for the direct current path from V_{DD} to ground is extremely short compared with that in switching and steady state conditions.

When the input pair is noncomplementary (both inputs being either logic 0 or logic 1), a DCVSL gate loses its complementary nature. More specifically, the output pair may be noncomplementary, resulting in the short-circuit power consumption lasting for a significantly longer time than the case with complementary inputs.

Take a 3-input NAND-AND gate as an example. The circuit schematic is shown in Figure 2(b). In normal operation conditions, we give the input vector of $A = B = C = 1$ and $\overline{A} = \overline{B} = \overline{C} = 0$. The *NAND_Out* port is pulled down to logic low through NMOS transistors N0, N1, and N2; this in turn activates PMOS transistor P1. As P1 is turned on, the *AND_Out* node is pulled to logic high and thus P0 is turned off. The time period when both PMOS and NMOS transistors are on is extremely short. Let us reconsider the 3-input NAND-AND gate with the same input vector, except that we make $A = \overline{A} = 1$. Now, there exist two paths from V_{DD} to the ground terminal: one is through N0, N1, and N2 and another one is through N3. The path through N0, N1, and N2 pulls the *NAND_Out* port low as before, which turns on P1. P1 then tries to pull the *AND_Out* port high. At the same time, the path to ground through N3 tries to pull the *AND_Out* node low. If N3 is stronger than P1 (which is typically the case), the *AND_Out* port is pulled low and this activates P0. Therefore, a path from V_{DD} to ground is created through P0, N0, N1, and N2, resulting in a *high* and *constant* short-circuit power. The constant short-circuit power remains as long as the duration of the input vector.

Figures 3(a) and 3(b) show the power waveforms with complementary and noncomplementary inputs, respectively. As shown in Figure 3(b), in the duration of the input vector $A = \overline{A} = B = C = 1$ (from 7 to 8 μs on the time axis), the peak power has a constant high value. This is because the noncomplementary input pair ($A = \overline{A}$) makes *NAND_Out* and *AND_Out* both stay at logic low. The time from 7 to 8 μs represents the high time of the shortest input pulse A. As a result, the two PMOS transistors, P0 and P1, are both turned on; thus, the two current paths from V_{DD} to ground (highlighted in Figure 2(b)) exist till the input vector is changed. The amplitude of short-circuit power is typically three orders of magnitude higher than the leakage power. This significant power difference between the cases using complementary and noncomplementary inputs is large enough for a monitoring device to indicate the presence of a HT.

We examine the average power for complementary and noncomplementary inputs for basic DCVSL gates using a typical IBM7RF technology library. As shown in Table 1, the increase on the average power (averaging power for all possible input patterns) caused by noncomplementary inputs is over three orders of magnitude. This is the basis for choosing DCVSL to implement functional units that facilitate HT detection. If the triggered HT flips the internal node of a functional unit, it will create a noncomplementary signal in the middle of that functional unit. Consequently, the power consumption will stay high for a long time, which is different from normal switching power.

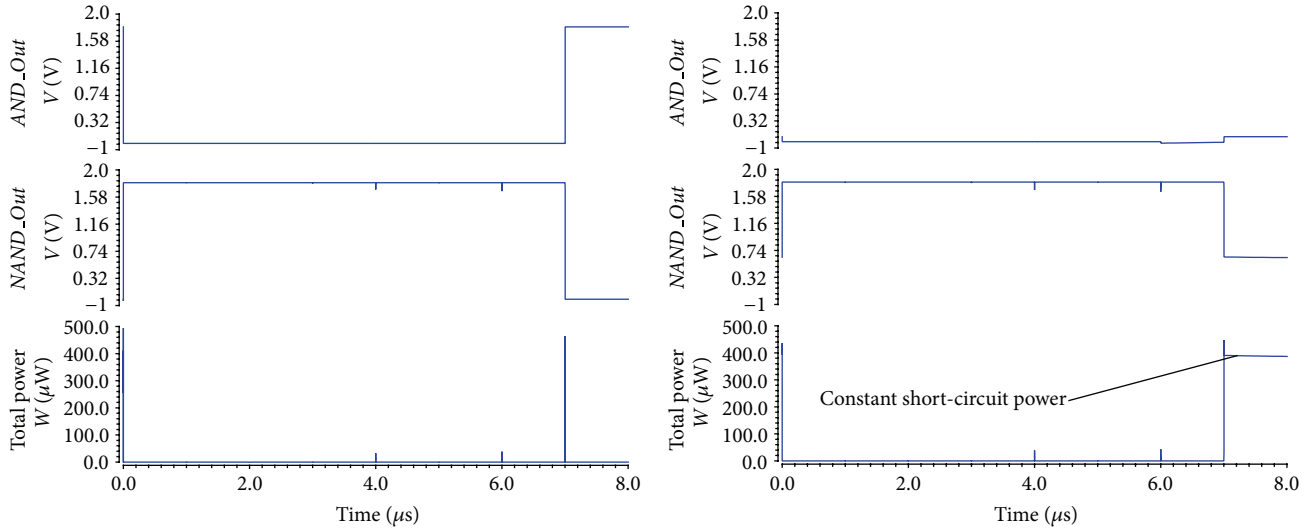

Figure 3: Voltage and power waveforms for DCVSL NAND3-AND3 gate. (a) Complementary inputs and (b) noncomplementary input $A = \overline{A}$.

Table 1: Power increase caused by noncomplementary inputs.

Logic gates	Average power	
	Power for complementary inputs	Power for noncomplementary inputs
Inverter	20.51 nW	205.25 μW
NAND2-AND2	12.76 nW	92.84 μW
NOR2-OR2	11.85 nW	92.61 μW
XNOR2-XOR2	19.97 nW	171.2 μW
NAND3-AND3	7.501 nW	40.36 μW
NOR3-OR3	6.673 nW	39.81 μW
XNOR3-XOR3	16.49 nW	84.90 μW
D-Flip-Flop	17.23 nW	181.8 μW

2.2.2. Probability of Abnormal Short-Circuit Power. The key reason for DCVSL gate having abnormal short-circuit power is the noncomplementary output nodes turning on the two PMOS transistors simultaneously. We assume that the consequence of a HT insertion on DCVSL functional units is flipping one of the complementary inputs. This is similar to HT insertion in other technologies; that is, a triggered HT is used to change the logic value of a logic gate or memory element.

Because of electrical and logical masking, the noncomplementary inputs (caused by HTs) do not always yield abnormal short-circuit power. As the logic gate topology varies between gates, it is difficult to obtain a closed-form expression for the probability of abnormal power occurrence. We summarize the general procedure for how to analyze the HT detection probability in DCVSL systems through abnormal power observation. Figure 4 is the flowchart for the analysis procedure.

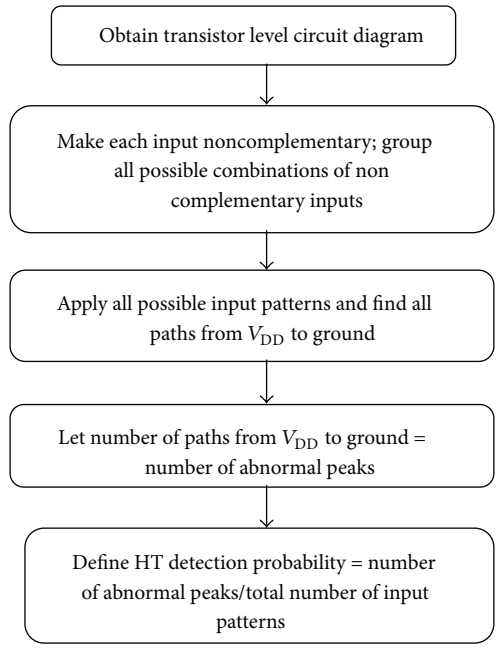

Figure 4: Flowchart for analyzing the HT detection probability for a DCVSL gate.

In order to create an erroneous output in DCVSL, a HT has to make one or more of the inputs noncomplementary. This may result in an erroneous output if the effect of the noncomplementary input is propagated and reaches the output port. An important point to note is that not all erroneous outputs are accompanied by abnormal power peaks. Only if the erroneous output creates at least one path from V_{DD} to ground, will we observe the abnormal short-circuit power.

Table 2: Probability of abnormal power and output error rate over all possible input patterns for DCVSL logic gates.

DCVSL gates	Percentage of abnormal power over all input patterns	Percentage of output error over all input patterns
Inverter	50.00%	100%
XOR2	41.66%	100%
XOR3	33.92%	100%
AND2	25.00%	25.00%
AND3	12.50%	12.50%
OR2	25.00%	50.00%
OR3	12.50%	25.00%
OAI21	23.21%	28.57%
AOI21	26.78%	50.00%
AOI22	25.89%	45.08%
OA22	25.89%	35.27%
MUX21	30.35%	55.00%
Average	27.72%	52.00%

We examine the probability of abnormal power and output error occurrence for all input patterns. Table 2 shows the ratio of the total number of abnormal power peaks over the total number of all input patterns for various basic DCVSL gates. The average probability for power exception and output mismatch are 27.7% and 52%, respectively. This means our HT detection method has over 50% chance to detect HTs, even if the HT trigger circuit is implemented with a single gate. This is a significant advantage over other power-based side-channel analysis methods, which have a lower bound on the size of detectable HTs.

Moreover, we observe that abnormal power occurs more often on the input pattern that produces the rare output value. For example, an AND3 gate produces high output only when all three inputs are high; the abnormal power appears at the exact input pattern if one of the inputs is not in the complementary form. To hide a HT, hackers often utilize the rare case to trigger the HT. As discussed above, our approach inherently achieves a higher detection rate for the HT triggered by rare cases. This means a system equipped by our method will pose a greater challenge to attackers in order to conceal HTs.

3. Experimental Results

3.1. Experimental Setup. We evaluated the proposed method on the 64-bit ripple carry adder, ISCAS'85 and ISCAS'89 benchmark circuits. The schematic and layout of the 64-bit adder were implemented in Cadence Virtuoso with the IBM CMOS7RF technology. We set all transistor lengths to 220 nm (minimum length in the CMOS7RF technology) and set the PMOS and NMOS transistor widths to 500 nm and 600 nm, respectively. The average power, leakage power, and peak dynamic power were obtained from schematic-level simulations by examining all possible input patterns. The area for DCVSL modules was obtained from customized layout in Virtuoso. Five metal layers were used in layout design. The fastest switching period for input is 1 μs. We synthesized the Verilog codes of ISCAS benchmark circuits in Synopsys Design Compiler with IBM CMOS7RF technology. The synthesized netlist is modified with an in-house python-based netlist generator, which converts CMOS netlist to DCVSL netlist. The behavior model of CMOS library is modified according to the gate output and power performance obtained from simulation in Cadence Virtuoso.

Table 3: Number of transistors for DUTs and HTs in this work.

Circuit	CMOS 64-bit adder	HT-1	HT-2	HT-3
Transistor number	2560	8	28	100
Circuits	DCVSL 64-bit Adder	C432	C1908	C3540
Transistor number	1644	2070	5516	9874
Circuits	S526	S832	S1196	S1488
Transistor number	1682	1408	3056	2824

Table 4: Power consumption for two 64-bit full adders and HT insertions.

Unit under test		Dynamic power (mW)	Leakage power (nW)
CMOS-based 64-bit full adder	Adder	24.6	65.78
	HT-1	0.444	0.419
	HT-2	0.942	1.243
	HT-3	1.028	2.583
DCVSL-based 64-bit full adder	Adder	8.002	47.50
	HT-1	0.566	0.328
	HT-2	0.892	0.993
	HT-3	1.544	2.465

HT detection rate is evaluated through gate-level simulation in Cadence NCVerilog. To observe the accumulated HT-induced effects through the system, we inserted the HTs payload on the inputs of DUTs. We particularly did so to model the propagation of HT effect in a large-scale system. To compare the area and power consumption of DUT and HTs, we designed three HTs. HT-1 is OR3 trigger circuit with XOR2 payload. HT-2 is OR(XOR(AND(x,y),z),w) trigger circuit with XOR2 payload. HT-3 is AND4 plus modulo-8 counter trigger circuit with XOR2 payload. The complexity of the DUTs and HTs in this work is listed in Table 3. As can be seen, the HTs are significantly smaller than the target design.

3.2. Case Study on a 64-Bit Full Adder. We implemented a 64-bit full adder using CMOS and DCVSL in Cadence Virtuoso. The layout area for these two adders is shown in Table 3. Because less PMOS transistors are needed in DCVSL, the area of DCVSL-based full adder is less than that of CMOS full adder when optimization is applied on both implementations. HTs are rarely triggered and the leakage power for HTs is a few orders of magnitude less than the adder switching power, as shown in Table 4.

All possible input patterns were applied to the 64-bit ripple carry adder. We placed a HT circuit to alter one complementary input pin in the adder. The power over time waveform is shown in Figure 5. As can be seen in

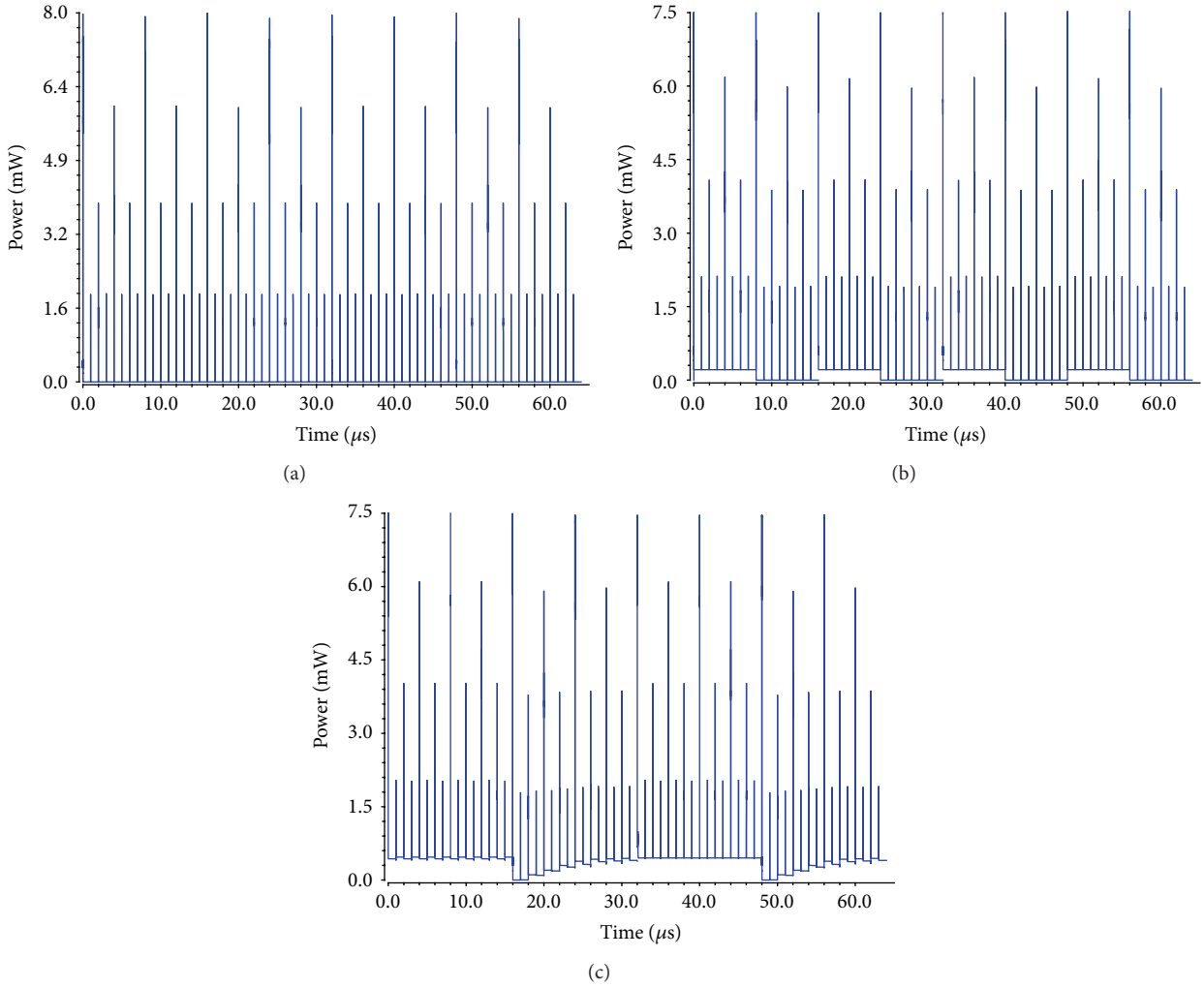

Figure 5: Power consumption for a 64-bit DCVSL full adder. (a) No HT, (b) HT on the 49th 1-bit full adder carry in port, and (c) HT on the 2nd 1-bit full adder carry in port.

Figure 5(a), when no HT is triggered, the switching power has instantaneous peaks whereas the leakage power remains flat (close to zero). Figure 5(b) shows the power for the adder with one HT inserted at the 49th 1-bit full adder. As can be seen, the power has an extra periodical increase, which is noticeably higher than the leakage power. This is the short-circuit power (discussed in Section 2.2) induced by the noncomplementary inputs from HT insertion. We placed the HT payload circuit to the 2nd 1-bit full adder and observed different power behavior. As shown in Figure 5(c), the increased short-circuit power appears in almost all input patterns. This is because the 2nd 1-bit full adder with noncomplementary inputs yields noncomplementary outputs, and those outputs are further propagated to other 1-bit full adders. Because of the propagation of HT effects, the power consumption is exceptionally higher than that in normal cases.

CMOS circuits have more PMOS transistors than the DCVSL version. Consequently, the dynamic power consumption of CMOS is higher than that of DCVSL. As shown in Figure 6, DCVSL has less average power consumption than CMOS. However, when the HT is triggered to change the noncomplementary inputs for the DCVSL-based full adder, the increased short-circuit power results in a dramatic increase on the average power. Figure 6 also shows that the average power difference between original and HT affected version is over 50X. If the HT is inserted at the early stage in the functional block, the average power difference increases to over two orders of magnitude. This is favorable for power-based side-channel analysis HT detection methods.

To assess the HT detection rate, we assume that HTs are inserted to change the complementary inputs. As input vectors A and B for a 64-bit full adder are equivalent, we select 64-bit input A to receive the potential impact from HTs. Besides half of the inputs, A, the carry-in bit for the first 1-bit full adder is another potential location for HT insertion. As the proposed method is independent of the particular HT trigger circuit, we flipped one of the complementary inputs to model the effect of HT insertion. As shown in Figure 7, for the HTs on A, the HT detection rate reaches 1. Given a HT area over chip area ratio below 1%, the HT detection rate is higher

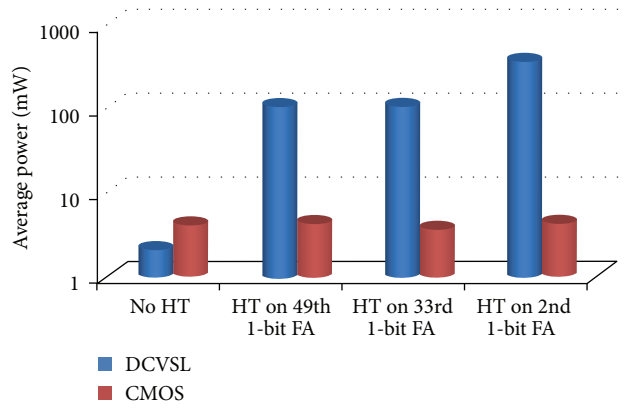

Figure 6: Impact of HT location on average power of 64-bit DCVSL adder.

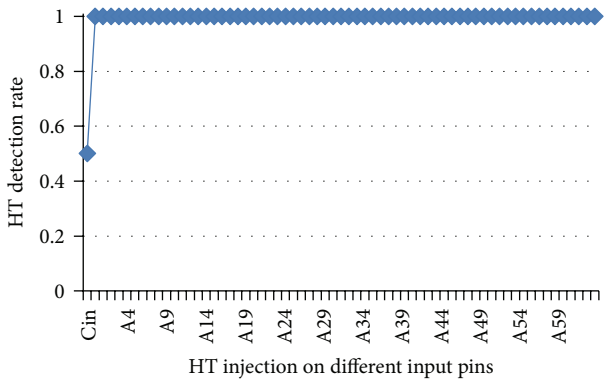

Figure 7: Impact of HT insertion locations on HT detection rate.

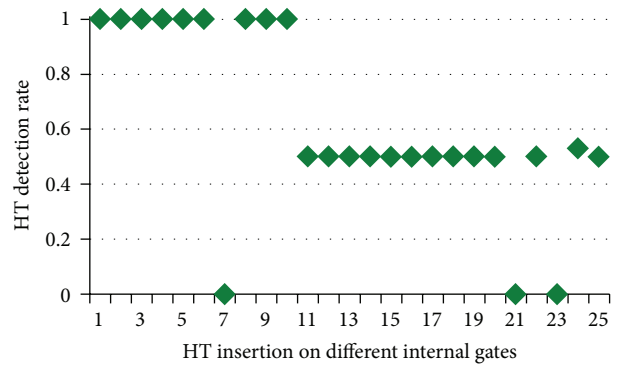

Figure 8: Impact of HT insertion location on HT detection rate.

than the one reported in [13]. Such high HT detection rate is mainly contributed by the noncomplementary inputs, which lead to internal noncomplementary outputs. Those outputs are further propagated to the remaining gates. Consequently, one HT injection possibly leads to more gate failures. Figure 7 also shows that the HT inserted on the carry-in (Cin) input can be detected with a HT detection rate of 0.5, which can be compensated by comparing outputs. Our simulation results show that, after the output comparison, the HT detection rate can be enhanced close to 1. The simulated HT detection rate was obtained from 200,000 random input patterns.

HTs placed on input pins at earlier stages in the design have higher potential to be detected, because of the propagation of noncomplementary outputs. We examine the impact of HT insertion locations on the HT detection rate. As shown in Figure 8, as the HT insertion location shifts towards the final output, the HT detection rate decreases to around 0.5.

The earlier the HT is inserted, the higher the probability of obtaining abnormal power behavior which can be used to determine the presence of HTs will be. For HT injection on the very early inputs, each HT detected case will have about 1.7 gates experiencing high short-circuit power, as shown in Figure 9(a). According to Tables 1 and 4, the short-circuit power for one gate is one order of magnitude higher than the leakage power of a full adder. Therefore, the power difference is high enough for use in HT detection. As shown in Figure 9(b), the HT inserted in the early 1-bit full adder stage yields an abnormal energy that is up to three orders of magnitude higher than normal leakage energy. HT insertion location approaching the final output yields less abnormal power, in terms of absolute energy value and the frequency of abnormal energy. As explained before, the latter HT injection location has a higher probability to demonstrate errors on the final outputs.

3.3. Evaluation on Benchmark Circuits. The proposed method is further evaluated with ISCAS benchmark circuits, which are composed of various logic gates listed in Table 2. In the experiments below, we assume that single HT is inserted in the benchmark circuit. More HT insertions in the target circuit lead to a higher HT detection rate, as more gates experience abnormal short-circuit power. The HT detection rate is defined as the number of cases experiencing abnormal short-circuit power over the total number of test cases. Three combinational benchmark circuits, c432, c1908, and c3540, are used to assess the HT detection rate of our method. 500,000 random input patterns were applied to the evaluation of c432 and c1908 circuits. Because of larger scale, c3540 was evaluated with 1,000,000 random input patterns.

As shown in Figure 10, our method achieves the HT detection rate up to 1 in the c432 circuit. The lowest HT detection rate is 0.7333. The majority of logic gates in c432 are Inverter and AND2; thus the HT rates are centered around two particular regions, 1 and 0.73. The scales of c1908 and c3540 are larger than c432; the kind of logic gates in c1908 and c3540 is more diverse than c432. These two factors affect the HT detection rate. Figures 11 and 12 show that the HT detection rate is distributed over the whole range, but the HT detection rate stays mostly above 0.7. We averaged the HT detection rate over all test cases in Figure 13. As can be seen, our method achieves a HT detection rate over 0.8 in c432 and c1908. The HT detection rate for c3540 is slightly low; however, our HT detection rate is still significant, as our method is not limited by the size of HTs and can be used to detect extremely small HTs. The average HT detection rate for the examined ISCAS'85 benchmark circuits is 0.76.

To examine the amount of power increased by each HT insertion, we first investigated the number of gates having

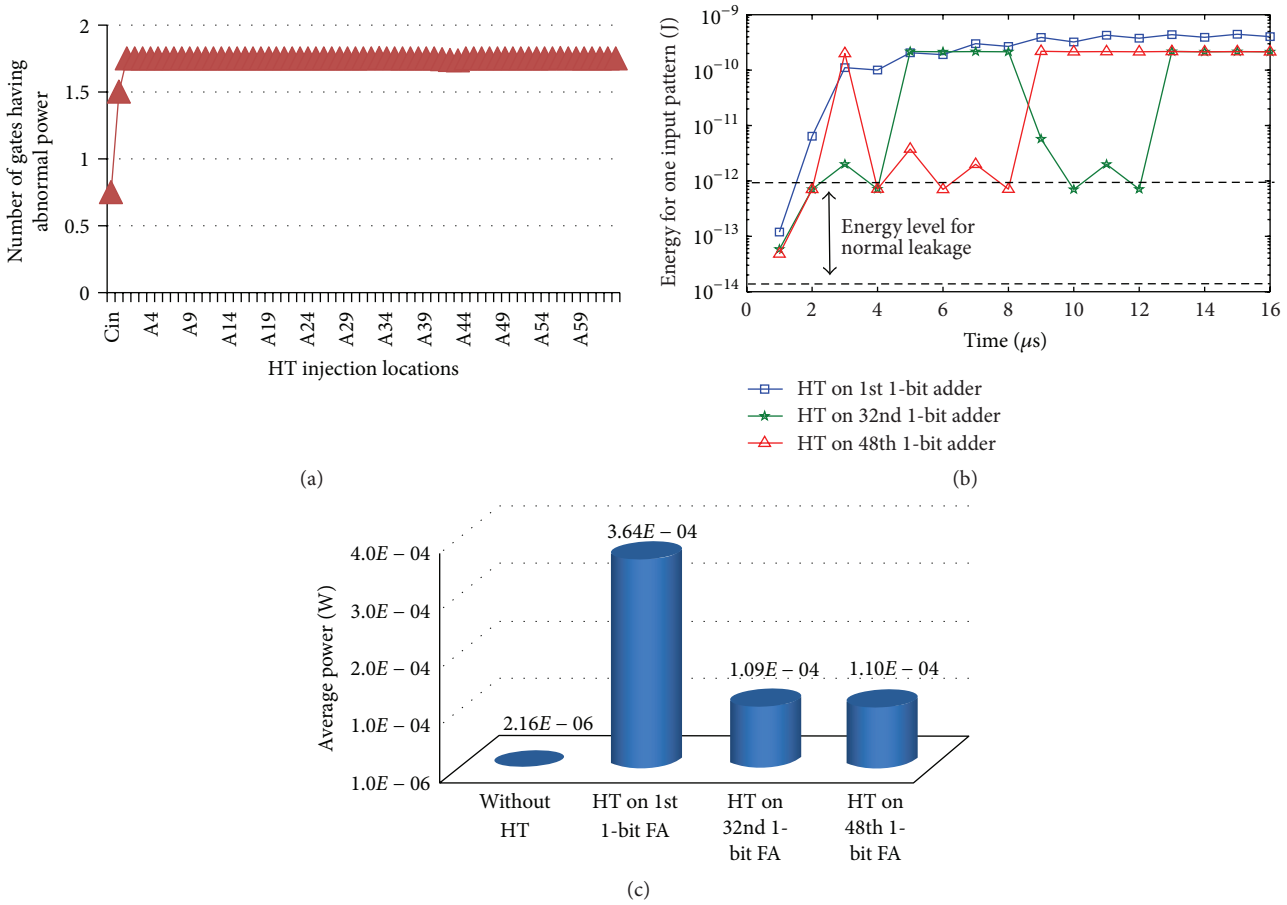

FIGURE 9: Results for HT-induced abnormal power assessment. (a) Average number of gates experiencing high short-circuit power per HT inserted case. (b) Abnormal energy caused by HT insertion over regular leakage energy. (c) Average power for three different HT injection locations.

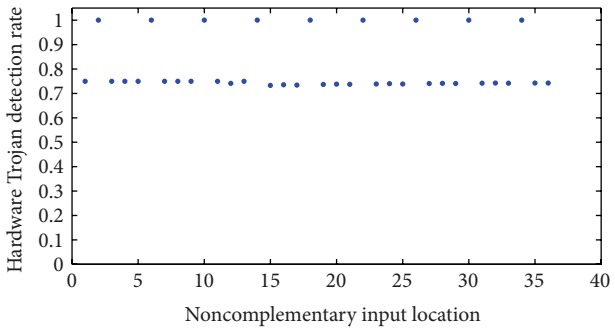

FIGURE 10: HT detection rate in c432.

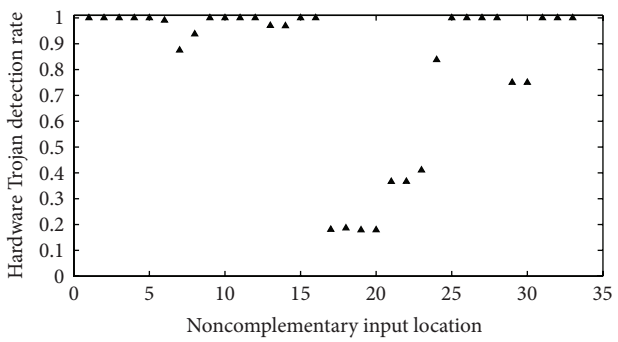

FIGURE 11: HT detection rate in c1908.

abnormal power upon HT insertion in the different locations of three ISCAS'85 benchmark circuits. Figure 14 shows the number of gates that are affected by one HT insertion. As can be seen, the number of gates yielding abnormal power generally increases with the circuit size and complexity. As shown in Figure 14, c3540 has the highest number of gates experiencing abnormal power per each HT insertion, compared to c1908 and c342. As HT insertion position moves towards the final output, the number of gates with abnormal power behavior decreases because the path of HT effect propagation is reduced. Since the abnormal short-circuit power also depends on input patterns of the target gate, the results reported in Figure 14 is not always integer valued. We averaged the number of gates affected by each HT insertion in three benchmark circuits. As shown in Figure 15, the average affected gate number for c3540 exceeds three. The higher number means more significant power will be induced by

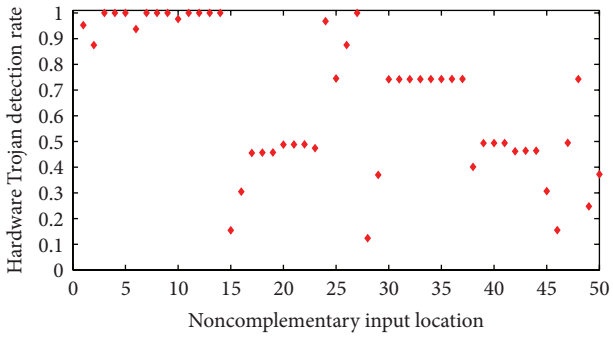

Figure 12: HT detection rate in c3540.

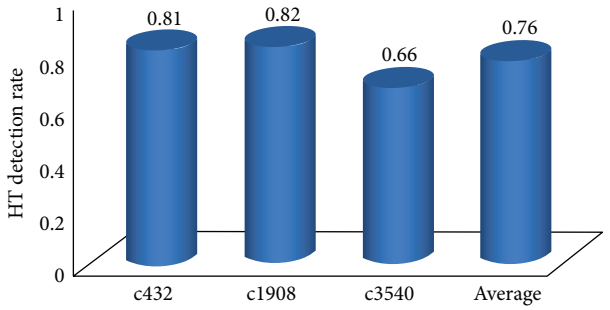

Figure 13: Average HT detection rate.

HT insertions; this feature has potential to be used in power-based HT detection.

Detecting the noncomplementary final output of DUT helps to improve the HT detection rate. As shown in Figure 16, not all test cases have abnormal power behavior. We collected the number of cases that have noncomplementary outputs (i.e., output error) and observed that the cases of noncomplementary DUT final output can achieve a HT detection rate of 1. This outstanding performance depends on circuit topology and the employed logic gates. Sometimes, the output error occurs at the same moment when abnormal short-circuit power is observed.

Sequential circuits are more likely to be affected by HT effect propagation, as latches and flip-flops have a higher probability to remain high with short-circuit power than combinational logic gates. We injected single HT on the inputs of benchmark circuits, s526, s832, s1196, and s1488, to model the impact of HT on circuits. As shown in Figure 17, on average, the HT detection rate on sequential circuit is higher than that in combinational circuits. The HT detection of s1488 and s1196 is close to 1. The average HT detection rate for the examined ISCAS'89 benchmark circuits is 0.85.

4. Conclusion

Hardware Trojans (HTs) challenge the chip security because of the increasing number of chips being fabricated, assembled, and packaged offshore. To enforce the confidence of chip security, efficient HT detection is imperative. HT detection can be performed during chip testing stage, although it

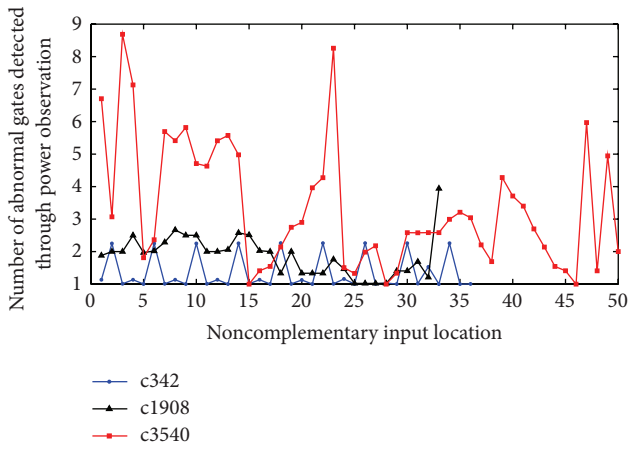

Figure 14: The number of gates experiencing abnormal power during each HT insertion.

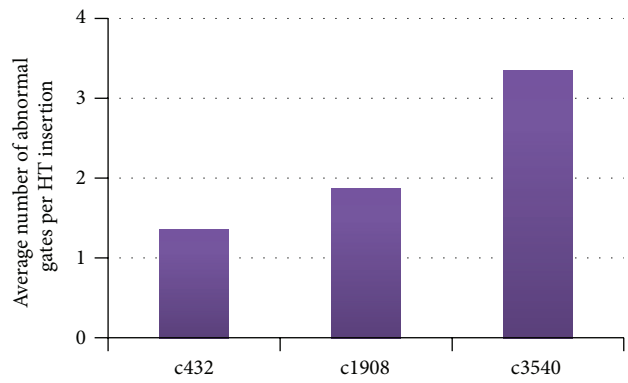

Figure 15: Average number of gates with abnormal power per each noncomplementary input pair.

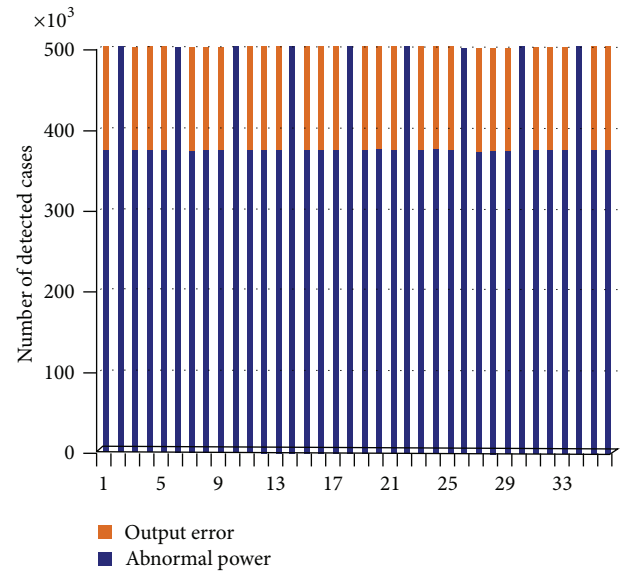

Figure 16: HT detection rate improvement by comparing complementary outputs in c432 circuit.

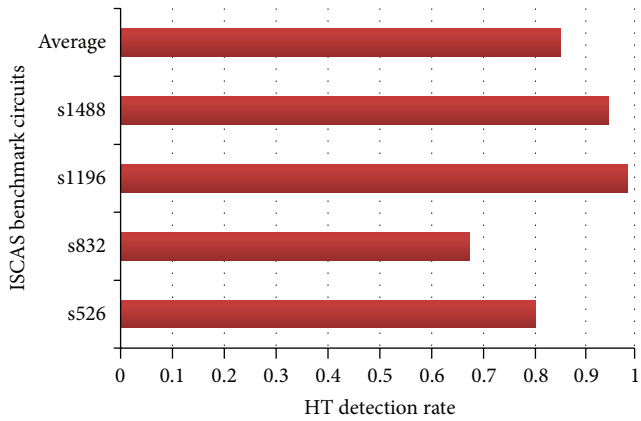

Figure 17: Average HT detection rate of different sequential benchmark circuits.

requires large numbers of test vectors and long verification times. As argued by many researchers, testing approaches may not be practical in identifying the rare events caused by HTs in a short period of time. Chip fingerprint is examined in IC authorization stages through side-channel analysis. Existing side-channel analysis approaches are challenged by process variation, lack of a perfect golden chip for comparison, and the presence of small-scale HTs. To address this need, we propose to use the inherent characteristic of DCVSL to detect HTs at runtime, without requiring a golden chip and a large number of test vectors. Our method is low-cost, convenient for user, and complementary to existing power-based side-channel analysis methods.

In this work, we exploit DCVSL's complementary feature on both inputs and outputs to detect hardware Trojans at runtime, rather than offline. Noncomplementary inputs in DCVSL-based systems lead to constant and abnormal short-circuit power peaks, which remain until the noncomplementary inputs disappear. A case study on a 64-bit ripple carry adder shows that the proposed method achieves from 50X to two orders of magnitude higher average power difference than CMOS-based power analysis. Such high power difference between normal operation and HT triggered conditions is desirable for power-base side-channel analysis. Evaluation on a 64-bit adder shows that our method achieves a HT detection rate approaching 100%, if HTs are inserted to flip one of the adder inputs logic value. As HT payload circuits are placed close to the final outputs, our abnormal power-based HT detection slightly loses its efficiency. The examination on the complementary characteristic of the outputs can improve the HT detection rate. Assessment on ISCAS'85 and ISCAS'95 benchmark circuits shows that the HT detection rate is in the range of 66% to 98%. On average, our method can detect 76% and 85% of HTs inserted in ISCAS'85 and ISCAS'89 benchmark circuits, respectively. By examining the complementary nature of the final output, we further improve the HT detection rate. Simulation on ISCAS'85 c432 circuit shows that the HT detection rate can be compensated to reach 100%.

In future work, we will validate the proposed method in larger-scale circuits. In addition, we will integrate our method with a current monitor to demonstrate the significance of proposed concept in real applications.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

References

[1] J. Markoff, "Old Trick Threatens the Newest Weapons," October 2009, http://www.nytimes.com/2009/10/27/science/27trojan.html?pagewanted=all&_r=1&.

[2] J. Ellis, "Trojan integrated circuits," http://chipsecurity.org/2012/02/trojan-circuit/.

[3] S. Johnson, "Fake chips threaten military," San Jose Mercury News, September 2010, http://www.mercurynews.com/breaking-news/ci_15990184.

[4] M. Banga and M. S. Hsiao, "A region based approach for the identification of hardware Trojans," in *Proceedings of the IEEE International Workshop on Hardware-Oriented Security and Trust (HOST '08)*, pp. 40–47, June 2008.

[5] D. Mukhopadhyay and R. S. Chakraborty, "Testability of cryptographic hardware and detection of Hardware Trojans," in *Proceedings of the 20th Asian Test Symposium (ATS '11)*, pp. 517–524, November 2011.

[6] 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.

[7] F. Wolff, C. Papachristou, S. Bhunia, and R. S. Chakraborty, "Towards Trojan-free trusted ICs: problem analysis and detection scheme," in *Proceedings of the Design, Automation and Test in Europe (DATE '08)*, pp. 1362–1365, Munich, Germany, March 2008.

[8] R. S. Chakraborty, F. Wolff, S. Paul, C. Papachristou, and S. Bhunia, "MERO: a statistical approach for hardware Trojan detection," in *Proceedings of the 11th International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 396–410, 2009.

[9] M. Banga and M. S. Hsiao, "VITAMIN: voltage inversion technique to ascertain malicious insertions in ICs," in *Proceedings of the IEEE International Workshop on Hardware-Oriented Security and Trust (HOST '09)*, pp. 104–107, July 2009.

[10] H. Salmani, M. Tehranipoor, and J. Plusquellic, "A novel technique for improving hardware trojan detection and reducing trojan activation time," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 20, no. 1, pp. 112–125, 2012.

[11] Y. Alkabani, "Trojan immune circuits using duality," in *Proceedings of the 15th Euromicro Conference on Digital System Design (DSD '12)*, pp. 177–184, 2012.

[12] Y. Jin and Y. Makris, "Hardware Trojan detection using path delay fingerprint," in *Proceedings of the IEEE International Workshop on Hardware-Oriented Security and Trust (HOST '08)*, pp. 51–57, June 2008.

[13] K. Hu, A. N. Nowroz, S. Reda, and F. Koushanfar, "High-sensitivity hardware Trojan detection using multimodal characterization," in *Proceedings of the Design, Automation & Test in Europe Conference & Exhibition (DATE '13)*, pp. 1271–1276, 2013.

[14] C. Bell, M. Lewandowski, and S. Katkoori, "A multi-parameter functional side-channel analysis method for hardware trust verification," in *Proceedings of the 31st IEEE VLSI Test Symposium (VTS '13)*, pp. 1–4, 2013.

[15] L. Wang, H. Xie, and H. Luo, "Malicious circuitry detection using transient power analysis for IC security," in *Proceedings of the International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering (QR2MSE '13)*, pp. 1164–1167, 2013.

[16] S. Narasimhan, D. Du, R. S. Chakraborty et al., "Hardware Trojan detection by multiple-parameter side-channel analysis," *IEEE Transactions on Computers*, vol. 62, no. 11, pp. 2183–2195, 2013.

[17] S. Narasimhan, X. Wang, S. Bhunia, W. Yueh, and S. Mukhopadhyay, "Improving IC security against Trojan attacks through integration of security monitors," *IEEE Design & Test of Computers*, vol. 29, no. 5, pp. 37–46, 2012.

[18] T. Huffmire, J. Valamehr, T. Sherwood et al., "Trustworthy system security through 3-D integrated hardware," in *Proceedings of the IEEE International Workshop on Hardware-Oriented Security and Trust (HOST '08)*, pp. 91–92, June 2008.

[19] X. Wang, H. Salmani, M. Tehranipoor, and J. Plusquellic, "Hardware Trojan detection and isolation using current integration and localized current analysis," in *Proceedings of the 23rd IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems (DFT '08)*, pp. 87–95, October 2008.

[20] F. Koushanfar and A. Mirhoseini, "A unified framework for multimodal submodular integrated circuits trojan detection," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 1, pp. 162–174, 2011.

[21] D. A. Rennels and H. Kim, "Concurrent error detection in self-timed VLSI," in *Proceedings of the 24th International Symposium on Fault-Tolerant Computing*, pp. 96–105, June 1994.