A Cluster-Based Distributed Active Current Sensing Circuit for Hardware Trojan Detection

Yuan Cao, *Student Member, IEEE*, Chip-Hong Chang, *Senior Member, IEEE*,
and Shoushun Chen, *Senior Member, IEEE*

***Abstract*— The globalization of integrated circuits (ICs) design and fabrication has given rise to severe concerns on the devastating impact of subverted chip supply. Hardware Trojan (HT) is among the most dangerous threats to defend. The dormant circuit inserted stealthily into the chip by the advisory could steal the confidential information or paralyze the system connected to the subverted chip upon the HT activation. This paper presents a transient power supply current sensor to facilitate the screening of an IC for HT infection. Based on the power gating scheme, it converts the current activity on local power grid into a timing pulse from which the timing and power-related side channel signals can be externally monitored by the existing scan test architecture. Its current comparator threshold can be calibrated against the quiescent current noise floor to reduce the impacts of process variations. Postlayout statistical simulations of process variations are performed on the ISCAS'85 benchmark circuits to demonstrate the effectiveness of the proposed technique for the detection of delay-invariant and rarely switched HTs. Compared with the detection error rate of a 4-bit counter-based HT reported by an existing HT detection method using the path delay fingerprint, our method shows an order of magnitude improvement in the detection accuracy.**

***Index Terms*— Hardware Trojan, side-channel analysis, current monitor, process variation, power gating.**

I. Introduction

THE dramatically increase in cognitive and organizational complexity of integrated circuits (IC) design is pushing the semiconductor industry towards a vertical specialization where various stages of IC design are disintegrated and outsourced to external firms and relocated across national boundaries that have the tacit knowledge and expertise. The risk of this geographical dispersion of chip design activities is the infiltration of malicious chips into the IC supply chain. Perpetrators and insiders can find many opportunities to implant into an IC dormant logics that are extremely difficult to be detected by conventional testing and verification methods [1], [2]. These hardware Trojans (HTs) may potentially leak confidential information controlled by the chip or cause catastrophic damages to valuable electronic systems and infrastructures at any time upon triggered by the rare and unknown conditions.

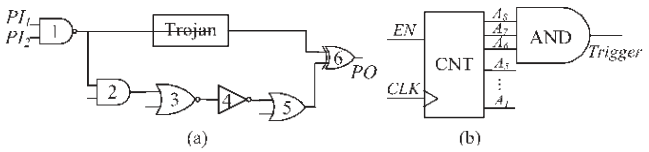

Fig. 1. Example of a HT (a) with no delay impact, (b) with no switching power impact.

With advanced etching and optical imaging tools, physical inspection methods can extract the circuitry and detect the Trojan. Destructive reverse engineering is costly and time consuming, which is not practical to be applied to all chips under test but useful for assuring the genuineness of extracted reference signatures for Trojan detection by other means. HTs do not affect the circuit's original functionality. It is impossible to anticipate the Trojan placements, structures, functions, sizes, etc. Even then, their presence can still alter the IC's speed, power consumption characteristics or reliability. This makes it possible to diagnose a chip for potential Trojan infection by side channel analysis albeit the challenges [3]–[21]. Side channels are signals of an IC in operation that can be probed externally to detect any anomalies in the internal behavior of a circuit. One major advantage of side channel analysis is the Trojans can be detected without being fully triggered [3]. Examples of popular side channel analysis methods include delay-based analysis [4]–[8] and power-based analysis [9]–[14].

Delay-based (or time-based) side channel analysis can succeed in HT detection if the additional delay due to the Trojan is distinguishable from the delay difference caused by process variations. One such method [4] adds a "shadow register" to latch the same data as the destination register along an arbitrary path. The shadow register clock runs at the same frequency as the system clock, but with adjustable phase shift to measure the path delay. This method can detect Trojans in the circuit at speed, but it suffers from a high area overhead due to the extra register and comparator for each path to be monitored. The main challenge encountered by delay-based side channel analysis is the Trojan can be inserted in such a manner that there is no difference in external delay measurement [15]. Fig. 1(a) illustrates such an example. Since the Trojan logics are embedded along the path in parallel, it is

unlikely that the delay-based side channel analysis will pick up any anomaly in timing path from the primary input PI_1 or PI_2 to the primary output PO.

Power-based side channel analysis provides the visibility of the chip's internal switching activities. In [9], random input patterns are applied to obtain a power signature for comparison with that of the Trojan-free chip. As the power signature is highly susceptible to the random noise induced by the process and temperature variations, advanced power-based analysis methods partition the entire chip into several regions to magnify the Trojan-to-circuit activity [10], [11]. The drawback is each region has to have its own power port for the power signature analysis. Besides, the attacker can also embed a Trojan that is activated only on a very rare condition [15], which results in no observable difference in the power signatures. The example in Fig. 1(b) shows an AND gate whose inputs are from the most significant bits of a counter. The Trojan can be triggered only after the counter has run for a much longer time than any standard test time. Another power-gated Trojan has been demonstrated to bypass the power-based side channel signal analysis [16]. To realize the triggering mechanism, the inputs of the Trojan are connected to some existing logic nodes of the original design. These Trojan gate connections increase the capacitive load on these nodes [17], together with the multiplexer inserted into an existing timing path to control the Trojan activation, they increase the path delay and switching activity duration even if the Trojan remains dormant. This can be considered as a special case of Trojan with low switching activity.

This paper proposes an active current sensing circuit to extract a signature that encapsulates both the timing and amplitude of switching activity from the transient power supply current (I_{DDT}) for HT detection. The proposed sensor utilizes the industrial power gating scheme, which is one of the most effective techniques in low power circuit design [22]–[25]. It employs sleep transistors to disconnect logic clusters from the power supply or ground to reduce the power consumption. The dynamic IR-drop across the sleep transistors in the active mode of operation can be sensed to detect path delay elongation by Trojan through region-based excitation of a number of paths per endpoint, including unobservable internal paths, such as paths without primary inputs, primary outputs or scan latches. Based on our preliminary experimentation [26], Trojan infected circuit can cause errant timing behaviors that are often shown up in logic as power supply droop, which can be picked up by monitoring the supply current. On the other hand, if the Trojan logics are inserted into a path in parallel (Fig. 1(a)), the timing signature alone will not be able to distinguish the difference of Trojan-free and Trojan-infected paths. But the abnormality of the I_{DDT} amplitude due to the Trojan will be detected by the sensor. Our proposed design includes a simple tunable threshold current comparator that can be calibrated to maximally discriminate between transient current and background noise and a multiplexer-based scan register to enable its transition-delay to be detected at the scan output vectors by the AC scan test with a pulse width modulated clock. This on-chip Trojan detection solution enables a more efficient screening of a large number of dubious

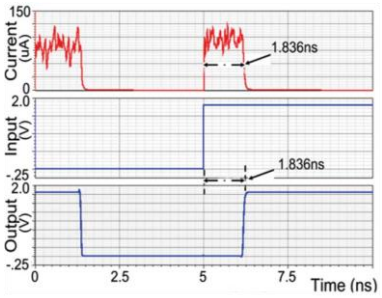

Fig. 2. I_{DDT}, input and output waveforms due to a sensitized path in C432.

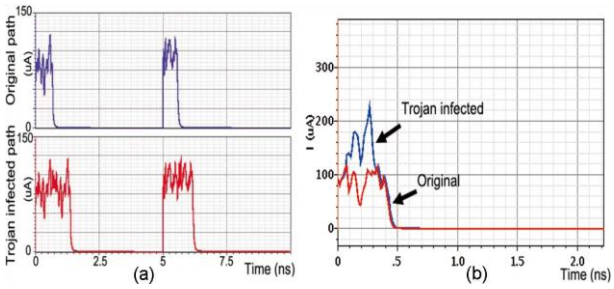

Fig. 3. Supply current waveforms for the sensitized path of Trojan-free and Trojan-infected circuits: (a) the Trojan is inserted in series, (b) the Trojan is inserted in parallel.

chips by eliminating the post-processing requirements from characterization-based methods [21].

The rest of the paper is organized as follows. Section II presents an example to illustrate the viability of the principle of detection behind the proposed method. In Section III, the design and operations of the proposed sensor for HT detection are elaborated. Simulation results are presented and discussed in Section IV. Finally, the conclusion is given in Section V.

II. Motivating Example

I_{DDT} conveys the unitary profile of switching activity and timing information of the sensitized paths of a chip. Fig. 2 shows the I_{DDT}, input and output voltage waveforms when an arbitrarily selected data path of ISCAS'85 benchmark circuit C432 is activated. C432 is a 27-channel interrupt controller which has 36 inputs and 7 outputs. It contains 160 gates. The propagation delay for this data path is $1.836ns$ based on the 50%-to-50% full swing voltage delay definition. The commencement and termination of the active switching current is clearly discernible from the quiescent current. The duration ($1.1836ns$) is the same as the propagation delay of the sensitized path. This timing signature of a subcircuit is found to be susceptible to subtle functional and topological modifications. Fig. 3 demonstrates the transient current differences between a Trojan-free path and a Trojan-infected path of C432. The Trojan inserted into this path consists of 7 logic gates, which contributes approximately 4% of additional logic to this original design. In Fig. 3(a), the Trojan inserted in series with the infected path induces current spikes that can evoke momentarily supply voltage droop and increase the path delay. Thus, the Trojan-infected path is distinguishable from the Trojan-free path with an elongated active current duration due to its extraneous switching. On the other hand, the Trojan inserted in parallel (Fig. 1(a)) does not show distinguishable

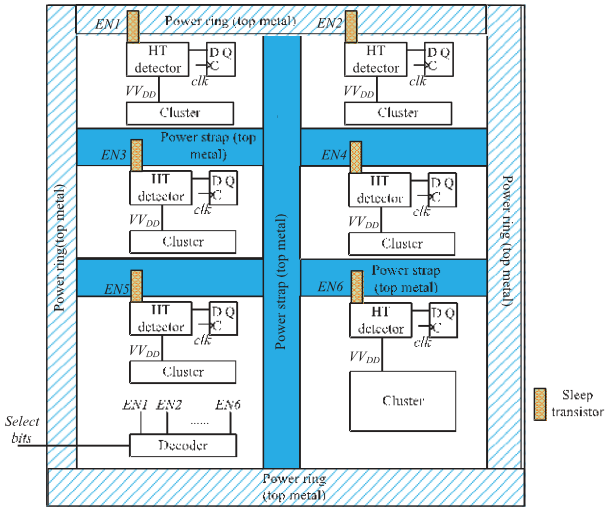

Fig. 4. Example of the deployment of the proposed HT detector with six virtual-power clusters.

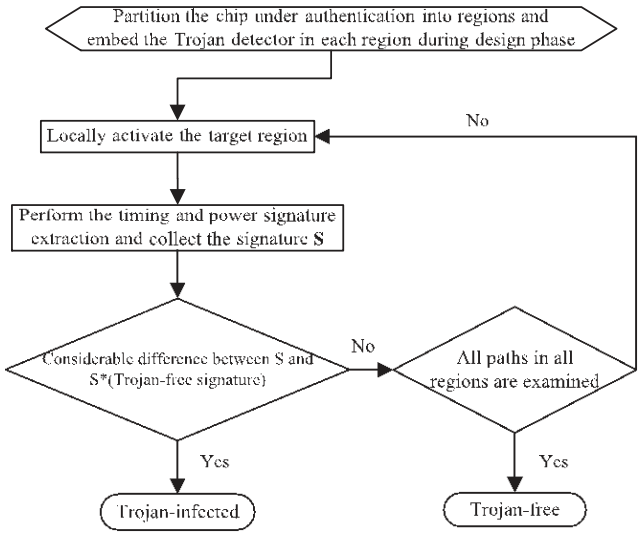

Fig. 5. The HT detection flow using the proposed HT-detector.

timing difference from the original design. However, the peak current is larger as shown in Fig. 3(b). While the Trojan path is shorter than the original path, its presence increases the loading and hence switching activities when the original path is sensitized. As a result, the amplitude of the switching current increases, although the switching duration remains the same.

The above observation leads to the thought of the implantation of small current sensors into a circuit to aid a more accurate and faster post-silicon Trojan detection and diagnosis. Its justification is analogous to the deployment of on-chip thermal sensors to aid thermal management when chip reliability and catastrophe failure due to thermal runaway is of great concern. We propose to implant a current detector based on the coarse-grained power gating technology. During the design phase, the original circuit is divided into regions. A current sensing circuit to be described in the next section is embedded into each region to monitor the transient current from the power strap or trunk of the power grid as depicted in Fig. 4. In coarse-grained region segmentation, the logic circuits of the same functional module are placed close to each other in the same power cluster and a sleep transistor is used to cut off the power to each cluster. The devices are powered by the virtual power supply VV_{DD} in its local power mesh. During the Trojan detection phase, only one cluster is powered on at a time by turning off the other sleep transistors to amplify the Trojan-to-circuit effect and reduce the test power. Since no transition will occur in the power-down clusters, no effort is needed to develop specific test patterns to trigger only part of the circuit but a small design effort is needed to divide the circuit into power grids and split the scan chain. Many power gating architectures and algorithms [22]–[25] can be considered. The scan partitioning technique [23] with very low DFT overhead in terms of die-area, circuit performance and power is used for our design. The switching time of the sleep transistors for all the clusters is controlled by a decoder. The characteristic signatures of the switching current envelope from each virtual power supply are extracted by its embedded detector and scanned out through the scan chain. By amortizing the circuit switching activities into clusters, extraneous activities that transcend regular circuit activities and process variations are more likely to be detected by the cluster-based current sensors in those regions where the Trojan resided. In this sense, the number of regions provides a trade-off between the resolution of the detectable Trojan and the hardware overhead.

The flow of the Trojan detection is shown in Fig. 5. Random test patterns are applied through the functional-test scan chain to locally activate the paths in the target region while the remaining regions are kept inactive by turning off their sleep transistors. The signature extracted from the regional current detector is compared with that of the Trojan-free chip (golden sample) for the same test patterns. If the difference of any region exceeds a threshold determined by the process variations, it signifies a probable existence of a Trojan in that region. If none of the regions exhibits an above threshold difference, the chip is most probably Trojan free based on the detectable HT resolution. The Trojan-free signatures can be extracted from a golden sample before its genuineness is confirmed by reverse engineering [27]. It may not need many attempts since only one golden chip is needed. Also, every unsuccessful attempt in this process is not completely fruitless as it means the discovery of a subverted or dubious chip. Presently, only a rare few emerging methods [6], [14], [21] are able to detect HT without the golden model but they are not without limitations. Typical prices for avoiding the golden model include the requirements of expensive computations, sophisticated process variation models and a large number of measurements to ensure accuracy for large chip with more gates [28].

For this HT-detection scheme to work, a dedicated and compact current sensor is required. When the sleep transistor connected to the virtual supply of a target region is turned on, it measures the duration and amplitude of transient current drawn from the virtual supply to a group of timing paths in the target region activated by the input pattern. The design of this current sensor is the focus of this paper.

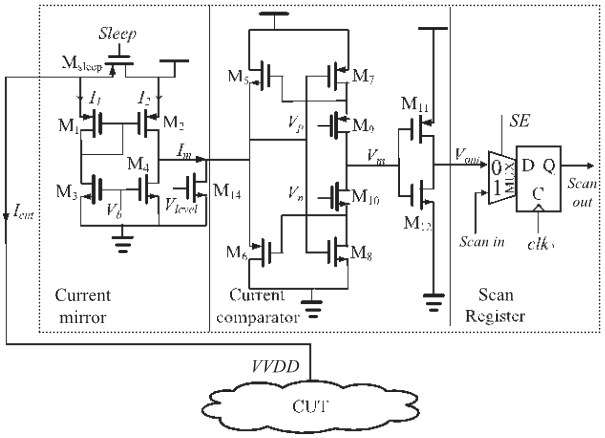

Fig. 6. Schematic of the proposed current sensing to path delay monitoring circuit.

III. Scan-Enabled Active Current Sensor

The schematic of the proposed active current sensor is shown in Fig. 6, where the cluster under test (CUT) refers to the cluster of circuits whose switching current is being monitored by the current sensor. Its principle of operation as a Trojan detector is explained as follows. The dynamic IR-drop across the on-resistance R_{on} of the sleep transistor M_{sleep} can be sensed to provide the visibility of the active current for the CUT. The dynamic current is mirrored to a current comparator to produce two voltage transitions that mark the path delay. The comparator output is latched into a scannable flip-flop. The latched output is propagated to an external output pin by daisy chaining the scan flip-flops of all detectors. The delay transition of the comparator output from each detector can be determined from the corresponding scanned output by varying the phase shift between the system clock and the sampling clock of the scan chain in the detectors. In what follows, the design and operation of each subcircuit will be elaborated.

A. Current Mirror

The current mirror utilizes the current monitor [29] originally developed for the I_{DDQ}/I_{DDT} testing. When the sleep transistor M_{sleep} is turned on initially, the gate voltage V_{level} for M_{14} is 0. When there is no current drawn by the CUT, i.e., $I_{cut} = 0$, the gate-source voltages of the transistor pair $(M_1 - M_2)$ are equal. A voltage drop is induced in the on-resistance R_{on} of M_{sleep} when the current I_{cut} drawn by the active CUT passes through R_{on}. This voltage drop causes a difference in the gate-source voltages of transistor pair $(M_1 - M_2)$ and produces the mirrored current $I_m = I_2 - I_1$, where I_1 and I_2 are the drain current of M_1 and M_2 respectively. I_m is given by [29]:

$$I_m \approx R_{on}(2\mu_p C_{ox}\frac{W}{L}I_1{}^3)^{\frac{1}{2}}(1+\frac{I_{cut}}{I_1}) \quad (1)$$

where μ_p, C_{ox} and W/L are the hole mobility, oxide capacitance and channel aspect ratio of M_1, respectively. The level shift transistor M_{14} is used to add a negative current offset to I_m. When its gate voltage V_{level} increases, the output current for the current mirror becomes:

$$I_m^{\emptyset} = I_m - I_{14} \quad (2)$$

where I_{14} is the drain current of M_{14}. V_{level} can be tuned to detect the peak current duration.

An important consideration is the sizing for the sleep transistor M_{sleep}. To reduce the area and power (leakage power and dynamic power) overheads caused by the addition of sleep transistors, smaller sleep transistor is preferred. A smaller sleep transistor with greater resistance will also improve the detector sensitivity. On the other hand, a greater on-resistance of the sleep transistor can result in a larger voltage drop across it and lower the VV_{DD} supply to the CUT. The sleep transistor is sized to meet the performance requirements of the CUT. As the maximum instantaneous current of a cluster of gates is much smaller than the summation of the peak currents of individual gates within the cluster, the size of a sleep transistor supporting a cluster of gates is much smaller than the combined area of sleep transistors connected to individual gates. To reduce the area overhead, a reasonably-sized sleep transistor is assigned to each cluster of mutually exclusive switching gates [30] under the peak current constraint of the sleep transistor.

The on-resistance R_{on} for an NMOS transistor is given by:

$$R_{on} = 1/(\mu_n C_{OX} W/L)(V_{GS} - V_t) \quad (3)$$

where V_t is the threshold voltage of the transistor. To limit the supply voltage droop to less than 5%, $(I_{cut} + I_1)R_{on} < 0.05V_{dd}$. R_{on} is empirically determined to be around 200• based on GF 65nm CMOS technology with a supply voltage of 1.2V.

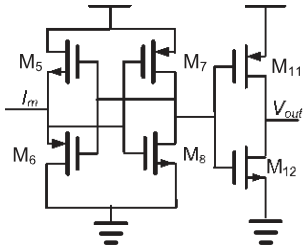

Fig. 7. Schematic of Traff's current comparator [31].

B. Current Comparator

The current comparator compares the mirrored current against the quiescent current threshold to produce a high output voltage level during the period of activity and a low voltage level when all sensitized path transitions have settled. The current comparator circuit in Fig. 6 is modified from the Traff's current comparator [31]. The original Traff's comparator is shown in Fig. 7. The transistor pair $(M_5 - M_6)$ of Traff's current comparator operates in the subthreshold region at the start of each comparison before the feedback loop takes effect, which results in a long settling time. This problem is overcome in our design by introducing two transistors, M_9 and M_{10}, in Fig. 6. This pair of transistors is biased in the

linear region, which increases the gate voltages of M_7 and M_8 to prevent M_5 and M_6 from entering the subthreshold region. The response time is improved at the expense of a reduced output voltage swing. Therefore, an inverting stage is needed in Fig. 6 to restore its rail-to-rail output. These two transistors also act as two voltage-controlled linear resistors. The charging and discharging currents of the comparator load capacitor can be adjusted by their gate voltages to subtly alter the slew rate and hence the width of V_{out}. This is equivalent to adding a small offset to the comparator threshold to compensate for the minute difference in quiescent currents of different chips due to the process variations.

V_{out} can be calibrated to mitigate the effect of process variation. A "reference pattern" that excites only a small number of paths of the region from the set of stimuli is applied when the power to the region is enabled. The pulse width of the voltage V_{out} is adjusted by V_p and V_n to be the same as that of the "reference chip" under the same test pattern. As only one sleep transistor of a cluster will be activated at any time, only two external pins need to be reserved for the calibration of the V_p and V_n voltages for all CUT detectors. After V_p and V_n have been calibrated, the pulse widths of the voltage V_{out} for other test patterns are then measured. As the Trojan does not affect all the paths of the CUT, the "reference pattern" selected for the calibration of V_p and V_n may or may not trigger the Trojan. If the Trojan logic is not excited by the "reference pattern" during this calibration, the transition delay of V_{out} of the Trojan-infected CUT will be exacerbated and become notably longer than that of the Trojan-free CUT when the Trojan-infected subcircuits are sensitized by other test patterns. If the "reference pattern" activates the Trojan-infected subcircuits, then the extended delay transition of V_{out} due to the excited Trojan under the "reference pattern" will be eliminated by the calibration but a negative offset will also be introduced into the subsequent measurements when the Trojan's infected subcircuits are not activated by the test patterns. In either case, the probability that a Trojan-infected CUT exhibiting disparate pulse width of V_{out} from the Trojan-free CUT under the same set of test patterns will increase after the calibration.

The proposed current comparator is implemented in GF $65nm$, 1.2 V CMOS technology and the circuit is simulated by Cadence Spectre simulator. The input current I_m to the comparator is emulated by a $20\mu A$ current source. The pulse width of I_m is varied in step of $100\,ps$. Fig. 8 (a) shows that the comparator output pulse width varies linearly with the input current pulse width for the fast (F), slow (S) and typical (T) corners of the process technology. The process variations introduce an offset into the linear transfer characteristic of the comparator. By adjusting the gate voltages V_p and V_n of the current comparator, this offset can be eliminated as shown in Fig. 8(b).

Fig. 9 shows the simulation results for a path delay measured by the proposed sensor for temperature ranges from 0 ℃ to 100 ℃. The change in temperature can introduce a DC offset to the measured path delay as shown in Fig. 9(a), which can also be compensated by calibration as shown in Fig. 9(b).

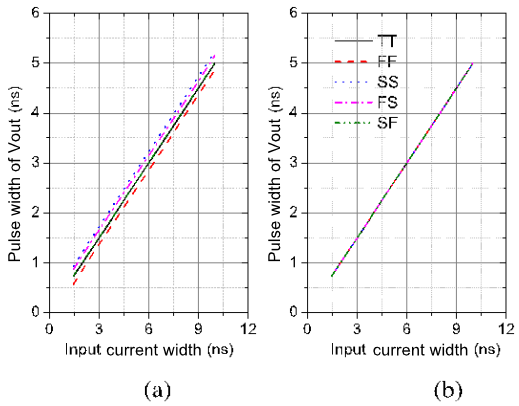

Fig. 8. Corner simulation of comparator output pulse width: (a) without calibration, (b) with calibration. The process corner is represented by a two-letter designator, where the first and second letters refer to the NMOS and PMOS corners, respectively. The letters T, F and S denote typical, fast and slow corners, respectively.

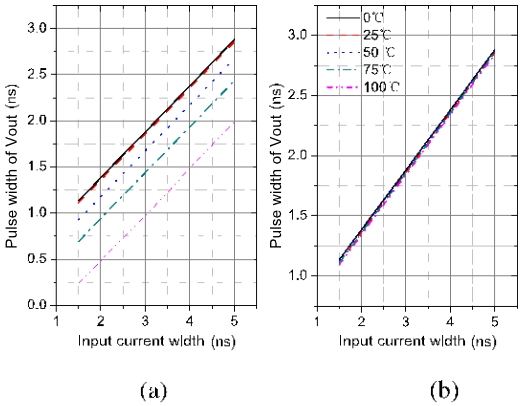

Fig. 9. Simulation of comparator output pulse width under temperature variations: (a) without calibration, (b) with calibration.

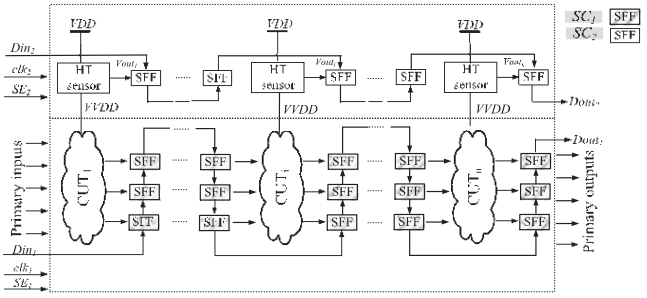

Fig. 10. Primary and secondary scan chains for the detection of current comparator output pulse width.

C. Scan Register

The current comparator output V_{out} is fed to a standard multiplexer-based scan FF. The scan FFs of all HT detectors are daisy chained to form a secondary scan chain to propagate the transition of V_{out} to an external scan output pin. The pulse width of V_{out} can be determined by the transition delay test [32] through the functional scan chain SC_1 and the secondary scan chain SC_2 as shown in Fig. 10, where n is the number of CUTs. The timing diagram for the transition delay test is shown in Fig. 11, where S_i and D_i are the

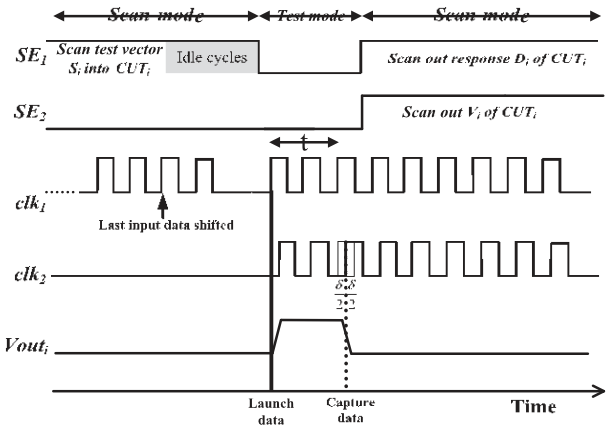

Fig. 11. Timing diagram of the sampling of transition delay.

input and output vectors of the i-th CUT. After turning on the sleep transistor of the i-th CUT, the scan-enable signal (SE_1) of the functional scan chain is asserted to shift the test pattern S_i into the input registers of the i-th CUT through SC_1 while the scan-enable signal (SE_2) of SC_2 is disabled. The input data S_i in SC_1 is launched into the i-th CUT at the rising edge of clk_1 when SE_1 is de-asserted. The current detector of the i-th CUT senses the commencement of circuit activities and produces a low-to-high transition on its V_{out}. The logic level V_i of V_{out} in the i-th CUT after a time delay t from the launching clock is captured into the scan FF of SC_2 at the last rising edge of clk_2 before SE_2 is asserted. clk_2, which is gated by $SE_1 \_ SE_2$ (_ denotes XNOR), has a phase shift from clk_1. By asserting SE_2, V_i can be scanned out to an observable scan-output pin. The process is repeated by launching the same input data with different capturing time (by changing the assertion time of SE_2 and the phase shift between clk_1 and clk_2) after SE_1 is deasserted until a high-to-low transition is detected at V_i from the scan output of SC_2. To capture the transition of V_{out}, the delay t is initially set to be slightly less than the pulse width of V_{out} of the Trojan-free CUT detector to capture the logic '1' of V_{out} and then the phase shift between clk_1 and clk_2 is incremented in timing steps of $\delta/2$ until the logic '0' of V_{out} is captured, where δ is the minimum discriminable delay exacerbation to signify the existence of Trojan. Idle cycles can be inserted between the last scan-in data and the de-assertion of SE_1 to allow the CUT to recover from the supply voltage droop and heat dissipation due to the input data scanning operation. clk_1 signal is disabled and the primary inputs are held constant during the idle cycles.

IV. Results and Discussion

A. Experiment Setup

Four virtual power clusters are considered in our simulation. The proposed detector is added into the CUT of each cluster. The CUT is a circuit from the ISCAS'85 benchmark suite [33]. Synopsys Design Compiler is used to map the benchmark circuits to the GF 65nm standard cell library. The Trojan circuit is inserted into the synthesized Verilog netlists. This is the more likely scenario when the hacker has no access to the RTL code, which is generally not provided to the foundry. Both netlists with and without Trojan are converted to the physical layout by Cadence SOC Encounter and stored in the industry standard GDS-II file. The simulation is carried out in the Cadence Spectre environment with the model file of parasitics and process variations provided by the foundry. Dynamic timing analysis without parameter variations and with parameter variations [34] are then performed on the Trojan-free and Trojan-infected circuits.

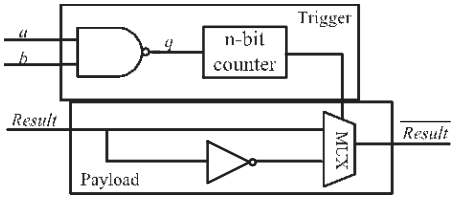

Fig. 12. Counter-based Trojan circuit architecture [35].

B. Trojan Circuits

The Trojan to be inserted into an arbitrarily selected CUT of the four clusters is designed using an n-bit counter and an NAND gate as shown in Fig. 12 [35]. The n-bit counter is clocked by the NAND gate output, which has its inputs a and b connected to the internal signals of the CUT. When the count exceeds a predefined number N, it triggers the Trojan and alters the $Result$ of the payload to $\overline{Result}$. The gate count of the one-gate payload and triggering mechanism of the Trojan used in this experiment is equivalent to 52 two-input NAND gates. N is set to a large value, e.g., 1000000, to reduce the chance for it to be detected by functional test. Two types of Trojan placements [15] are considered for each analysis. The first placement method replaces any output port of the CUT by the output $\overline{Result}$ of the Trojan circuit by connecting the input $Result$ of the Trojan's payload to the original output of the CUT. This Trojan introduces a very small delay of an inverter and a MUX delay for the inserted path. It exhibits very little additional switching activity during normal operation as it can be activated only by a rare set of input vectors. For the second placement method, the same counter-based Trojan (Fig. 12) is embedded into a path in parallel as in Fig. 1(a) such that the delay of the Trojan payload is buried within the much longer delay of other reconvergent paths of the CUT. In the following experiments, the former Trojan placement with very low switching activity is first analyzed before the Trojan with no delay impact is analyzed in Section IV-D.

C. Detection of Trojan With Low Switching Activity

Before a randomly sampled manufactured die is reverse engineered to ascertain its genuineness [1], it is first exercised with random test vectors. The phase shift of clk_2 with respect to the system clock clk_1 is successively increased to capture the logic value of V_{out} in the i-th CUT. Every phase shift when the detector captures the falling edge of V_{out} for each input test vector is recorded. These become the signatures of the golden model once a chip is identified as genuine.

TABLE I
TRANSITION DELAYS OF DETECTOR OUTPUTS FOR THE GENUINE AND INFECTED DESIGNS

No.	Clock period (ns)	Phase Shift (ps)	Scan outputs of detectors	
			Genuine	Infected
1	5	350	1111	1111
2	5	400	1111	1111
3	5	450	0000	**1**000
4	5	500	0000	**1**000
5	5	550	0000	0000

The design under test is then exercised with the same set of the test vectors starting with the corresponding phase shifts of clk_2 recorded from the Trojan-free model. The clock shift is gradually adjusted to find the falling edge of V_{out} of the design under test. Table I lists the four-bit streams corresponding to the logic states of V_{out} latched into the detector scan registers of the four clusters with different phase shifts of clk_2 for the Trojan-free and Trojan-infected benchmark circuit C2670. The period of clk_1 is set to be $5ns$. With the modern clock generator and phase lock loop (PLL), the phase shift of clk_2 is increased at a time step of $\delta/2 = 1\% \times 5ns = 50ps$. This time step determines the smallest Trojan detectable. Given that clock skew as low as $1ps$ in $180nm$ fabrication technology has been reported [36], single-gate Trojan can be detected in principle provided that such precision of phase shift can be generated at reasonable cost and the Trojan-to-circuit induced activity is higher than the background noise. As will be demonstrated in later experiment, the Trojan-to-circuit activity can be increased by reducing the cluster size and the background noise can be reduced by calibration. By varying the phase shift of clk_2 from $350ps$ to $550ps$, the high-to-low transition of V_{out} is detected in all but the first cluster when the phase of clk_2 stepped from $400ps$ to $450ps$. The falling transition of V_{out} of the first cluster is detected when the phase shift increased from $500ps$ to $550ps$. The CUT of the first cluster is indeed the only CUT among the four clusters that is embedded with a Trojan. The Trojan extended the active current duration by about $100ps$, which can be captured using a phase shift resolution of $50ps$. By increasing the step size $\delta/2$ of the phase shift to $150ps$, the falling transitions of V_{out} from all four clusters occurred at the same phase shift of clk_2, which means that the Trojan-infected and Trojan-free CUTs are indistinguishable. The resolution of the phase shift to successfully detect this Trojan may have to be further increased as the extra duration of the switching activity induced by the Trojan may be masked by the manufacturing process variations (PVs). PVs cause important physical and electronic parameters, such as the device length and width, and its threshold and saturation voltages to deviate from the nominal specifications [37].

Monte Carlo simulation method [38] can be adopted to introduce randomly sampled device parameter variations from a normal distribution. Each iteration of the Monte Carlo simulation represents a unique set of variations applied to a design. Table II shows the key parameter variations of GF $65nm$ CMOS technology used in our simulation. This information is provided by the foundry to represent the ranges of parameter

TABLE II
THE KEY PARAMETER VARIATIONS USED IN DYNAMIC TIMING ANALYSIS

Parameter	Unit	NMOS	PMOS
Channel length chip mean variation L	nm	± 5	± 5
Channel width chip mean variation W	nm	± 13	± 13
Long channel chip mean Vt	mV	± 43	± 45
Vtsat	mV	± 93	$+90 \sim -87$

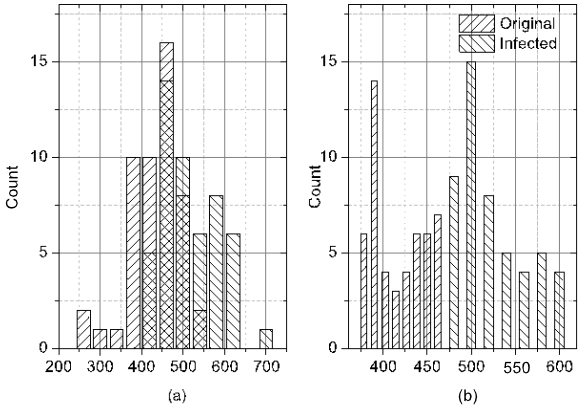

Fig. 13. Monte Carlo simulation results for the active current duration distributions: (a) before calibration, (b) after calibration.

TABLE III
STATISTICS OF FIG. 13

	Before PV calibration		After PV calibration	
	Original	Infected	Original	Infected
Average delay (ps)	430	517	421	520
Standard deviation (ps)	60	69	29	37
Max deviation (ps)	164	190	50	77

values of the physical design due to the manufacturing PVs. To demonstrate the effectiveness of our proposed calibration method, the post-layout statistical Monte Carlo simulation of 100 random process variation tests (50 tests each on Trojan-free and Trojan-infected designs) is performed to measure the actual active current duration of C2670 and compare against that of the golden model. At each iteration, a set of test vectors from the previous experiment are used. The distributions of the active current duration of the Trojan-free and Trojan-infected CUTs before the comparator is calibrated by V_p and V_n (see Section III-B) are shown in Fig. 13(a). The difference between the mean values of the two distributions is $87ps$, which is slightly lower than the value of $\delta = 100ps$ derived from our dynamic timing analysis without considering process variations. However, the standard deviations of both distributions exceeded $\delta/2$. The overlaps between the two histograms are tests that show no difference in the pulse widths of V_{out} between the Trojan-free and Trojan-infected CUTs due to the masking effect of PVs. Fig. 13(b) shows the distributions of the pulse width of V_{out} of the Trojan-free and Trojan-infected CUTs after the comparator threshold calibration proposed in Section III-B. The difference between the means of the two distributions has increased to $99ps$ and

TABLE IV
DETECTION ERROR RATE WITH AND WITHOUT PV CALIBRATION FOR SERIAL PLACEMENT OF TROJAN IN ISCAS'85 BENCHMARKS

Benchmark	Gates count	Trojan area overhead (%)	Detector area overhead (%)	Estimated DER from histograms (%)				DER with $\delta/2 = 50ps$ (%)			
				Uncalibrated		Calibrated		Uncalibrated		Calibrated	
				False negatives	False positives	False negatives	False positives	False negatives	False positives	False negatives	False positives
C432	160	8.1	2.3	10	10	0	0	10	10	0	0
C499	202	6.4	1.9	9	13	0	0	10	13	0	0
C880	383	3.4	0.98	14	12	0	0	14	12	0	0
C2670	1193	1.1	0.31	13	17	0	0	13	18	0	0
C3540	1669	0.78	0.23	15	16	0	1	15	17	0	1
C5315	2406	0.54	0.16	18	16	2	2	19	16	2	2
C6288	2406	0.54	0.16	20	16	2	1	20	17	2	2

the standard deviations have been lowered to below $\delta/2$ after calibration. In fact, the two distributions do not overlapped unlike Fig. 13(a). For ease of comparison, the statistics of the distributions of Fig. 13(a) before calibration and Fig. 13(b) after calibration are summarized in Table III. The delay difference between the Trojan-free and Trojan-infected circuits due to the process variations has been magnified after calibration, which increases the Trojan detection rate. The detection error rate (DER) can be estimated from the histograms of V_{out} pulse width as follows:

$$DER = \frac{F}{N} \tag{4}$$

where F is the number of matching V_{out} pulse widths between the Trojan-free and Trojan-infected histograms and N is the total number of tests. The DER includes the false negatives (accepting a Trojan-infected design as Trojan-free) and the false positives (rejecting a genuine design as Trojan-infected). To estimate the false positive and false negative rates from the histogram, we choose the mean value between the lowest and the highest active current durations of the overlapped areas of the histograms as threshold. Those tests in the overlapped areas that fall below the threshold are false positives and those above are false negatives. From Fig. 13, the DER is 30% (17 false positives and 13 false negatives) before calibration and 0% after calibration. It should be noted that the DER estimated from the histogram assumes that phase shift of clk_2 has infinitesimal resolution. In practice, the active current duration, i.e., the pulse width of V_{out}, is detected from the scan output of SC_2 by the transition delay test with a finite phase shift resolution of clk_2. Table IV shows the DER of the proposed method with and without the PV calibration for different ISCAS'85 benchmark circuits by embedding an 8-bit counter based Trojan in serial into a randomly selected timing path of a cluster. The Trojan and detector overheads are expressed as a percentage of their respective gate count over the gate count of the original design excluding the routing overheads. As our method requires only one scan register per cluster as opposed to one shallow register per path of [4] used in the delay-based HT detection methods [7], [8], the routing complexity of clock and scan enable signals is significantly lower. A post-layout statistical Monte Carlo simulation with a total of 100 runs of device variations were carried out on the Trojan-free and Trojan infected designs (50 runs each) for each benchmark circuit. The DER obtained based on the histogram of the actual pulse width of V_{out} and that detected by the transition delay test with $\delta/2 = 50ps$ are compared. Most circuits have zero DER for the PV-calibrated Trojan detector. The maximum DER is only 4% for C5315 and C6288 with the PV-calibration. The DER obtained by the transition delay test with $\delta/2 = 50ps$ is at most 1% worse than the DER estimated from the histograms with infinitesimal clock phase resolution for both the PV-uncalibrated and PV-calibrated detection.

D. Detection of Trojan With no Delay Impact

Trojan with rare switching impact has been demonstrated to be relative well detected by the transition delay test with the proposed current detector. Nevertheless, Trojan with no delay impact [15] may not be detected as successfully by the delay-based side channel signal analysis. This can be easily demonstrated by the static timing analysis. Fig. 14 shows the static timing analysis results for the Trojan-free design and the Trojan-infected design with the 8-bit counter-based Trojan embedded in serial and in parallel. The extra delay for the Trojan embedded in serial can be detected by the delay-based side channel analysis as shown in Fig. 14(a), but there is no observable delay difference from the primary inputs to the primary outputs when the Trojan is embedded in parallel, as shown in Fig. 14(b). Our proposed current detector provides a means to indirectly compare the amplitude of the switching current profile of a CUT against that of the Trojan-free CUT under the same excitation to detect such a Trojan. This is achieved by adjusting not only the phase shift of clk_2 but also the gate voltage V_{level} of M_{14}. Table V shows parts of the simulation result. Initially, V_{level} is set to be $0mV$. The phase shift of clk_2 is gradually increased until the falling edge of V_{out} is detected. No difference between the pulse width of V_{out} extracted from the Trojan-free chip and the Trojan-infected design at the same V_{level} is observed at the scan registers in SC_2. When V_{level} is increased to $600mV$, a rising transition at the phase shift of $450ps$ and a falling transition at the phase shift of $550ps$ are detected for the active cluster (Cluster 1 in this case) of the Trojan-infected circuit, whereas no transition is detected for the active cluster from the signature of the genuine design. This narrow pulse width of V_{out} is due to the additional current drawn by the Trojan. V_{level} is increased until V_{out} of the active cluster scanned out of SC_2 is '0' on the first phase shift of clk_2. If no transition in V_{level} is detected upon completion of the phase shift test at this V_{level}, the circuit is declared to be Trojan-free.

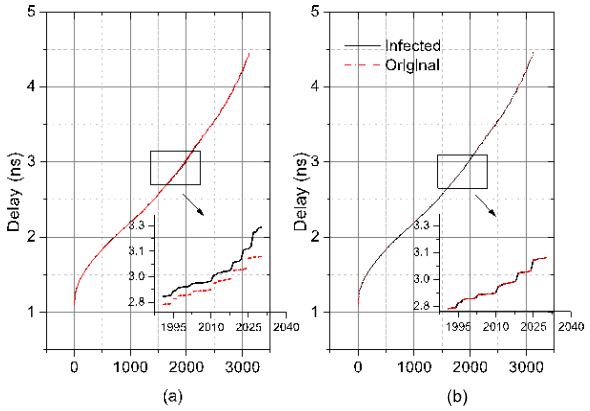

Fig. 14. The delay impacts with different placements of Trojan: (a) Trojan embedded in serial, (b) Trojan embedded in parallel.

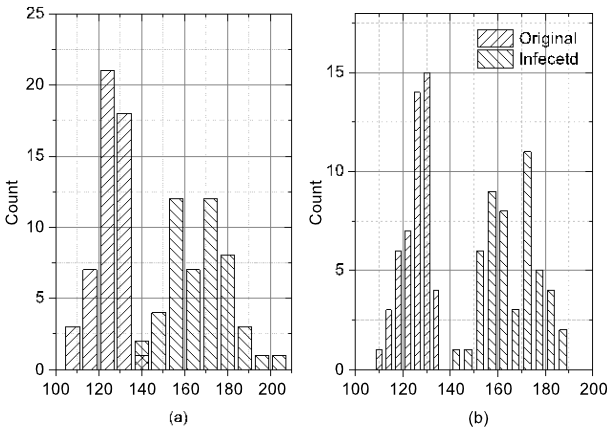

Fig. 15. Monte Carlo simulation results for the average active current amplitude distributions: (a) before calibration, (b) after calibration.

TABLE V
DETECTOR OUTPUTS FOR THE GENUINE AND INFECTED DESIGNS FOR TROJAN WITH NO DELAY IMPACT

No.	Clock period (ns)	Phase Shift (ps)	Scan outputs of detectors			
			$V_{level} = 0mV$		$V_{level} = 600mV$	
			Genuine	Infected	Genuine	Infected
5	5	350	1111	1111	0111	0111
6	5	400	1111	1111	0111	0111
7	5	450	1111	1111	0111	1111
8	5	500	1111	1111	0111	1111
9	5	550	1111	1111	0111	0111
10	5	600	1111	1111	0111	0111
11	5	650	0111	0111	0111	0111

TABLE VI
STATISTICS OF FIG. 15

	Before calibration		After calibration	
	Original	Infected	Original	Infected
Average current amplitude (μA)	125	167	126	168
Standard deviation (μA)	6.8	13.8	5.8	10.7
Max deviation (μA)	20.4	29.9	14.1	23.6

The effect of PV has a smaller influence on the amplitude difference introduced by the Trojan. Fig. 15 shows the 100 runs of Monte Carlo simulation results for the average active current amplitude distributions of V_{out} obtained from the Trojan-free and Trojan-infected C2670. Table VI shows the statistics of the histograms in Fig. 15. Calibration of the current comparator described in Section III-B does not lead to appreciable changes in the average current amplitude for both circuits. However, it helps to improve the detection sensitivity by lowering the standard deviation of the average active current amplitude of the Trojan-infected circuit. The standard deviation of the active current for Trojan-infected circuit has been reduced by about 22.5% by calibration, which is more substantial than the 14.7% reduction of standard deviation for the Trojan-free circuit. Before calibration, the DER estimated from the histograms is 3% with 1 false positive and 2 false negatives. It reduces to 0% after calibration. Table VII shows the DER of the proposed method with and without the PV calibration for different ISCAS'85 benchmark circuits by embedding an 8-bit counter based Trojan in parallel into a cluster. The DER estimation from the active current pulse amplitude of V_{out} produces perfect zero DER for all except C6288, which has only one false positive detection. The DER for each benchmark circuit was also obtained by the transition delay test with the same post-layout statistic Monte Carlo simulation of device variations on the Trojan-free and Trojan infected designs. The DER results for the uncalibrated current detector with finite phase shift resolution of clk_2 are the same as those estimated from the histogram. The finite resolution of the clock phase shift leads to only a slightly higher DER than that estimated from the histogram for the calibrated current detector. After the PV calibration, all Trojan-infected CUTs have been successfully detected except for C5315 which has a false positive and a false negative. Because the switching current amplitude contributed by this type of Trojan outweighs the PV, the rate of success for its detection is higher than the serially embedded Trojan even without the PV calibration.

It is observed that the false negatives/positives in Tables IV and VII grow with the size of the cluster due to the increase in circuit activity. For large and complex design, more clusters are needed to maintain the detection accuracy.

E. Scaling the Trojan

To evaluate the Trojan detection sensitivity of the proposed method, the size of the Trojan is scaled down by reducing the counter length. The Trojan circuits of different counter lengths are randomly inserted into the CUT (C2670) during the 100 runs of Monte Carlo simulation. The results in Table VIII show that the DERs obtained by the transition delay test with $\delta/2 = 50ps$ for the uncalibrated and PV-calibrated current detectors. The DER increases slightly as the Trojan size is scaled down. With the proposed PV calibration technique, the Trojan detection sensitivity has been improved significantly, especially when the parametric variation due to the Trojan is small and comparable to the process variations. Compared with the DER of 64% for the detection of a 4-bit counter based Trojan embedded in the one-round DES circuit with a Trojan area overhead of 0.76% in SMIC $0.13\mu m$ CMOS technology reported by the delay-based side channel analysis of [5],

TABLE VII
DETECTION ERROR RATE FOR TROJAN WITH NO DELAY IMPACT IN ISCAS'85 BENCHMARKS WITH AND WITHOUT PV CALIBRATION

Benchmark	Gates count	Trojan area overhead (%)	Detector area overhead (%)	DER from histograms (%)				DER with $\delta/2 = 50ps$ (%)			
				Uncalibrated		Calibrated		Uncalibrated		Calibrated	
				False negatives	False positives	False negatives	False positives	False negatives	False positives	False negatives	False positives
C432	160	8.1	2.3	0	0	0	0	0	0	0	0
C499	202	6.4	1.9	0	0	0	0	0	0	0	0
C880	383	3.4	0.98	0	0	0	0	0	0	0	0
C2670	1193	1.1	0.31	2	1	0	0	2	1	0	0
C3540	1669	0.78	0.23	1	1	0	0	1	1	0	0
C5315	2406	0.54	0.16	3	4	0	0	3	4	0	1
C6288	2406	0.54	0.16	3	3	0	1	3	3	1	1

TABLE VIII
DERS OF THE PROPOSED METHOD FOR DIFFERENT TROJAN AREA OVERHEADS

Counter length	8-bit	4-bit	2-bit	1-bit
Trojan area overhead	1.09%	0.58%	0.34%	0.21%
DER (un-calibrated)	15%	16%	16%	20%
DER (calibrated)	0%	1%	2%	2%

our method has a much greater accuracy. Similar 4-bit counter based Trojan with a Trojan area overhead of 0.58% can be detected by our proposed method with a DER of as low as 1% despite simulated in a 65*nm* technology node with higher variations.

F. Sensor Security

Our proposed detector forms an integral part of the power grid, which makes its removal or tampering much easier to be detected than the Trojan itself from the deteriorated circuit performance and structural test results. As the power grid is extremely sensitive to any small change in current, the sensing resistance R_{on} can be placed as close as possible to the power supply node so that the Trojan cannot be strategically placed to evade detection. Since the Trojan draws the same amount of current regardless of its location, the additional current flows at the power supply node will always be sensed by R_{on}. If the attacker has access to the reference pattern of a cluster, he may implant a Trojan in that cluster and resize the calibration transistors M_9 and M_{10} of Fig. 6 to mask the positive delay offset of the Trojan. However, this negative delay offset created by the attacker will be added to the remaining paths in the same cluster. When other random patterns activate these paths, a discernible "negative" deviation of the signatures from those of the golden chip will be detected, which indicates that its calibration circuit has been tampered. Another possible attack is to sensitize the paths under all possible excitations including the reference patterns and then replace the scan registers of the scan chain by a non-volatile memory. However, the memory required to store the responses to these excitations is extremely large. Its area and power consumption are conspicuous and can be easily detected by basic side channel analysis.

V. CONCLUSION

This paper suggests a new possibility of detecting the presence of hardware Trojan in an IC through sensing its local active current based on the power gating technology. A novel on-chip active current sensing circuit that comprises a current mirror, a current comparator with adjustable threshold and a multiplexor-based scan register is proposed to detect the commencement and ceasing of switching current on local power grid when timing paths around the region are sensitized. The active current duration captured by the detector can be easily decoded from the scan output by a structural test methodology. In contrary to many other delay-based side channel analysis, this method can detect the Trojan with no delay impact by analyzing the deviation in current amplitudes. The detector is built with a calibrator to adjust the current comparator threshold against process variations. Its improved Trojan detection sensitivity has been demonstrated by the post layout Monte Carlo simulation. As the proposed sensor enables at-speed test without affecting the normal circuit timing and functionality, it can be incorporated into the real-time trust evaluation framework [16] to monitor the active current timing and duration in the field. When an HT is activated during normal circuit operation, the measured characteristics of the power trace will change dramatically to alert for anomalies. Such in situ monitoring is particularly useful for detecting sophisticated Trojans that have escaped the pre-deployment test.

REFERENCES

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

[2] "Report of the defense science board task force on high performance microchip supply," Office of the Under Secretary of Defense for Acquisition, Technol., and Logistics, Defense Science Board (DSB), U.S. Department of Defense, Washington, DC, USA, Tech. Rep., Feb. 2005.

[3] X. Wang, M. Tehranipoor, and J. Plusquellic, "Detecting malicious inclusions in secure hardware: Challenges and solutions," in *Proc. IEEE Int. Workshop Hardw.-Oriented Security Trust*, San Francisco, CA, USA, Jun. 2008, pp. 15–19.

[4] J. Li and J. Lach, "At-speed delay characterization for IC authentication and Trojan Horse detection," in *Proc. IEEE Int. Workshop Hardw.-Oriented Security Trust*, San Francisco, CA, USA, Jun. 2008, pp. 8–14.

[5] Y. Jin and Y. Makris, "Hardware Trojan detection using path delay fingerprint," in *Proc. IEEE Int. Workshop Hardw.-Oriented Security Trust*, San Francisco, CA, USA, Jun. 2008, pp. 51–57.

[6] M. Li, A. Davoodi, and M. Tehranipoor, "A sensor-assisted self-authentication framework for hardware Trojan detection," in *Proc. Design, Autom. Test Eur. Conf. Exhibit. (DATE)*, Dresden, Germany, Mar. 2012, pp. 1331–1336.

[7] B. Cha and S. K. Gupta, "Efficient Trojan detection via calibration of process variations," in *Proc. IEEE 21st Asian Test Symp. (ATS)*, Niigata, Japan, Nov. 2012, pp. 19–22.

[8] B. Cha and S. K. Gupta, "Trojan detection via delay measurements: A new approach to select paths and vectors to maximize effectiveness and minimize cost," in *Proc. Design, Autom. Test Eur. Conf. Exhibit. (DATE)*, Grenoble, France, Mar. 2013, pp. 18–22.

[9] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, and B. Sunar, "Trojan detection using IC fingerprinting," in *Proc. IEEE Symp. Security Privacy*, Berkeley, CA, USA, May 2007, pp. 296–310.

[10] M. Banga and M. S. Hsiao, "A region based approach for the identification of hardware Trojans," in *Proc. IEEE Int. Workshop Hardw.-Oriented Security Trust*, San Francisco, CA, USA, Jun. 2008, pp. 40–47.

[11] R. Rad, J. Plusquellic, and M. Tehranipoor, "A sensitivity analysis of power signal methods for detecting hardware Trojans under real process and environmental conditions," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 18, no. 12, pp. 1735–1744, Dec. 2010.

[12] I. Verbauwhede and P. Schaumont, "Design methods for security and trust," in *Proc. Design, Autom. Test Eur. Conf.*, Nice, France, Apr. 2007, pp. 672–677.

[13] H. Salmani and M. Tehranipoor, "Layout-aware switching activity localization to enhance hardware Trojan detection," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 76–87, Feb. 2012.

[14] S. Narasimhan, X. Wang, D. Du, R. S. Chakraborty, and S. Bhunia, "TeSR: A robust temporal self-referencing approach for hardware Trojan detection," in *Proc. IEEE Int. Symp. Hardw.-Oriented Security Trust (HOST)*, San Diego, CA, USA, Jun. 2011, pp. 71–74.

[15] S. Wei, K. Li, F. Koushanfar, and M. Potkonjak, "Hardware Trojan horse benchmark via optimal creation and placement of malicious circuitry," in *Proc. 49th Annu. Design Autom. Conf. (DAC)*, San Francisco, CA, USA, Jun. 2012, pp. 90–95.

[16] Y. Jin and D. Sullivan, "Real-time trust evaluation in integrated circuits," in *Proc. Design, Autom. Test Eur. Conf. Exhibit. (DATE)*, Dresden, Germany, Mar. 2014, pp. 1–6.

[17] C. Lamech, R. M. Rad, M. Tehranipoor, and J. Plusquellic, "An experimental analysis of power and delay signal-to-noise requirements for detecting Trojans and methods for achieving the required detection sensitivities," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 1170–1179, Sep. 2011.

[18] S. Wei and M. Potkonjak, "Scalable segmentation-based malicious circuitry detection and diagnosis," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Design*, San Jose, CA, USA, Nov. 2010, pp. 483–486.

[19] S. Wei and M. Potkonjak, "Integrated circuit security techniques using variable supply voltage," in *Proc. 48th ACM/EDAC/IEEE Design Autom. Conf.*, San Diego, CA, USA, Jun. 2011, pp. 248–253.

[20] S. Wei and M. Potkonjak, "Scalable consistency-based hardware Trojan detection and diagnosis," in *Proc. 5th Int. Conf. Netw. Syst. Security (NSS)*, Milan, Italy, Sep. 2011, pp. 176–183.

[21] S. Wei and M. Potkonjak, "Scalable hardware Trojan diagnosis," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 20, no. 6, pp. 1049–1057, Jun. 2012.

[22] E. Pakbaznia and M. Pedram, "Coarse-grain MTCMOS sleep transistor sizing using delay budgeting," in *Proc. Design, Autom. Test Eur. Conf. (DATE)*, Munich, Germany, Mar. 2008, pp. 385–390.

[23] S. Bhunia, H. Mahmoodi, D. Ghosh, and K. Roy, "Power reduction in test-per-scan BIST with supply gating and efficient scan partitioning," in *Proc. 6th Int. Symp. Quality Electron. Design (ISQED)*, San Jose, CA, USA, Mar. 2005, pp. 453–458.

[24] A. A. A. Bsoul and S. J. E. Wilton, "An FPGA architecture supporting dynamically controlled power gating," in *Proc. Int. Conf. Field-Program. Technol. (FPT)*, Beijing, China, Dec. 2010, pp. 1–8.

[25] L. Whetsel, "Adapting scan architectures for low power operation," in *Proc. Int. Test Conf.*, Atlantic City, NJ, USA, Oct. 2000, pp. 863–872.

[26] Y. Cao, C.-H. Chang, and S. Chen, "Cluster-based distributed active current timer for hardware Trojan detection," in *Proc. IEEE Int. Symp. Circuits Syst.*, Beijing, China, May 2013, pp. 1010–1013.

[27] Y. Jin, N. Kupp, and Y. Makris, "Experiences in hardware Trojan design and implementation," in *Proc. IEEE Int. Workshop Hardw.-Oriented Security Trust*, Francisco, CA, USA, Jul. 2009, pp. 50–57.

[28] K. Hu, A. Nowroz, S. Reda, and F. Koushanfar, "High-sensitivity hardware Trojan detection using multimodal characterization," in *Proc. Design, Autom. Test Eur. Conf. Exhibit. (DATE)*, Grenoble, France, Mar. 2013, pp. 1271–1276.

[29] I. Pecuh, M. Margala, and V. Stopjakova, "1.5 volts Iddq/Iddt current monitor," in *Proc. IEEE Can. Conf. Elect. Comput. Eng.*, Edmonton, AB, Canada, May 1999, pp. 472–476.

[30] M. Anis, S. Areibi, M. Mahmoud, and M. Elmasry, "Dynamic and leakage power reduction in MTCMOS circuits using an automated efficient gate clustering technique," in *Proc. 39th Design Autom. Conf. (DAC)*, New Orleans, LA, USA, Jun. 2002, pp. 480–485.

[31] H. Traff, "Novel approach to high speed CMOS current comparators," *Electron. Lett.*, vol. 28, no. 3, pp. 310–312, Jan. 1992.

[32] I. Park and E. J. McCluskey, "Launch-on-shift-capture transition tests," in *Proc. IEEE Int. Test Conf.*, Santa Clara, CA, USA, Oct. 2008, pp. 1–9.

[33] *ISCAS'85 Benchmarks Circuits*. [Online]. Available: http://web.eecs.umich.edu/~jhayes/iscas.restore/, accessed Feb. 4, 2014.

[34] D. Rai and J. Lach, "Performance of delay-based Trojan detection techniques under parameter variations," in *Proc. IEEE Int. Hardw.-Oriented Security Trust (HOST)*, Francisco, CA, USA, Jul. 2009, pp. 58–65.

[35] H. Liu, H. Luo, and L. Wang, "Design of hardware Trojan horse based on counter," in *Proc. Int. Conf. Quality, Rel., Risk, Maintenance, Safety Eng. (ICQR2MSE)*, Bangkok, Thailand, Jun. 2011, pp. 1007–1009.

[36] M. Saint-Laurent and M. Swaminathan, "A digitally adjustable resistor for path delay characterization in high-frequency microprocessors," in *Proc. Southwest Symp. Mixed-Signal Design*, Austin, TX, USA, Feb. 2001, pp. 61–64.

[37] S. Borkar, T. Karnik, S. Narendra, J. Tschanz, A. Keshavarzi, and V. De, "Parameter variations and impact on circuits and microarchitecture," in *Proc. Design Autom. Conf. (DAC)*, San Francisco, CA, USA, Jun. 2003, pp. 338–342.

[38] L. Lin, S. Srivathsa, D. K. Krishnappa, P. Shabadi, and W. Burleson, "Design and validation of arbiter-based PUFs for sub-45-nm low-power security applications," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 4, pp. 1394–1403, Aug. 2012.

Yuan Cao (S'09) received the B.S. degree from Nanjing University, Nanjing, China, in 2008, and the M.E. degree from the Hong Kong University of Science and Technology, Hong Kong, in 2010. He is currently pursuing the Ph.D. degree in electrical and electronic engineering with Nanyang Technological University (NTU), Singapore.

He is with VIRTUS, IC Design Centre of Excellence Center, NTU. His research interests include hardware security, application-specified integrated circuit physical unclonable function, and analog/mixed-signal very large scale integration circuits and systems.

Chip-Hong Chang (S'92–M'98–SM'03) received the B.Eng. (Hons.) degree from the National University of Singapore, Singapore, in 1989, and the M.Eng. and Ph.D. degrees from Nanyang Technological University (NTU), Singapore, in 1993 and 1998, respectively. He served as a Technical Consultant in the industry prior to joining the School of Electrical and Electronic Engineering at NTU in 1999, where he is currently an Associate Professor. He holds joint appointments at NTU as the Assistant Chair of Alumni of the School of Electrical and Electronic Engineering from 2008 to 2014, the Deputy Director of the Center for High Performance Embedded Systems from 2000 to 2011, and the Program Director of the Center for Integrated Circuits and Systems from 2003 to 2009. He has coedited one book, published four book chapters, and more than 200 research papers in refereed international journals and conferences. His current research interests include hardware security and trust, low-power and fault-tolerant arithmetic circuits, and digital filter design.

Dr. Chang has served as an Associate Editor of the IEEE ACCESS since 2013, the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS I from 2010 to 2013, the IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS since 2011, *Integration*, the *VLSI Journal* since 2013, and the *Microelectronics Journal* since 2014, and an Editorial Advisory Board Member of the *Open Electrical and Electronic Engineering Journal* and the *Journal of Electrical and Computer Engineering*. He was also a guest editer for several journal special issues and served on many international conference advisory and technical program committees. He is a Fellow of the Institution of Engineering and Technology.

Shoushun Chen (M'05–SM'13) received the B.S. degree from Peking University, Beijing, China, in 2000, the M.E. degree from the Chinese Academy of Sciences, Beijing, in 2003, and the Ph.D. degree from the Hong Kong University of Science and Technology, Hong Kong, in 2007.

He held a Post-Doctoral Research Fellowship with the Department of Electronic and Computer Engineering, Hong Kong University of Science and Technology, for one year after graduation. From 2008 to 2009, he was a Post-Doctoral Research Associate with the Department of Electrical Engineering, Yale University, New Haven, CT, USA. In 2009, he joined Nanyang Technological University (NTU), Singapore, as an Assistant Professor.

Dr. Chen serves as a Technical Committee Member of Sensory Systems and the IEEE Circuits and Systems Society, an Associate Editor of the IEEE SENSORS JOURNAL, and the Program Director (Smart Sensors) of VIRTUS, IC Design Centre of Excellence, NTU. His research interests include smart vision sensors, motion detection sensors, energy-efficient algorithms for bioinspired vision, and analog/mixed-signal very large scale integration circuits and systems.