Cluster-based Distributed Active Current Timer for Hardware Trojan Detection

Yuan Cao, Chip-Hong Chang and Shoushun Chen
School of Electrical and Electronic Engineering, Nanyang Technological University

***Abstract*—With the globalization of integrated circuit (IC) design and fabrication, there is a growing concern on the devastating impact of subverted chip supply. This paper presents a current sensing circuit that converts the current activity on local power grid to a timing pulse to detect if an IC is Trojan-infected. This new approach increases the Trojan detection sensitivity by combining the switching activity and path sensitization abnormalities into a single side-channel signal that can be easily monitored by existing scan test structure. One main advantage of the proposed regional Trojan detector is that the current comparator threshold can be calibrated against the quiescent current noise floor to reduce the impacts of process variations. Experiments are performed on a Trojan-infected benchmark circuit to demonstrate the feasibility of the proposed technique.**

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 may potentially leak confidential information controlled by the chip or cause catastrophic damages to valuable electronic systems and infrastructures any time upon triggered by random or unknown condition.

Even though it is impossible to model all possible Trojan placements, structures, functions, sizes, etc. and the Trojan will not affect the circuit's functionality, 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 many challenges [3]-[8]. 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 main advantage of side-channel analysis is the Trojans can be detected without being fully triggered [8]. Examples of popular side channel analysis methods include time-based analysis [3], [4] and power-based analysis [5]-[7]. Time-based side channel analysis can succeed in hardware Trojan detection if the additional delay due to the Trojan is distinguishable from the delay difference caused by process variations. One such method [3] adds a "shadow register" to latch the data of the destination register of a path. The shadow register clock has the same frequency as the main clock, but with adjustable phase shift to measure the path delay. The method suffers from a high area overhead due to the extra register and comparator for every path to be monitored. The dedicated "shadow clock" also complicates the clock distribution networks and clock skews may become a critical timing problem. Furthermore, Trojans inserted in the internal nodes for the design without primary inputs or outputs cannot be detected by this approach. On the other hand, power-based side-channel analysis provides the visibility of the chip's internal switching activities. In [5], random input patterns are applied to obtain a power signature for comparison with that of the Trojan-free chip. The main problem of this method is its sensitivity to random noise induced by the process and temperature variations. To reduce the variability, advanced power-based analysis methods partition the entire chip into several regions to magnify the Trojan-to-circuit activity [6]. The drawback is each region has to have its own power ports for the power signature analysis.

This paper proposes an active current sensor to extract the timing signature of a chip for hardware Trojan detection. Unlike other timing-based analyses, it senses the power supply transient (I_{DDT}) rather than directly observing the path delay. The proposed circuit can 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 the scan latches. This is because Trojan infected circuit can cause errant timing behaviors that are often show up in logic as power supply droop, which can be picked up by monitoring the supply current. Our proposed design includes a simple tunable threshold current comparator that can be calibrated to maximally discriminate between transient and static currents, and a multiplexer based scan register to enable its transition-delay to be detected at the scan output vectors by AC scan test with a pulse width modulated clock.

II. Percept of Proposed Side-channel Analysis

I_{DDT} conveys the unitary profile of switching activity and timing information of the sensitized paths in a chip. Fig. 1(a) shows the I_{DDT}, input and output voltage waveforms when an arbitrarily selected data path of ISCAS'85 benchmark 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 path is $1.1836ns$ based on the 50%-to-50% full swing voltage delay definition. The commencement and ending of the active switching current is clearly discernible from the quiescent current and its duration ($1.1836ns$) is the same as the propagation delay of the sensitized path. This timing signature of a subcircuit is shown to be susceptible to subtle functional and topological modifications. Fig. 1(b) demonstrates the transient current differences between a

Trojan-free and a Trojan-infected path of C432. The Trojan inserted into this path consists of 7 different logic gates, which contributes approximately 4% of additional logic to this path. Trojan induced current spikes can evoke momentarily supply voltage droop and increase the path delay. Thus, Trojan-infected path is distinguishable from the Trojan-free path with an elongated active current duration due to its extraneous switching.

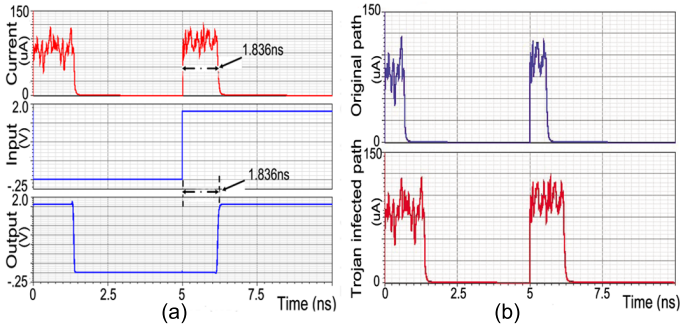

Fig. 1. Waveforms for (a) a sensitized path. (b) currents of Trojan-free and Trojan-infected paths.

Analogous to the deployment of on-chip thermal sensors for dynamic thermal management, small current sensors can be implanted to aid a more accurate post-silicon Trojan detection and diagnosis. During the design phase, the circuit is divided into regions and a current detector is inserted into each region to sense the transient current from the power strap or trunk of the power grid. By amortizing circuit activity into regions, extraneous activity that transcend regular circuit activity and process variations are more likely to be detected by the cluster-based current sensors in those regions where the Trojan resided. Therefore, the number of regions is a tradeoff between the resolution of the Trojan and the sensor overhead. The flow of the Trojan detection is shown in Fig. 2. Random non-functional test patterns are applied to locally activate the target region while keeping the remaining regions inactive or at low activity. The timing signature extracted from the regional current detector is compared with that of the Trojan-free chip for the same test pattern. If the difference in timing signatures of any region exceeds a threshold determined by the process variance, it signifies a probable existence of a Trojan in that region. If none of the regions exhibit an above threshold timing difference, the chip is most probably Trojan free for the detectable resolution.

In this paper, we focus on the design of current sensor to measure the duration of transient current pulses upon activation of a number of circuit paths in a target region by an input pattern, which can be applied through the scan chain.

III. Scan-enabled active current timing sensor

The schematic of the proposed active current timing sensor is shown in Fig. 3, where CUT refers to the cluster under test. For each region, only 12 additional transistors and 1 scan flip-flop (FF) are required for the active current timing sensor as opposed to 1 comparator, 1 shadow register, dual clocks and 1 FF to lock the result bit required by the shadow register technology for each path under test. Its principle of operation as a Trojan detector is explained as follows: a resistor R is

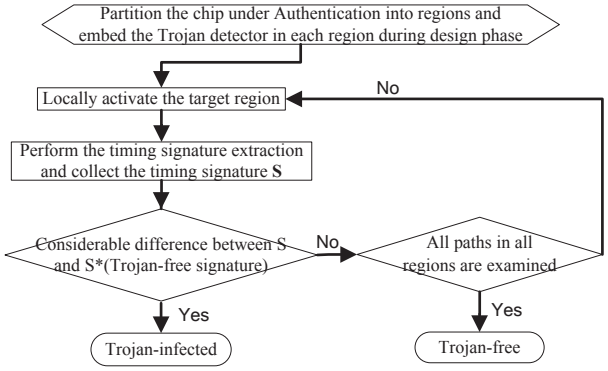

Fig. 2. The proposed hardware Trojan detection flow.

used to sense the switching current of the CUT from the power supply. The dynamic current is mirrored to a current comparator to produce two voltage transitions that mark the path delay. The delay transition is detected by latching the comparator output into a scan flip-flop and propagating it to the scan output using a variable duty cycle sampling clock (clk). The operations of each subcircuit are detailed as follows.

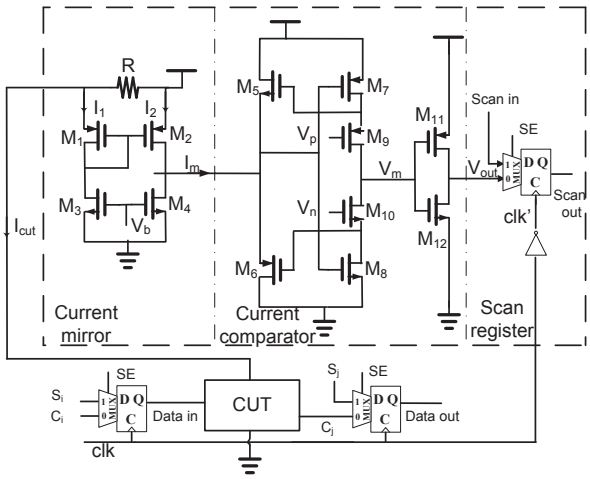

Fig. 3. Schematic of the proposed current sensing to path delay monitoring circuit.

A. Current mirror

The current mirror utilizes the current monitor [9] originally developed for the I_{DDQ}/I_{DDT} testing. 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 R when the current I_{cut} drawn by the active circuit passing through R. This voltage drop causes a difference in the gate-source voltages of transistor pair (M_1/M_2) and the mirrored current $I_m = I_2 - I_1$ is given by [9]:

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

where μ_p, C_{ox} and V_t are the hole mobility, oxide capacitance and threshold voltage of the transistor, respectively.

The most important component is the sensing resistor R. If R is too small, the current sensitivity is poor. If R is too large, M_1 will get into the subthreshold region. To limit the supply

voltage droop to less than 5%, $(I_{cut} + I_1)R < 0.05V_{dd}$. R is determined to be 50Ω by parametric simulation.

B. Current comparator

The current comparator compares the mirrored current against the quiescent current threshold to produce a high output voltage during the period of activity and a low voltage level when all sensitized path transitions have settled. The proposed current comparator circuit shown in Fig 3 is modified from Traff's current comparator [10]. 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}, biased in the linear region. This pair of transistors 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 3 to restore its rail-to-rail output. These two transistors have another advantage that they act as two voltage-controlled linear resistors. The charge and discharge 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 account for the minute difference in quiescent currents of different chips due to the process variations.

C. Scan register

The current comparator output V_{out} is fed to a standard multiplexer-based scan FF so that transition delay test [12] can be applied to propagate the transition of V_{out} to the scan output. Once the input data is loaded through the scan chain to the CUT, the scan shift enable signal SE is deasserted to allow the rising edge of the clock signal to launch the input data into the CUT and produce a low-to-high transition on V_{out}. The logic level of V_{out} will be latched into the scan FF at the falling edge of the clock. The falling edge triggered scan FFs of all detectors are chained together to enable their V_{out} to be propagated to an observable output by asserting SE. The process is repeated by launching the same input data with different capturing times when SE is deasserted until a high-to-low transition is detected in the same bit position of the scan output. To sample the transition of V_{out} to an observable output, the on-time of the duty-cycle modulated clock 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 incremented in timing steps of $\delta/2$ until the logic '0' of V_{out} is captured, where δ is the minimum timing elongation due to the smallest detectable Trojan. The timing diagram is shown in Fig. 4. Idle cycles are inserted to allow the CUT to recover from the supply voltage droop and heat dissipation due to the data scanning operation. Clock pulse is disabled and primary inputs are held constant during the idle cycles.

IV. Results and Discussion

To test the effectiveness of our proposed Trojan detector, a counter based hardware Trojan [11] shown in Fig. 5 is inserted into ISCAS'85 C432 benchmark at internal signal nodes. The

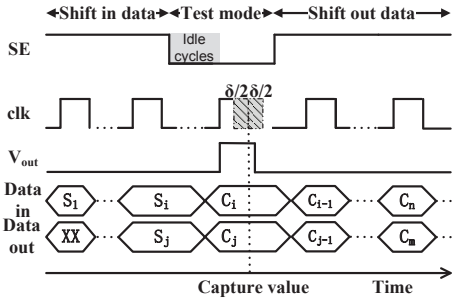

Fig. 4. The timing diagram for the sampling of transition delay.

8-bit counter is clocked by the NAND gate output, which has its inputs a and b connected to some internal signals of C432. When the counter exceeds a predefined number n, it triggers the Trojan and alters the $Result$ of the payload to $*Result$. n is set to 1000000 to reduce the chance for it to be detected by functional testing. The active current sensors presented in Section III are embedded in four clusters of C432. The Trojan-free and Trojan infected designs are synthesized using CSM $0.18\mu m$ CMOS standard cell technology. Fig. 6 shows the simulation results at each node of a current sensor in the Trojan-free design. Although the sampled current I_m from the power node for the path is several orders smaller than I_{cut}, the sensitized duration is accurately detected by the current comparator and compared against the active time span of the pulse-width modulated clock clk. By varying the duty cycle of clk from 38% to 58% in step size of $\delta/2 = 4\% = 0.2ns$, the high-to-low transition of V_{out} in region 1 is detected between 42% and 46% duty cycle of the genuine circuit while it is delayed till duty cycle 50% and 54% for the infected circuit, as shown in Table I. Since the timing difference is equal to $\delta = 0.4ns$, the Trojan is found by the detector in region 1 where it was inserted.

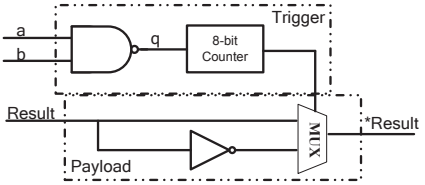

Fig. 5. Counter-based Trojan circuit architecture.

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

No.	Clock period (ns)	Duty cycle	Scan outputs of detectors	
			Genuine	Infected
1	5	38%	1111	1111
2	5	42%	**1111**	1111
3	5	46%	**0000**	1000
4	5	50%	0000	**1000**
5	5	54%	0000	**0000**
6	5	58%	0000	0000

Fig. 7 (a) shows the pulse width of V_{out} of the active current timing sensor versus the input current width simulated by Cadence Spectre simulator, where f, s and t denote the fast, slow and typical corners of the process. The process variations

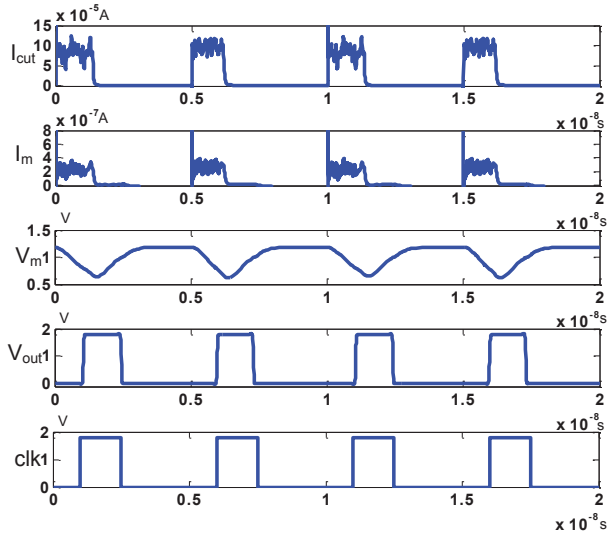

Fig. 6. The waveform on each node of active current timing sensor.

introduce an offset in the linearly related input and output delays. By adjusting the gate voltages V_p and V_n of the current comparator, this offset can be nullified as shown in Fig. 7 (b).

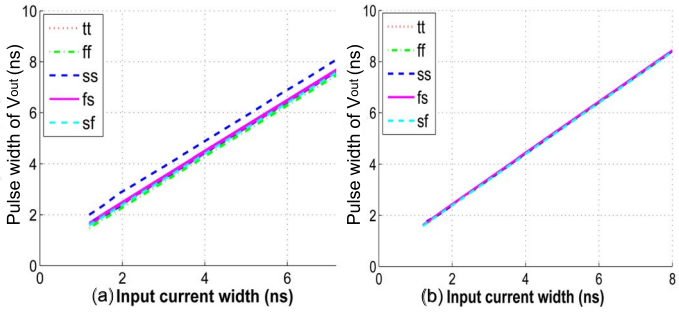

Fig. 7. (a) Corner simulation result without calibration, (b) corner simulation result with calibration.

A Monte Carlo simulation of 50 samples is also run for an arbitrary path delay in C432 by Spectre. Fig. 8 illustrates the normalized delays contributed by the Trojan and the path delays measured by the pulse width of V_{out} with and without the threshold calibration. From the figure, the variation for the path delay is smaller with the calibration. Table II compares the statistics of the path delay measured based on the 50%-to-50% delay definition adopted by [3] and the pulse width of V_{out} obtained by our Trojan detector with calibration. The results show that our sensing method has a lower standard deviation and noticeably smaller peak deviation.

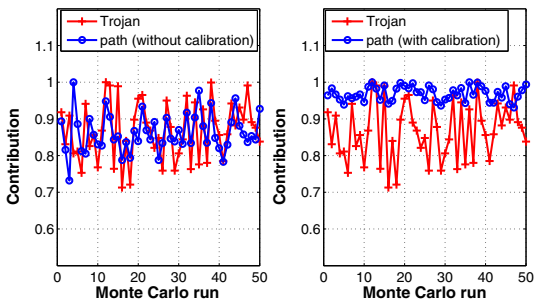

Fig. 8. Monte Carlo simulation result of a path delay in C432.

TABLE II
COMPARISON OF PATH DELAY MEASURED BASED ON 50%-TO-50% DELAY DEFINITION AND OUR PROPOSED METHOD

Method	50% to 50% definition	Proposed
Average delay (ps)	655.08	1908.3
Standard deviation (ps)	40.17	38.96
Max deviation (ps)	104.86	73.75

.

V. Conclusion

This paper suggests a new possibility of detecting the presence of hardware Trojan in an IC through sensing its local active current duration. A novel 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 and register 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. 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 Monte Carlo simulation.

Acknowledgment

The authors would like to thank the Advantest Corporation for the support of this research.

References

[1] M. Tehranipoor and F. Koushanfar, "A survey of hardware Trojan taxonomy and detection," *IEEE Design 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", *Defense Science Board, US DoD,* Feb. 2005.

[3] J. Li and J. Lach, "At-speed delay characterization for IC authentication and Trojan horse detection," in *Proc. IEEE Int. Workshop Hardware-Oriented Security and Trust (HOST 08),* San Francisco, USA, June 2008, pp. 8-14.

[4] Y. Jin and Y. Makris, "Hardware Trojan detection using path delay fingerprint," in *Proc. IEEE Int. Workshop Hardware-Oriented Security and Trust (HOST 08),* San Francisco, USA, June 2008, pp. 51-57.

[5] Y. Alkabani and F. Koushanfar, "Active hardware metering for intellectual property protection and security," in *Proc. 16th Usenix Security Symp.,* Boston, USA, Aug. 2007, pp. 291-306.

[6] M. Banga and M. Hsiao, "A region based approach for the identification of hardware Trojans," in *Proc. IEEE Int. Workshop Hardware-Oriented Security and Trust (HOST 08),* San Francisco, USA, June 2008, pp. 40-47.

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

[8] X. Wang, M. Tehranipoor, and J. Plusquellic, "Detecting malicious inclusions in secure hardware: challenges and solutions," in *Proc. IEEE Int. Hardware-Oriented Security and Trust (HOST),* San Francisco, USA, June 2008, pp. 15-19.

[9] I. Pecuh, M. Margala, and V. Stopjakova, "1.5 Volts Iddq / Iddt current monitor," in *Proc. IEEE Canadian Conf. on Electrical and Computer Engineering,* Alberta, Canada, May 1999, pp. 472-476.

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

[11] H. Liu, H. Luo, and L. Wang, "Design of hardware Trojan horse based on counter," in *Int. Conf. on Quality, Reliability, Risk, Maintenance, and Safety Engineering ($ICQR^2MSE$),* Bangkok, Thailand, June 2011, pp. 1007-1009.

[12] I. Park and E. J. McCluskey, " Launch-on-Shift-Capture Transition Tests," in *Proc. IEEE Int. Test Conference,* Santa Clara, USA, Oct. 2008, pp. 1-9.