Improving IC Security Against Trojan Attacks Through Integration of Security Monitors

Seetharam Narasimhan, Xinmu Wang, and Swarup Bhunia
Case Western Reserve University

Wen Yueh and Saibal Mukhopadhyay
Georgia Tech

Editor's notes:
This paper describes using on-chip monitors to significantly improve the sensitivity of side-channel signal analysis techniques to malicious inclusions in integrated circuits known as hardware Trojans.
—Mohammad Tehranipoor, University of Connecticut

Security of electronic circuits is rapidly becoming a critical design parameter. Among various hardware security and trust issues, a relatively recent but serious threat deals with malicious modification of a design by an adversary—either during design or fabrication. These attacks, popularly known as *hardware Trojan* attacks, are poised to greatly affect the design and test landscape of ICs due to increasing use of untrusted intellectual properties and tools in the design flow and outsourcing of fabrication services to untrusted foundries [1]. Figure 1a shows a simple hardware Trojan circuit, which flips an internal node value (S) when a Boolean condition $a'bc$ evaluates to true. Figure 1b shows insertion of a Trojan inside a system on chip (SoC). Existing research have exposed vulnerability of a design to various forms of Trojan attacks [1], [2]. They have also shown these Trojans can easily evade conventional postsilicon test and validation approaches [2] and manifest themselves during in-field operation often with catastrophic consequences, especially in security-critical applications.

In the past, various approaches to detect hardware Trojans during post-manufacturing test have been proposed [1]. These approaches either aim at detecting Trojan effects in functional behavior of a chip [2] or in side-channel signature such as current or delay [3]–[8]. The first class of solutions is shown to be generally effective for detecting Trojans of very small size [2]. However, they greatly suffer from the difficulty of triggering an unknown Trojan and observing its malicious effect in logic values at primary outputs. On the other hand, side-channel analysis, primarily focusing on supply current analysis, has emerged as an attractive class of validation approach primarily due to the ease of test generation. Moreover, some Trojans which do not affect any logic value directly, but use side-channels to leak secret information from the IC [9], cannot be detected through functional testing approaches. Other Trojans that would also evade logic testing include "reliability" Trojans, which are realized by alteration of transistor sizes, coupling wires, or process steps, to cause potential malfunctions after long periods of

Digital Object Identifier 10.1109/MDT.2012.2210183
Date of publication: 24 July 2012; date of current version: 23 October 2012.

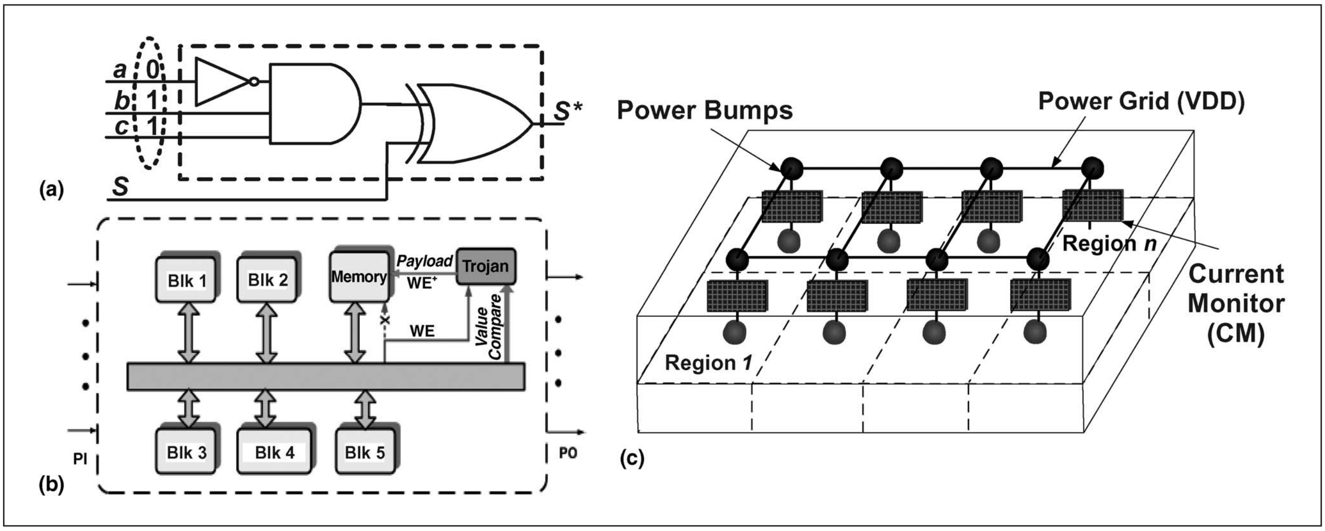

Figure 1. (a) An example Trojan circuit. (b) A Trojan inserted in a system-on-chip to maliciously alter memory write enable (WE). (c) On-chip current monitors for increasing sensitivity of side-channel analysis-based Trojan detection.

operation. Side-channel analysis can be effective in detecting these Trojan attacks.

However, the major challenge with side-channel analysis is that a small Trojan (e.g., of size 10–100 transistors) in a large multimillion transistor design would induce a barely noticeable effect in supply current, even with the best available measuring instrument, and intelligent vector generation. In other words, the "detection sensitivity", measured as the percentage deviation in supply current due to a Trojan, is too low to identify a Trojan reliably. The problem of reduced detection sensitivity is greatly accentuated by the noise due to process and environmental fluctuations [5]. Similar to testing for faults and functional bugs, Trojan detection can also benefit from specially crafted on-chip embedded structures. Such design solutions are referred to as *Design-for-Security (DfS)* techniques, such as ring-oscillators [4] to detect delay variations and modified scan flip-flops [1] to increase Trojan trigger probability. In addition to DfS approaches, several sensitivity improvement techniques have been proposed for the external supply current based Trojan detection. By using multiple parameters (e.g., supply current along with maximum operating frequency) [5] or through comparative analysis of current signatures from various parts of the same chip [6], [7], one can increase the detection sensitivity even in the presence of process variations. Region-based approaches [8] that exploit the presence of multiple power pins can help increase the sensitivity of Trojan detection. However, the off-chip current measurement circuitry still limits the detection sensitivity for ultrasmall Trojans.

In this paper, we propose monitoring of supply current inside an IC through insertion of an array of on-chip current sensors. We consider dynamic supply current analysis for identifying malicious circuitry or Trojans. Such DfS structures result in significantly higher detection sensitivity than conventional off-chip current monitoring based approaches. Moreover, they provide a scalable solution for designs of arbitrary size and complexity as well as Trojans of various forms and sizes. We propose efficient implementation of these on-chip sensors to minimize the design overhead in terms of area, power and performance, while providing high resolution of sensed current. We note that one can leverage on existing power-gating circuit used in modern designs for low power to further reduce the overhead. Using a realistic model of power grid, we provide extensive analysis of detection sensitivity for on-chip as well as external sensors.

We also analyze the security issues associated with these sensors themselves. One concern with on-chip DfS structures is the possibility of intentional tampering by an adversary. For example, scan-based techniques and power-analysis can be rendered ineffective by power-gating a Trojan in test-mode with the easily identifiable *Test Control* signal. Moreover, an adversary can insert a Trojan in a way such that it bypasses the on-chip current sensors and draws current directly from the power grid. We discuss several low-cost alternative solutions to these issues.

The paper is organized to focus on implementation of current sensors and analysis of their effectiveness for Trojan detection. We start with the motivation behind using on-chip current sensors and then present a simple yet effective design for sensing the current being sourced by each circuit block. Next, we present simulation results to show the effectiveness of the proposed technique considering a model of the power distribution network. Finally, we discuss the major design issues and conclude.

Overall approach

Side-channel analysis for Trojan detection has the benefits of higher coverage even for rarely activated unobtrusive Trojans. However, in order to make it effective for Trojans of arbitrary size and nature, we need to drastically increase the detection sensitivity. Among different side-channel parameters (delay, quiescent current or IDDQ, and transient current or IDDT), transient current analysis has emerged as an attractive choice. This is because an adversary can easily insert a Trojan to avoid any impact on critical path delay. Because the number of paths increases exponentially as a function of the circuit nodes, it is practically infeasible to monitor delay for all timing paths in a design. On the other hand, quiescent or static current analysis has following challenges: 1) impact of process variation in IDDQ is significantly more than that in delay or IDDT due to exponential dependence of subthreshold leakage on device threshold voltage; and 2) unlike IDDT, where switching can be localized to a region to increase detection sensitivity, IDDQ has less dependence on input vector, which cannot be used to turn off leakage of select circuit blocks.

In this work, we focus on improving Trojan detection sensitivity in transient current analysis. However, the integrated security monitors can be used for other forms of side-channel analysis. We note that existing work on monitoring supply current from external supply pins to detect Trojans is severely limited in detecting small Trojans (e.g., smaller than an 8-bit comparator in a design with about 10^5 transistors [5]). The issue of low sensitivity for large designs is aggravated in presence of process noise, which tends to increase each technology generation. We address this issue by integrating an array of transient current sensors on a die. This allows us to measure the supply current drawn by various regions of the chip without suffering from the attenuation and filtering effects of the on-chip power distribution network (PDN), the power pins which have large parasitic capacitances, as well as noise introduced by external measurement circuitry. Figure 1c illustrates the overall approach where multiple current sensors are inserted on-chip to achieve high-resolution measurement of region-specific currents. We place the arrays of current sensors over functional blocks or regions of the IC such that they are connected to the PDN using separate power bumps.

There are two major steps for on-chip current sensor-based Trojan detection:

1) transient current sensing; and
2) Trojan detection using the sensed current considering the effect of process and measurement noise.

Side-channel analysis approaches are based on the fact that a malicious modification should be reflected in the transient current (IDDT) of an IC. For example, if the original circuit has N_{orig} gates and consumes I_{orig} current, the insertion of N_{troj} extra gates in the circuit for implementing the Trojan will increase the current by I_{troj} which can be observed by measuring the supply current under nominal conditions. The region-specific currents measured by individual sensors will inherently provide more sensitivity than the external supply current values [8]. The digitized average transient supply current from the different spatially distributed current sensors are used to compute a spatial self-referential metric [6], which eliminates the effect of inter-die process variations. In order to eliminate the random and systematic intra-die process variations, we use the Temporal Self-Referencing (TeSR) methodology, as described in [7]. In this method, the average transient supply current is compared for the same die (or part of the die) for the same set of vectors over multiple time intervals to detect any uncorrelated switching activity due to a Trojan circuit. Note that other transient current based Trojan detection methods can also exploit the high-resolution reading from the on-chip sensors to minimize false detection probability and improve coverage for Trojans of different types and sizes. In this paper, we explore the challenges and provide solutions for increasing sensitivity of side-channel analysis-based Trojan detection techniques. The inherent limitations, such as the need for process calibration or the requirement of a golden die, depend on the actual technique being used.

Current sensor design

In this section, we discuss the challenges associated with the design and integration of the current sensors in a die and effective ways to address them. We present the design strategies for high resolution but low overhead on-chip transient current sensors. The supply current drawn by a circuit can be sensed using a high-precision resistor in series with the supply node (VDD/VSS) of a functional block or circuit under test (CUT) and by measuring the voltage drop across it. Such an approach for sensing current has been used for power characterization in a circuit [11]. Since on-chip resistors suffer from high variability with process and temperature and consume large area to implement even a nominal value of resistance, one can use the low-resistance power-gating transistor connected with the header or footer of a circuit block to implement an on-chip sense resistor. Modern chips often use supply-gating transistors which can be used to turn off parts of the circuit during idle states to reduce their leakage. Figure 2a shows the schematic of a current monitor circuit, which uses these transistors to measure supply current. The virtual VDD voltage (VDDV) is level-shifted and integrated to estimate the average power per cycle (or over multiple cycles, if the frequency is high compared to the integrator bandwidth which is limited by the achievable on-chip R/C values). Unlike [11], we need to digitize the average current values with high precision, trading off area and power overhead for better resolution,

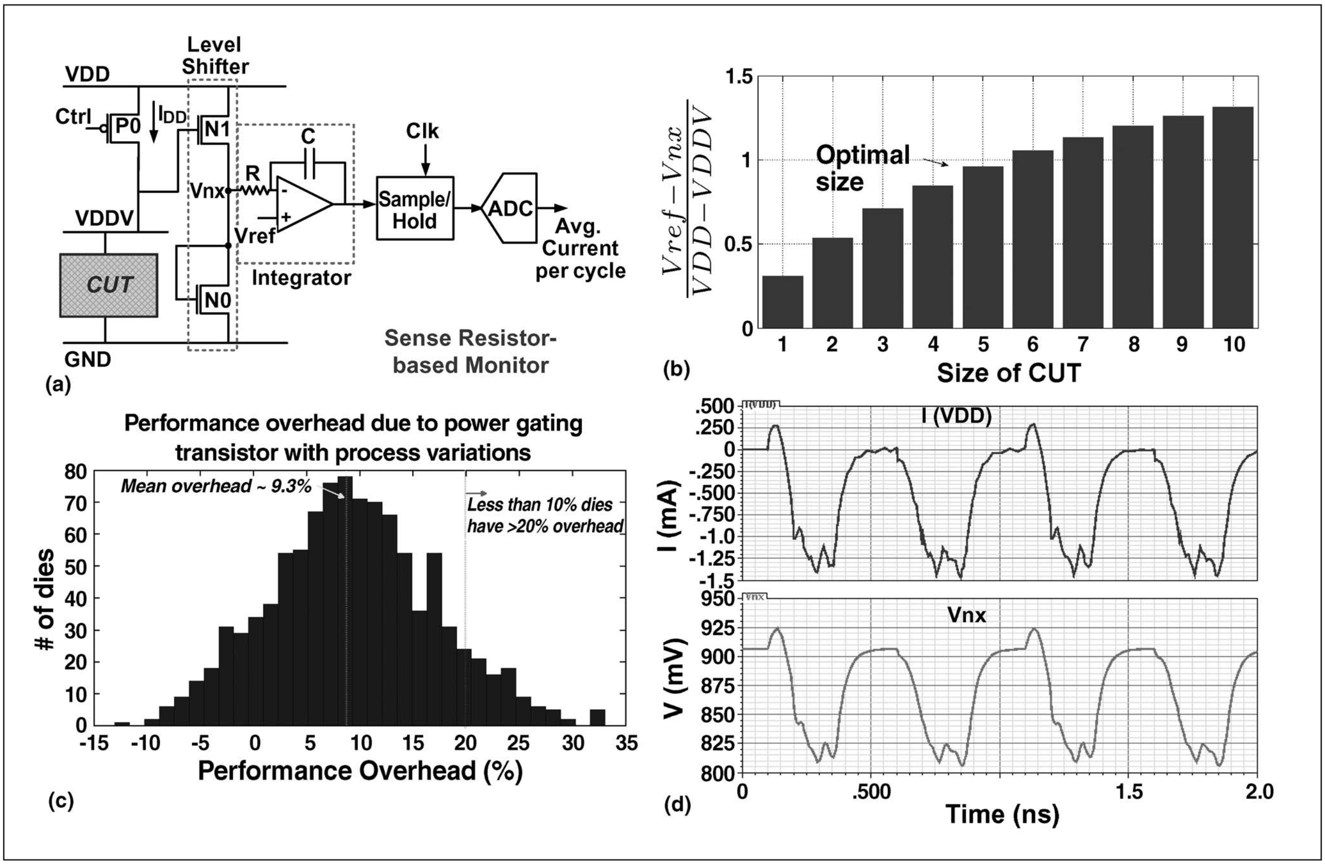

Figure 2. (a) Sense resistor-based current monitor [11]. (b) Sizing of the power gating transistor. (c) Performance overhead due to power gating transistor is less than 20% (for 90% of the dies) under process variations. (d) Waveforms of supply current and corresponding sensed voltage.

which directly translates to better Trojan detection sensitivity.

We also need a control circuit, which collects the data from multiple current sensors and sends them out through the output pins of a chip. To reduce the area overhead, we can serially send out the current values through a single pin, similar to the scan-out process. The conventional scan-chain can be used for test vector application to different parts of the CUT, and to disable other parts of the IC by turning off the power-gating transistors. During the normal mode of operation, the sensing circuitry including the integrator and the ADC unit can be reused for assisting with run-time power reduction techniques like Dynamic Voltage and Threshold Scaling (DVTS) [11], thus avoiding the presence of a clearly identifiable test control signal.

The layout of the first stage of the current sensor circuit is done in TSMC 0.18 μm technology. We extract the parasitic capacitance associated with the power gating transistor to study the effect of the power grid on the internal and external sensed current. It should be noted that this transistor should add minimum resistance in the supply line to limit the performance overhead. In our implementation, we limited the series resistance to produce a voltage drop of 10%, under worst-case switching conditions at nominal process corner. By changing the size of the CUT (chain of 5 inverters), it is seen from Figure 2b that the voltage sensitivity is optimal for 5X size. By comparing the delay of an inverter chain with and without the power gating transistors, one can see from Figure 2c that even under large process variations (using Monte Carlo simulations with inter-die variation of $\sigma = 20\%$, intra-die variation of $\sigma = 10\%$), only 10% of dies cross 20% delay overhead. The overhead can be further reduced by up-sizing the gating transistors, or partitioning the original circuit into smaller blocks, at increased area overhead. The current waveforms for the CUT and the corresponding sensed parameters ($I(VDD) =$ supply current, $Vnx =$ level-shiftedvoltage) are shown in Figure 2d. The proposed current sensing approach has the following features:

1) The sensors are in close physical proximity to the circuit under test and hence can mitigate the effect of power grid noise very well. This improves the sensitivity of detecting hardware Trojan attacks through side-channel analysis during post-silicon trust validation. Since each sensor monitors current of a specific region, proposed approach can automatically localize presence of a Trojan.
2) The current sensors can be reused in normal mode to reduce leakage by acting as supply gating transistors. During trust validation, these sensors can be selectively turned off to power-gate certain parts of a circuit, which are not amenable for deactivation through functional/structural vectors, thereby further improving Trojan detection sensitivity.
3) The sensors can enable run-time monitoring of Trojan effect, which can be extremely helpful when post-silicon trust validation cannot provide 100% confidence. At run time, whenever a current monitor detects current draw beyond a predetermined threshold, it can raise a flag.

It is imperative that the current sensors incur area (due to inserted DfS circuits), power (due to sensing circuit), and performance (due to introduction of series resistance in supply path) overheads. These parameters are traded-off for sensitivity of current measurement which directly translates to the size of a Trojan that can be detected under fixed signal-to-noise ratio (SNR). The noise can be due to process variations and measurement noise, with the variability of the resistance and temperature being prominent factors. The number of current sensors can be increased to get higher sensitivity from smaller partitions of the circuit, but it comes at the cost of larger area overhead. The area overhead can be amortized by sharing large part of the monitors including the ADC and read-out circuits among different current sensors.

Design considerations

Similar to other DfS approaches, the trustworthiness of the on-chip measurement circuitry itself needs to be verified. What happens if an adversary tampers the current monitors in a way that compromises its Trojan detection capability? Broadly, there can be two types of tampering possible: 1) a Trojan circuit bypasses a current monitor (Figure 3a); and 2) an adversary tampers the sensor itself to report incorrect current values (Figure 3b). In order to detect such tampering, we propose using the following approaches. Any Trojan must draw some current from the PDN and this causes a droop in the

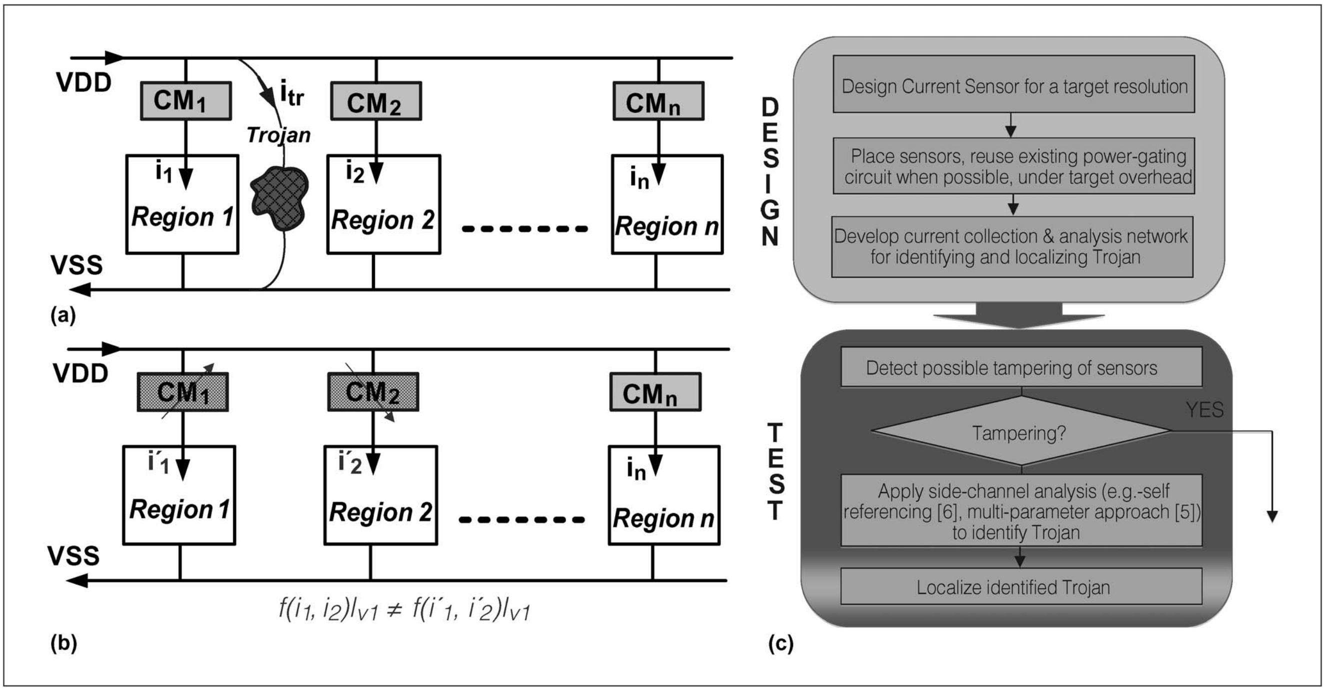
VDD
CM_1
i_{tr}
Trojan
CM_2
CM_n
i_1
Region 1
i_2
Region 2
i_n
Region n
VSS
(a)
VDD
CM_1
CM_2
CM_n
i'_1
Region 1
i'_2
Region 2
i_n
Region n
VSS
$f(i_1, i_2)|_{V1} \neq f(i'_1, i'_2)|_{V1}$
(b)
DESIGN
Design Current Sensor for a target resolution
Place sensors, reuse existing power-gating circuit when possible, under target overhead
Develop current collection & analysis network for identifying and localizing Trojan
TEST
Detect possible tampering of sensors
Tampering?
YES
Apply side-channel analysis (e.g.-self referencing [6], multi-parameter approach [5]) to identify Trojan
Localize identified Trojan
(c)

Figure 3. (a) Tampering mechanism in which a Trojan bypasses current monitors to evade detection. (b) Another possible tampering in which an attacker alters the sensed current by changing the gating transistor size. (c) Overall flow for inserting on-chip security monitors and side-channel analysis based trust validation.

local supply voltage, causing discrepancy in the relationship between the nearby current sensor and those far away, which are not affected by this droop. Though the discrepancy can be small for tiny Trojans, the process-invariance of this relationship (since measured current in different sensors shift in the same way with inter-die variations) helps in detecting such bypassing. In case the sensors themselves are altered—e.g., by upsizing or downsizing the supply gating transistors, the tampering can be evident by verifying a predefined relationship among them for specific vectors (Figure 3b). The current drawn through these sensors will be largely vector dependent and an adversary cannot guess the relationship due to the inordinately large input space.

A major advantage of using distributed power gating transistors to monitor current is that one or more of these transistors can be turned off to minimize background current in specific regions. It helps to selectively test certain regions at high sensitivity. Moreover, it also helps to easily detect potential bypassing of an always-on Trojan (e.g., the MOLES Trojan in [9]) by turning off all the sensors. Finally, possible tampering of the current sensors can be completely avoided by exploiting the emerging trend in 3D integration [10]. One can migrate the security monitors in a different layer, which can be fabricated in a less advanced technology at a trusted foundry and integrated with the original die through heterogeneous 3D integration.

Figure 3c shows the integrated flow of sensor insertion during design and Trojan detection during test. Once the sensors are designed according to a target resolution, they need to be placed in strategic locations of a die. We use an activity and controllability dependent placement approach, which aims at maximizing the detection sensitivity under vector control. This is done in two steps. First, we estimate the activity of different regions; divide it into subregions of equal activity and assign a sensor to each subregion. Next, inside a subregion, we perform controllability analysis to quantify its responsiveness to the input vectors. Subregions with less controllability receive more sensors to improve resolution for arbitrary Trojans. The maximum sensor count is limited by the design overhead. Once the sensors are placed, the power-gating transistor can be appropriately sized based on the average activity of a region. The final step in the design phase is to connect the sensor outputs to a read-out circuitry. This is done by routing the digitized current values serially to an output port. Potential disabling of a Trojan by the test control signal can be detected by noting the relationship between measured currents.

Results

The PDN was designed and modeled using distributed R-L-C grids with values from PDN of real processor chips obtained from the industry. The off-chip power supply network (including pin, package, PCB impedances) is modeled using lumped R-L-C impedances. The basic design of the 2D on-chip power grid and the off-chip power components are based on the design reported in [12]. In this section, we present simulation results comparing Trojan detection sensitivity between on-chip and off-chip analysis considering the effect of PDN.

We used the models of the PDN as well as external power supply impedance to compare the sensitivity of external current monitors with that of the on-chip (internal) current monitors. The Trojan was simulated as a single extra inverter of increasing strength in a length-5 chain of inverters (CUT). Different such inverter chains of varying strengths (1X to 10X) were connected to different current sensors to account for varying size of the original circuit. Table 1 compares the internal and external sensitivity values using two equations, the mean difference over mean golden ($\Delta\mu/\mu_g * 100\%$), and mean difference over standard deviation of golden ($\Delta\mu/\sigma_g$) for four different sizes of Trojan. The second sensitivity equation captures the effect of the process-induced spread in measured current between different dies.

The area overhead of the current sensor is primarily contributed by the power gating transistors whose sizing represents a tradeoff between area and performance overhead and detection sensitivity. We have considered 10X size of the PMOS transistor, which limits the supply noise to 10% of the supply voltage in the nominal process corner for a 5X strength inverter chain, whereas the level shifter uses minimum sized NMOS transistors. The leakage current through the level-shifter is considerable (comparable to dynamic current for a chain of inverters), but by gating the bottom NMOS transistor, the current overhead was reduced by 7 orders of magnitude during run-time.

Figure 4a and b shows the distribution of the current values (internal and external, respectively), where the overlap due to process spread causes the sensitivity for the external current to greatly diminish. Figure 4c demonstrates the effectiveness of a multiple-parameter approach [5] (considering $F_{\max}$ or maximum frequency of operation for process calibration) for the internal sensed current to distinguish Trojan-containing chips (red) from golden ones (blue). Figure 4d–f show the external current and internal sensed voltage waveforms for golden (blue) and Trojan (red) cases. Since the internal current for one region will be a fraction of the total supply current, the sensitivity is increased for a specific Trojan size. Figure 4e shows the effect for a Trojan which draws current through the sensor #58, whereas the Trojan in Figure 4f bypasses the sensor (see Figure 3a) and has less detection sensitivity. Figure 4g shows the spatial matrix of current values from all the sensors in a 12X12 grid. Since the CUT was composed of inverter chains of different sizes, the corresponding matrix shows that the Trojan circuit (red) is located near sensor #58, which is supplying current to an inverter chain of strength 4X but deviates from the sensed average current drawn by other circuits of same size.

Table 1 Comparison of On-Chip Versus Off-Chip Detection Sensitivity for Different Sizes of Trojan Circuits Under Process Variations.

Trojan Size	On-chip Sensitivity				Off-chip Sensitivity			
Formula	1X	2X	3X	4X	1X	2X	3X	4X
$\Delta\mu/\mu_g$*100%	2.85	5.68	8.69	11.87	0.040	0.060	0.080	0.090
$\Delta\mu/\sigma_g$	0.38	0.75	1.15	1.57	0.002	0.003	0.004	0.005

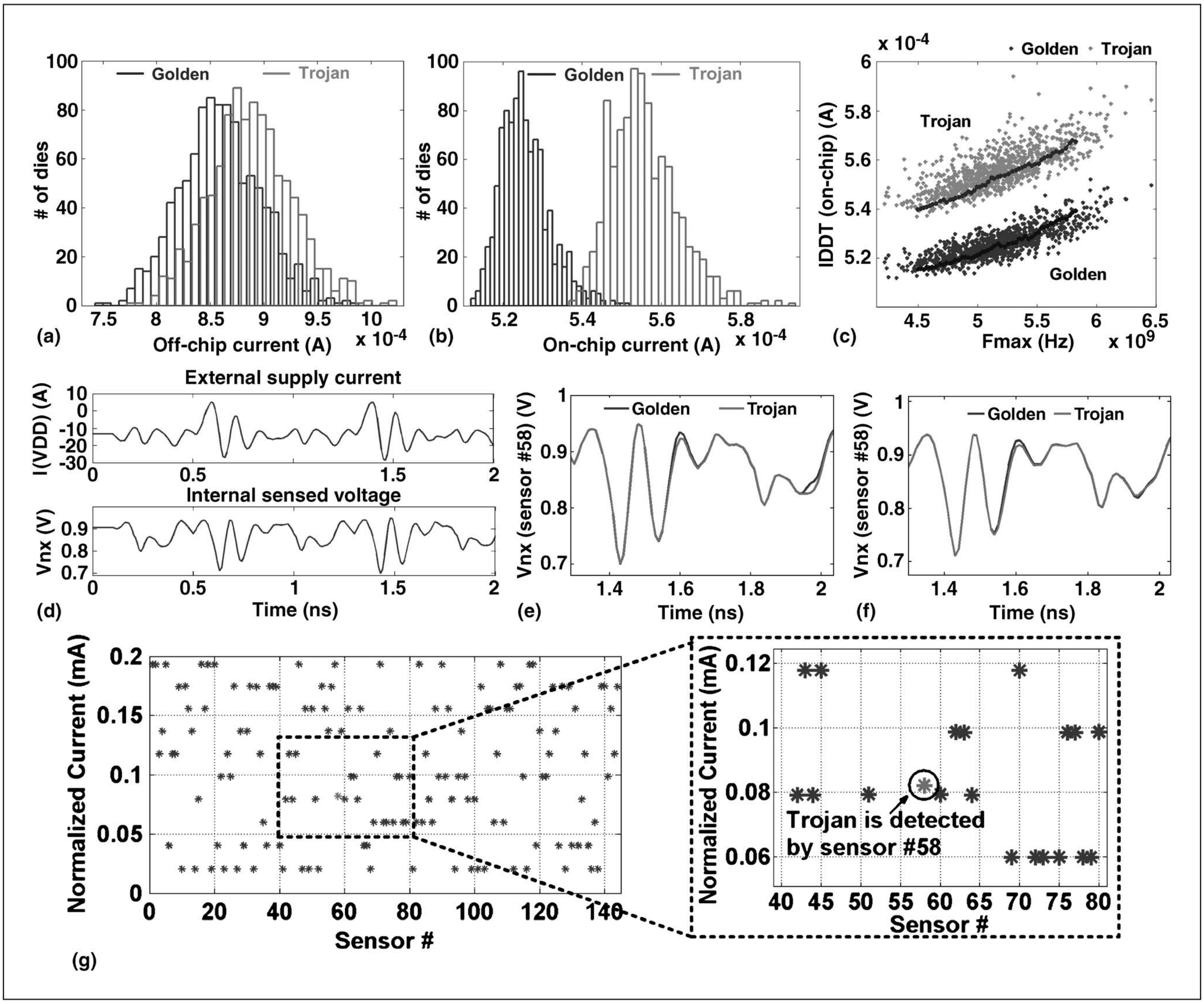

Figure 4. Comparison of (a) on-chip versus (b) off-chip current without (blue) and with Trojan (red), considering effect of process variations. (c) Using the multiple-parameter approach [5], the Trojan-containing chips are readily identified. (d) The external current and internal sensed voltage waveforms for sensor #58. The sensed voltage waveforms (blue—golden, red—Trojan) are shown (e) for a Trojan which is readily detected (sensitivity = 5.5%) and (f) for one which bypasses the sensor, but is still detected (sensitivity = 3.5%). (g) The self-referential relationship among the average internal currents is plotted in a simple matrix format to show the effect of intra-die variations and the effect of Trojan on one of the circuits-under-test. The sensed current values from different parts of the chip are compared to each other for a single IC, where a Trojan is detected by sensor #58, which deviates from the values of other sensors measuring current for similar CUT (this method exploits spatial self-similarity in currents from different regions of the same chip [6]). The inset zooms in on a part of the plot to illustrate the deviation clearly.

To analyze the effectiveness of selective power gating during trust validation, we considered an advanced encryption system (AES) circuit of approximately 10^5 transistors in predictive 45 nm process and inserted a combinational Trojan of equivalent size of 4 inverters. By turning off different number of sensors, we observed sensitivity increase between 2.4X to 12X. Finally, to evaluate run-time monitoring capability, we consider a Trojan that can activate undesired write in a processor cache. We consider a low-power 16 KB cache in 45 nm process and a comparator-based combinational Trojan that causes a memory write on activation. From the layout of the cache and Trojan, we observe that the memory leakage current is 1.8e-5A, while the total dynamic current contributed by Trojan and write access is 1.6e-4A, which is about 9X higher than the leakage and hence can be easily detected by the on-chip monitor.

We have presented a design-for-security approach based on integrating current sensors in an IC for verifying its trustworthiness and security against the hardware Trojan attacks. Considering a realistic power-grid model, we have shown that an array of carefully designed and placed sensors can lead to drastic improvement in Trojan detection sensitivity compared to external current measurement based side-channel analysis. The sensor design can take advantage of existing power-gating transistors in a design, commonly used to achieve low power operation. Unlike external sensing, the proposed approach can be easily scaled to large designs by using appropriate number of sensors in strategic locations. We discuss solutions to make potential tampering of the sensors evident and benefits of using the sensors for Trojan localization and run-time monitoring of Trojan effects. Future work would include extension of the approach to 3D stacked IC and validation using test chips. ■

Acknowledgment

This work has been partially supported by the National Science Foundation (NSF) under Grant CNS-1054744 and CCF-0964514.

■ References

[1] M. Tehranipoor and F. Koushanfar, “A survey of hardware Trojan taxonomy and detection,” *IEEE Des. Test Comput.*, 2010.

[2] R. S. Chakraborty et al. “MERO: A statistical approach for hardware Trojan detection,” in *Workshop on Cryptographic Hardware and Embedded Syst. (CHES)*, 2009.

[3] M. Potkonjak et al. “Hardware Trojan horse detection using gate-level characterization,” in *Proc. Des. Automation Conf.*, 2009.

[4] X. Zhang and M. Tehranipoor, “RON: An on-chip ring oscillator network for hardware Trojan detection,” in *Proc. Design Automat. Test in Eur.*, 2011.

[5] S. Narasimhan et al. “Multiple-parameter side-channel analysis: A non-invasive hardware Trojan detection approach,” in *Proc. IEEE Int. Symp. Hardware-Oriented Secur. Trust (HOST)*, 2010.

[6] D. Du et al. “Self-referencing: A scalable side-channel approach for hardware Trojan detection,” in *Proc. Workshop on Cryptograph. Hardware and Embedded Syst. (CHES)*, 2010.

[7] S. Narasimhan et al. “TeSR: A robust temporal self-referencing approach for hardware Trojan detection,” in *Proc. IEEE Int. Symp. Hardware-Oriented Secur. Trust (HOST)*, 2011.

[8] R. Rad et al. “A sensitivity analysis of power signal methods for detecting hardware Trojans under real process and environmental conditions,” *IEEE Trans. VLSI Syst.*, 2010.

[9] L. Lin et al. “Trojan side-channels: Lightweight hardware Trojans through side-channel engineering,” in *Proc. Workshop on Cryptograph. Hardware and Embedded Syst. (CHES)*, 2009.

[10] T. Huffmire et al. “Trustworthy system security through 3-D integrated hardware,” in *Proc. IEEE Int. Workshop on Hardware-Oriented Secur. Trust (HOST)*, 2008.

[11] N. Mehta and B. Amrutur, “Dynamic supply and threshold voltage scaling for CMOS digital circuits using *in-situ* power monitor,” *IEEE Trans. VLSI Syst.*, 2011.

[12] M. S. Gupta et al. “Understanding voltage variations in chip multiprocessors using a distributed power-delivery network,” in *Proc. Design Automat. Test in Eur.*, 2007.

Seetharam Narasimhan is a security researcher at the Security Center of Excellence, Intel Corp., Hillsboro, OR. His research interests include low power and robust design, hardware security and implantable electronics. He received the PhD degree in computer engineering from Case Western Reserve University, Cleveland, OH.

Wen Yueh has research interests which include developing modeling methodologies to control the multiphysics interactions for an energy-efficient heterogeneous 3D system. He received the MS degree in electrical and computer engineering from Rutgers University, and is a PhD student at the

School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta.

Xinmu Wang has research interests which include hardware security and low power and robust VLSI design. She received the BE degree in electronic information science and technology from Harbin Institute of Technology, China. She is a PhD student in computer engineering at Case Western Reserve University, Cleveland, OH.

Saibal Mukhopadhyay is an associate professor of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta. His research interests include design of energy-efficient and reliable circuits and systems in nanometer technologies. He received the PhD degree in electrical engineering from Purdue University, West Lafayette, IN.

Swarup Bhunia is an associate professor of Electrical Engineering and Computer Science, Case Western Reserve University, Cleveland, OH. His research interests include low power and robust design, hardware security, and implantable electronics. He received the PhD degree in electrical engineering from Purdue University, West Lafayette, IN.

■ Direct questions and comments about this article to Seetharam Narasimhan, EECS Department, Case Western Reserve University, Cleveland, OH 44106; sxn124@case.edu.