High-Sensitivity Hardware Trojan Detection Using Multimodal Characterization

Kangqiao Hu*, Abdullah Nazma Nowroz†, Sherief Reda† and Farinaz Koushanfar*
*ECE Department, Rice University, Houston, Texas, 77005
Email: kangqiao.hu, farinaz@rice.edu
†School of Engineering, Brown University, Providence, RI, 02906
Email: abdullah_nowroz, sherief_reda@brown.edu

***Abstract*—Vulnerability of modern integrated circuits (ICs) to hardware Trojans has been increasing considerably due to the globalization of semiconductor design and fabrication processes. The large number of parts and decreased controllability and observability to complex ICs internals make it difficult to efficiently perform Trojan detection using typical structural tests like path latency and leakage power. In this paper, we present new accurate methods for Trojan detection that are based upon post-silicon multimodal thermal and power characterization techniques. Our approach first estimates the detailed post-silicon spatial power consumption using thermal maps of the IC, then applies 2DPCA to extract features of the spatial power consumption, and finally uses statistical tests against the features of authentic ICs to detect the Trojan. To characterize real-world ICs accurately, we perform our experiments in presence of 20% - 40% CMOS process variation. Our results reveal that our new methodology can detect Trojans with 3-4 orders of magnitude smaller power consumptions than the total power usage of the chip, while it scales very well because of the spatial view to the ICs internals by the thermal mapping.**

I. Introduction

The ever-increasing cost of manufacturing Integrated Circuits (ICs) in small-scale CMOS technology has led to the eminence of third party foundry business practice. While the practice saves cost by utilizing the economy of scale, it exposes the chips by authentic designers to threats including hardware malware (Trojan) insertion, unlicensed IP handling, and IP piracy [1], [2]. Since the ICs form the core for the computing and communication systems used in contemporary personal, commercial, and government affairs, their exposure endangers the full systems built upon them. Therefore, granting trust in presence of unreliable third-party fabrication has become a major challenge.

IC Trojans are implemented by unsought chip modifications during the third-party fabrication process; they traitorously change or tamper with the chips to provide opportunities for later exploits including controlling, monitoring, or spying the chip contents or secret keys [1], [3]. Trojans can be very hard to detect, due to the increasing complexity of the contemporary chips and lack of controllability/observability to the post-silicon chip internals. Also, they may be often inactive, only triggered as needed in special time intervals. Thus, devising noninvasive methods for examining the ICs and detecting Trojans has been recognized as an important research problem.

978-3-9815370-0-0/DATE13/

Our objective is to provide a novel methodology for Trojan detection using multimodal post-silicon spatial thermal and power estimates. Chips can be thermally characterized using infrared emissions from the backside of silicon die, which then can be processed to get detailed spatial power maps [4]. These thermal and power maps provide a much higher resolution Trojan detection method than previous current-based methods. This detection procedure is easily scalable and does not require test vectors. The major contributions of this paper are as follows.

- We propose a multimodal characterization framework which includes thermal maps and power maps to detect and locate IC Trojans. Our detection framework includes acquiring post-silicon thermal maps and applying thermal inversion methods.
- Using the multimodal characterization, we provide 2-dimensional principal component analysis (2DPCA) framework for Trojan detection which can accurately detect very small size Trojan using the thermal and power maps.
- To create realistic chips, we add 20-40% process variations (PV) to gate lengths, widths and oxide thickness which can hide Trojans. To cover a wide range of variations, in our experiment we set five different PV levels with different standard variances which are obtained from realistic spatial variability models.
- We design virtual Trojans with power consumption varying from 0.05% to 0.2% of total IC power consumption placing the Trojans in different locations.
- We present an extensive set of simulation results with three different benchmarks with realistic chips and very small Trojan sizes. We show that our proposed methods are able to detect and locate Trojans as small as 0.05% of the total power consumption very efficiently and accurately.

The organization of this paper is as follows. Section II provides the necessary background. In Section III we provide the framework for our proposed Trojan detection procedure. In Section IV we describe our experimental setup and present our experimental results to demonstrate the effectiveness of our approach, and finally, Section V summarizes our main results and discusses future direction.

II. Related Work

Reports of instances of malware in military chips have triggered further research and investigations into the Trojan detection problem [2]. One of the early work in this area [5] utilized the dynamic current (power) measurements by destructive testing of a few ICs from the design to build signatures. The assumption was that the fingerprint did not contain any malware. The existence of Trojan(s) in other chips was verified by non-invasively comparing against the signatures formed by destructive testing. In another approach, verification and functional testing method simulates the inputs and then checks the corresponding outputs for the desired patterns [6]. Functional testing suffers from state-space explosion and lack of targeted verification output, and therefore, its scope and effectiveness are rather limited.

A number of Trojan detection methods have focused on detecting based on structural test measurement and analysis such as delay or current [7], [8], [9]. The typical assumption for these Trojan detection approaches is that a golden model of the chip can be formed by post-layout simulations. The structural properties of the manufactured chips under investigation are then compared with this model. An effective technique pursued in this category is gate-level characterization [8], [9] which measures the chip's delay or current for a number of test vectors. Assuming that the currents (delays) linearly add up, a linear system is then constructed from the measurement set. Solving the system of linear equations translates the side-channel characteristics to smaller gate-level structural properties. While effective, this technique does not perform well for larger chips with more gates, higher accumulated measurement noise, and more sophisticated process variation models. The approaches based on regional testing of accumulated current which have a higher resolution only work for certain types of packaging and measurement probes [7], [10].

The thermal to power inversion procedure involves infrared imaging from the backside of the silicon die, and then converting the thermal image to spatial power maps. While some of these works have been very successful in estimating the spatial power maps accurately [4], none of the previous works have utilized the spatial power maps to detect Trojans. Our proposed method utilizes these very high resolution thermal and power maps in order to detect IC Trojans which results into a very high sensitivity Trojan detection technique.

III. Detection Framework

A. Spatial Temperature and Power Characterization

In this paper, we present a novel Trojan detection method based on multimodal post-silicon spatial temperature and power characterization. The first mode corresponds to using infrared techniques to obtain very high resolution thermal maps by running various workloads in the chip. These thermal maps can be used to obtain accurate and detailed corresponding spatial power maps which corresponds to the second mode. Our proposed method utilizes both thermal and power maps to detect and locate Trojans which consumes as small power as 0.05 - 0.2 $\%$ of total power consumption of the chip.

1) Temperature Characterization: For real chips, we can use infrared imaging techniques to obtain the thermal maps of post-silicon chips for Trojan detection. We can obtain optical access to the die through the silicon backside by removing the packages's heat spreader. Silicon is transparent in the infrared spectral region and this transparency allows the capturing of thermal infrared emissions using infrared imaging techniques.

For the purpose of this paper, we first apply random vectors to the ICs and get the estimated power trace of each block by Primetime-PX and then use HotSpot [11] simulation tools to create the steady state thermal maps of various test bench circuits as described in Section IV-B. For real chips, it typically takes less then 60s to reach the steady state. We denote the steady-state thermal maps obtained using design-time simulations and Monte-Carlo simulations at various PV corners of the original chip by $\mathbf{A}_1, \mathbf{A}_2, ...$ and the thermal maps from chips under test by using infrared imaging by $\mathbf{T}_1, \mathbf{T}_2, ...$ We use authentic thermal maps as the training set and perform our method of 2DPCA on the thermal maps under tests for Trojan detection as described in Section III-B

2) Power Characterization: The chip power and temperature are related by the heat equation, which can be discretized as follows by linear matrix formulation,

$$\mathbf{Rp + e = t}, \tag{1}$$

where the 2-D thermal map $\mathbf{T}$ is represented by a vector $\mathbf{t}$ that gives the measured temperatures at every pixel of the imaging system, and the continuous power signal is represented by a vector $\mathbf{p}$ that gives the power density at a set of discrete die locations and the vector $\mathbf{e}$ denotes measurement noise in the infrared imaging system. The matrix $\mathbf{R}$ represents the thermal resistivities between different locations [4]. For each specific chip, the matrix $\mathbf{R}$ can be estimated either by analytical methods, by simulation or experimentally on the real chip. We create matrix $\mathbf{R}$ by HotSpot simulation, by dividing the chip into 10×10 blocks, and exciting each block at a time. Thermal map corresponding to one excited block represents one column in the matrix $\mathbf{R}$. The lower bound of the block size is limited by the precision of infrared camera. Detection accuracy increases as the block size decreases. There is a trade-off between the size of the blocks and computation time.

Given the thermal map vector $\mathbf{t}$ and matrix $\mathbf{R}$, the objective is to find the best power map vector $\mathbf{p}$ that minimizes the total squared error between the temperatures as computed from the estimated power $\mathbf{p}$ and the thermal measurements. For our case, we first subtract the thermal maps $\mathbf{t}_{min}$ corresponding to minimum estimated design time power $\mathbf{p}_{min}$, from the thermal maps $\mathbf{t}$ of chips under test, where $\mathbf{t}_{min} = \mathbf{R}\mathbf{p}_{min}$, and then invert the residual thermal maps, $\mathbf{t}_r$ to get the residual power estimates $\mathbf{p}_r$.

$$\begin{gathered} \mathbf{t}_r = \mathbf{t} - \mathbf{t}_{min}, \\ \arg_{\mathbf{p}_r} \min \parallel \mathbf{R}\mathbf{p}_r - \mathbf{t}_r \parallel^2, \\ \text{s. t.} \quad \mathbf{p}_r \geq 0, \end{gathered} \tag{2}$$

where $||\cdot||$ indicates the L_2 norm. We apply 2DPCA analysis on the residual power map $\mathbf{p}_r$ for Trojan detection.

Figure 1(a) and 1(c) shows MIPS (Microprocessor without Interlocked Pipeline Stages) processor thermal maps generated by HotSpot. We divide the chip into 10x10 blocks and estimate the spatial power maps using above optimization formulation, shown in Figure 1(b) and 1(d). The Trojan location is shown in both the thermal and power maps.

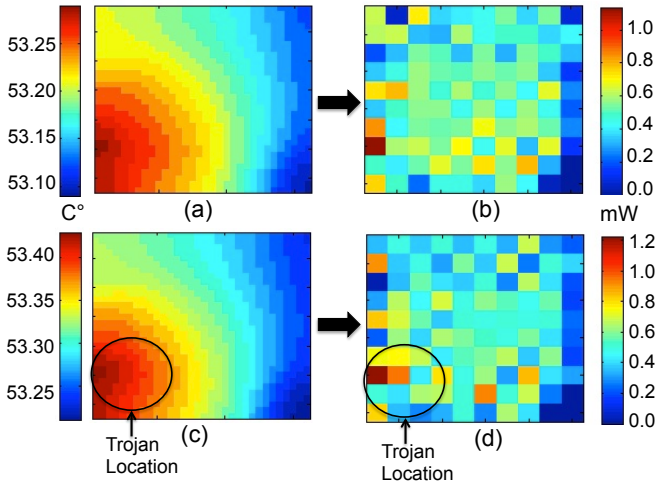


Fig. 1. MIPS processor Thermal Map (C°) and Estimated Power map (mW) a) Thermal map without Trojan, b) Estimated power map without Trojan, c) Thermal map with Trojan, and d) Estimated power map with Trojan

B. 2-Dimensional Principal Component Analysis

1) Algorithm: Principal Component Analysis (PCA) is a classical feature extraction and data representation technique widely used in the areas of pattern recognition and computer vision. PCA is mathematically defined as an orthogonal linear transformation that transforms the data to a new coordinate system such that the greatest variance by any projection of the data comes to lie on the first coordinate (called the first principal component), the second greatest variance on the second coordinate, and so on. Two-dimensional principal component analysis (2DPCA) developed by J. Yang is an image projection technique that makes use of the spatial correlation information to achieve better performance than conventional one-dimensional PCA [12]. The basic idea of 2DPCA is to project image $\mathbf{A}$, an $m \times n$ random matrix, onto a projection vector $\mathbf{x}$ by the following linear transformation:

$$\mathbf{y} = \mathbf{A}\mathbf{x} \tag{3}$$

The discriminatory power of $\mathbf{x}$ is evaluated by the total scatter of the projected samples where the following criterion is adopted:

$$J(\mathbf{x}) = tr(\mathbf{S_x}) \tag{4}$$

$\mathbf{S_x}$ is the covariance matrix of the projected feature vectors of the training samples and $tr(\mathbf{S_x})$ is the trace of $\mathbf{S_x}$. The covariance matrix $\mathbf{S_x}$ is given by the following equation:

$$\begin{aligned} \mathbf{S_x} &= E[(\mathbf{y} - E\mathbf{y})(\mathbf{y} - E\mathbf{y})^T] \\ &= E[((\mathbf{A} - E\mathbf{A})\mathbf{x})((\mathbf{A} - E\mathbf{A})\mathbf{x})^T] \end{aligned} \tag{5}$$

So,

$$tr(\mathbf{S_x}) = \mathbf{x}^T E[(\mathbf{A} - E(\mathbf{A}))^T(\mathbf{A} - E(\mathbf{A}))]\mathbf{x} = \mathbf{x}^T\mathbf{G}_t\mathbf{x} \tag{6}$$

where $\mathbf{G}_t$ is the image covariance (scatter) matrix. Suppose there are totally M image samples for training, then

$$\mathbf{G}_t = \frac{1}{M}\sum_{j=1}^{M}(\mathbf{A}_j - \bar{\mathbf{A}})^T(\mathbf{A}_j - \bar{\mathbf{A}}) \tag{7}$$

The optimal projection axes, $\mathbf{x}_{opt,1}, \mathbf{x}_{opt,2}, ..., \mathbf{x}_{opt,d}$, are the eigenvectors of $\mathbf{G}_t$ corresponding to the largest d eigenvalues.

2) Feature Extraction and Identification: In our experiment, 1000 thermal maps, $\mathbf{A}_1, \mathbf{A}_2, ..., \mathbf{A}_{1000}$, of authentic chips are used to evaluate the optimal projection axes $\mathbf{x}_{opt,1}, \mathbf{x}_{opt,2}, ..., \mathbf{x}_{opt,d}$. Then the extracted thermal feature matrix $\mathbf{B}$ is defined by

$$\mathbf{B} = [\bar{\mathbf{A}}\mathbf{x}_{opt,1}, \bar{\mathbf{A}}\mathbf{x}_{opt,1}, ..., \bar{\mathbf{A}}\mathbf{x}_{opt,d}] \tag{8}$$

For a given set of testing ICs, a feature matrix $\mathbf{B}_i$ is obtained for each IC after the transformation by 2DPCA. Then the distance between the testing feature matrix $\mathbf{B}_i$ and the authentic feature matrix $\mathbf{B}$ is calculated by

$$d(\mathbf{B}, \mathbf{B}_i) = \|\mathbf{B}_i - \mathbf{B}\|_2 \tag{9}$$

where $\|\mathbf{B}_i - \mathbf{B}\|_2$ is the Euclidean distance between $\mathbf{B}_i$ and $\mathbf{B}$. If the distance is larger than a certain threshold, the testing IC is identified as Trojan inserted.

C. Trojan Localization

The inherent low-pass filter of heat conduction function makes it hard to accurately locate the Trojan, since most of the high frequency components are lost in the thermal maps [4]. With the detailed spatial power characterization technique these frequency components are well recovered in the power maps. We use the estimated residual power maps to locate the trojans in the chip by finding the maximum power location in the trojan detected chips.

IV. Experimental Setup and Results

To test our proposed Trojan detection methods we provide sophisticated simulation results which mimic a realistic experiment setup with process variation, and test three different benchmarks. We vary trojan sizes and locations across the chips. We provide the experimental results of two approaches. First, the thermal map based method which is more efficient in terms of computation time but less accurate; this does not require the thermal-to-power inversion procedure which increases detection time. Second, the detailed spatial power based method which is very accurate and can detect and locate very small Trojan; this requires the thermal-to-power inversion procedure.

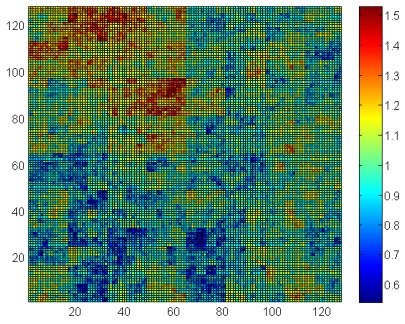


Fig. 2. Gate parameter scale with 40% PV

A. Process Variation

To characterize real-world ICs accurately, we add $20-40\%$ Process Variation (PV) to the gates' parameters. We use multi-level quad-tree approach to model the spatial within-die PV [13]. Higher levels of the quad-tree structure reflect the spatial correlations in larger scale while lower levels reflect the spatial correlations in smaller scale [13]. Figure 2 demonstrates the PV profile generated by an 8-level quad-tree. The effect of PV on dynamic power is neglected in our experiment since it is insignificant compared to the effect of PV on leakage power. Since I_{sub} is the dominant component of leakage power, we assume that the leakage current is equal to sub-threshold current. We add PV to gates' length, gates' width and gates' oxide thickness as [14]. In our experiment we set 5 different PV levels with variation of 20%, 25%, 30%, 35% and 40%, which introduces $\pm 0.5\%$ to $\pm 3\%$ variation to total power consumption.

B. IC Benchmarks

Three benchmarks from Opencores that are developed with Hardware Description Language (HDL) are used in our analysis: 1) 128-bit Advanced Encryption Standard (AES) cipher, 2) 32-bit MIPS Processor, 3) Reed-Solomon Decoder. Table I gives the basic information of benchmarks including number of gates, core size and total power consumption with standard voltage $1.1V$ at 1GHz. We used Design Compiler synthesis tool from Synopsys to map the benchmarks to Nangate 45nm library and used Primetime-PX from Synopsys to estimate the average power consumption during a certain period with random vectors. We used Cadence SoC Encounter RTL compiler for floor planning, placing and routing, and Hotspot [11] for IC temperature simulation.

C. Trojan Design and Insertion

We have designed Trojans modules with power consumption varying from 0.05% to 0.2% total IC power consumption. Our Trojans do not have any specific functional modules but certain power consumption that are used to evaluate the minimum size of Trojan that can be detected. Despite the Trojan type, sequential or combinational, the power consumption ratio of the Trojan circuit and the IC is the only factor that impact our detection results. The Trojan circuits are implemented using the same standard cells as the ICs with a constant core utilization of approximate 70%. We divide the IC area into 10×10 blocks and insert one Trojan per chip into the blank space within these blocks. The impact of core utilization will be studied in the future work. For each benchmark at different PV levels, 10000 chips with different sizes of Trojans inserted in different locations are generated. So, with different PV levels, different Trojan sizes, different Trojan locations 100,000 chips of each benchmark are generated for testing.

TABLE I
TEST BENCHES

Test bench	Number of Gates	Core Size (μm^2)	Total Power (W)
AES	10610	163×163	0.0732
MIPS	8661	195×195	0.0494
RS Decoder	23224	394×394	0.12

D. Trojan Detection with Thermal Maps

Based on the method proposed in Section III-B, we first calculate the optimal projection vectors for each benchmark. All the thermal maps are simulated by HotSpot in $2^n \times 2^n$ grids. n depends on the die size and the resolution of infrared camera, $5 \times 5 \mu m^2$. Thus, the thermal resolution of MIPS and AES is 32×32 grids, and RS Decoder is 64×64 grids. The thermal maps with resolution $2^n \times 2^n$ have 2^n eigenvectors in total. The number of eigenvectors that are used for feature extraction is determined by the magnitude of corresponding eigenvalues. Here we use benchmark AES as an example. We select eigenvectors corresponding to the first 10 largest eigenvalues as the optimal projection axes. Then the average thermal map of 1000 authentic chips are used to extract the golden feature matrix $\mathbf{B}$ as shown in Figure 3. Then for each testing chip, the distance of its feature matrix and the golden feature matrix is computed. Figure 4 illustrates the distance distribution of authentic ICs and Trojan infected ICs. Figure 4(a) is an experiment with 20% PV and 4(b) is the experiment with 40% PV and the same measurement error. From the figure, we can clearly see that as the magnitude of PV increases the histogram of distance begins to overlap, which makes it hard to distinguish the authentic chips from the Trojan infected chips. We have implemented experiments that vary the false positive and magnitude of process variation.

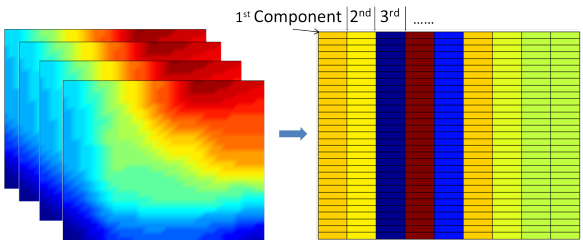
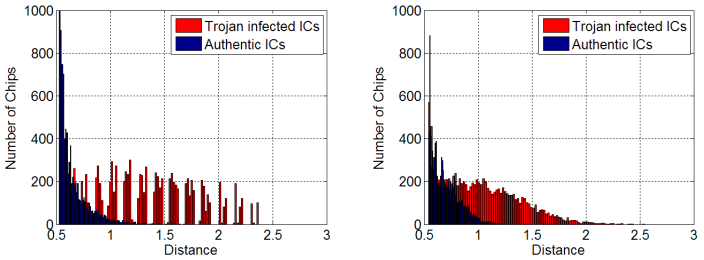


Fig. 3. Golden feature matrix extraction

1) Detection Results under Different False Positive Rate: As we mention in Section III, the testing IC instance is identified as an authentic chip or a Trojan infected chip by a certain threshold that is associated with detecting false



(a) AES under 20% PV (b) AES under 40% PV

Fig. 4. Feature matrix distance between testing chip and golden chip

positive. Based on the distance histogram e.g. Figure 4 of training chips, we apply a kernel function to estimate the actual probability distribution function (pdf) $f(d)$ for the authentic instances, where d denotes the distance from the golden feature matrix. Therefore, for a certain threshold d_{th}, the false positive is $\alpha = 1 - F(d_{th})$. By this, we fix the false positive to a certain value and observe how the false negative changes.

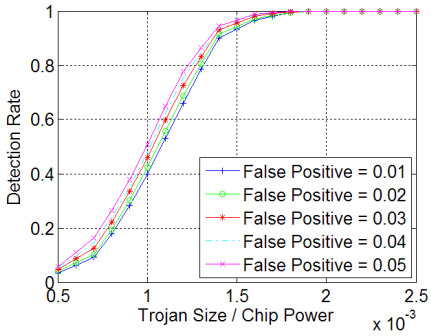


Fig. 5. With fixed PV (0.2) and nominal voltage value (1.1V), the detection rate of AES under different false positive

Figure 5 shows that as the false positive increases, the detection rate increases while the false negative decreases. The controllability of the threshold makes us easily adjust the algorithm to trade off false alarm and detection rate according to different detection requirements.

2) Detection Results under Different PV Level: The impact of PV is the most important factor that affects the performance of Trojan detection method. Figure 6 shows that with the fixed false positive rate, as the magnitude of PV increases, the detection rate decreases. The detection rate decreases in the following order: AES, MIPS, RS Decoder. The main difference of these three benchmarks are the total power and the core size. If we define *power density*, as $\rho = \frac{P}{S_{core}}$, where P is total power and S_{core} is the size of the core, we notice that ρ decreases in the same order as performance, which means $\rho_{AES} > \rho_{MIPS} > \rho_{RS}$. The chip with higher power density will generate more heat during the same period, thus, a larger temperature gradient is formed, which makes the region with Trojan more prominent.

E. Trojan Detection and Localization with Spatial Power Mapping

1) Detection Results under Different PV Level: We subtract the authentic thermal maps from the thermal maps under test, and perform thermal to power inversion on the residual thermal maps to estimate the spatial residual power as described in Section III-A. Figure 7 shows results from process variation experiment which shows a similar trend as Figure 6, but we can clearly see that the detection rate increases significantly using the spatial power estimates.

2) Trojan Location error using 10×10 power maps: The Trojan location is obtained by the method proposed in Section III-C. We compute the Euclidean distance of the estimated location and the real location, by normalizing the distance to the chip core dimension we get the estimation of location error.

F. Overall Sensitivity

Table II lists all the experimental results with thermal mapping and power mapping. Overall the power mapping approach has a much higher sensitivity than the thermal mapping approach. From the table we can see that with the medium PV level, 0.3, and the Trojan size larger than 0.25% chip size, the power mapping approach achieves a detection rate larger than 93% with a false alarm equal to 1% for all the three benchmarks. Also, we see that if the testing IC is identified as Trojan chip, the method can fast locate the Trojan within 10% error to the chip dimension. The main reason for the dramatic improvement from thermal mapping to power mapping is the proper recovery of the high frequency components of the power map. Also, the thermal to power inversion is an L_2 norm based approach which is very sensitive to outliers.

V. Conclusion

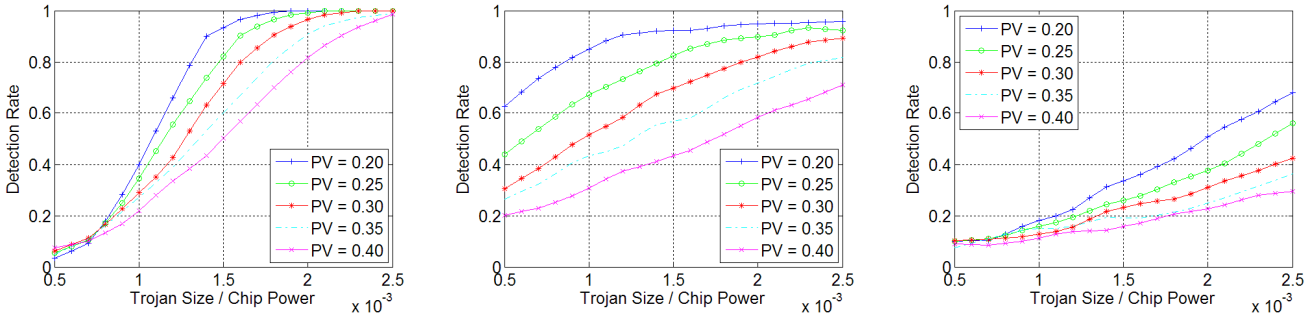
In this paper we have investigated the use of multimodal post-silicon spatial thermal and power maps in order to detect and locate Trojans in modern ICs. Through an extensive set of benchmarks and experiments, we have demonstrated that using high resolution thermal maps increase the Trojan detection sensitivity. To improve the sensitivity further, we have inverted the thermal maps to get detailed spatial power maps, and utilized the power maps for Trojan detection. These power maps can also reveal the Trojan location very accurately. Using proposed multimodal methods, we are able to detect Trojans which consume power as small as 0.05% to 0.2% of total power consumption. To create realistic chips, we have added 20-40% process variations. For future work, we will add measurement noise which is present in a real infrared imaging setup to our thermal maps generated by HotSpot. To explore the impact of ICs' supply voltage, we plan to vary chips supply voltage while creating the thermal maps and decrease the Trojan sizes even further.

Acknowledgments: This work is partially supported by NSF grant numbers 1115424 and 1116858.

References

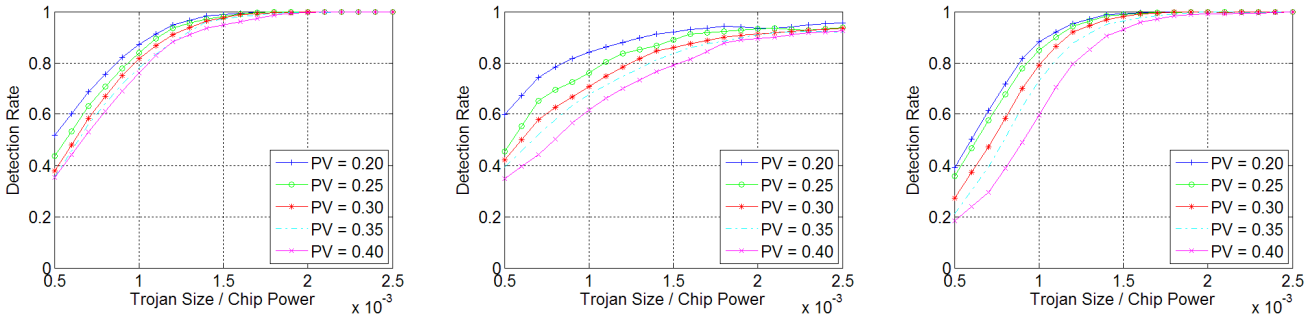
[1] M. Tehranipoor and F. Koushanfar, "A survey of hardware Trojans: taxonomy and detection," *IEEE Design Test of Computers*, vol. 27, no. 1, pp. 10–25, 2010.

[2] "Defense Science Board (DSB) study on high performance microchip supply, http://www.acq.osd.mil/dsb/reports/2005-02-hpms_report_final.pdf."



(a) AES (b) MIPS (c) RS Decoder

Fig. 6. With fixed false positive rate (1%) and nominal voltage value (1.1V), the detection rate under different process variation level using thermal maps



(a) AES (b) MIPS (c) RS Decoder

Fig. 7. With fixed false positive rate (1%) and nominal voltage value (1.1V), the detection rate under different process variation level using power maps

Detection Method		Thermal Mapping Detection Rate %					Power Mapping Detection Rate %					Location Error % Chip Width				
Benchmark	Trojan Size\PV	0.2	0.25	0.3	0.35	0.4	0.2	0.25	0.3	0.35	0.4	0.2	0.25	0.3	0.35	0.4
AES	0.05%	8.0	2.0	2.2	2.7	3.0	51.7	43.6	37.8	35.6	35.2	4.1	4.5	4.5	5.0	5.1
	0.10%	26.5	19.1	15.4	16.3	11.4	87.3	83.9	81.6	78.0	76.2	3.9	4.3	4.4	4.6	4.6
	0.15%	86.5	67.2	54.4	43.5	31.2	98.8	98.2	99.5	97.1	94.8	3.3	4.0	4.2	4.4	4.5
	0.20%	99.7	96.7	89.9	77.6	64.9	100.0	99.8	97.6	97.4	97.5	2.7	3.3	3.3	3.5	3.6
	0.25%	100.0	100.0	100.0	96.5	90.8	100.0	100.0	100.0	100.0	100.0	1.7	1.6	1.8	1.9	2.2
MIPS	0.05%	32.0	19.7	11.7	8.0	5.6	60.0	45.5	42.2	39.3	34.8	6.2	7.4	7.5	8.1	10.6
	0.10%	60.6	39.0	23.3	16.5	10.8	84.1	76.1	70.8	67.8	61.7	5.7	7.0	7.2	7.4	7.8
	0.15%	81.8	62.6	40.1	26.0	17.7	92.2	89.0	86.1	83.6	79.0	5.3	6.2	7.1	7.3	7.6
	0.20%	91.1	77.8	58.2	39.4	27.6	93.5	93.4	91.2	91.0	89.4	4.7	4.8	5.3	5.3	5.4
	0.25%	92.4	88.5	73.7	55.9	39.3	95.6	94.0	93.5	92.1	92.5	2.7	2.5	2.8	2.9	2.9
RS Decoder	0.05%	5.4	5.0	2.7	2.3	2.3	39.0	35.8	27.3	21.1	18.4	6.5	6.6	6.8	7.3	7.4
	0.10%	9.8	7.5	4.3	4.8	3.7	88.2	85.0	79.2	72.9	59.7	6.1	6.1	6.5	7.5	7.5
	0.15%	21.2	13.4	9.1	7.3	4.8	99.2	98.8	98.0	96.4	93.1	5.5	4.8	5.5	5.8	5.9
	0.20%	36.2	22.2	12.5	9.3	6.1	100.0	99.9	99.8	99.8	99.1	3.7	4.4	4.4	4.3	4.5
	0.25%	57.0	38.1	20.9	12.8	10.1	100.0	100.0	99.9	100.0	99.9	2.7	3.7	4.1	4.2	4.2

TABLE II
EXPERIMENTAL RESULTS

[3] J. Zheng and M. Potkonjak, "Securing netlist-level FPGA design through exploiting process variation and degradation," in *International Symposium on Field-Programmable Gate Arrays*, 2012, pp. 129–139.

[4] R. Cochran, A. Nowroz, and S. Reda, "Post-Silicon Power Characterization Using Thermal Infrared Emissions," in *International Symposium on Low Power Electronics and Design*, 2010, pp. 331–336.

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

[6] F. Wolff, C. Papachristou, S. Bhunia, and R. Chakraborty, "Towards TROJAN-free trusted ICs: Problem analysis and detection scheme," in *Design, Automation and Test in Europe*, 2008, pp. 1362–1365.

[7] R. Rad, J. Plusquellic, and M. Tehranipoor, "Sensitivity analysis to hardware TROJANS using power supply transient signals," in *International Workshop on Hardware-Oriented Security and Trust*, 2008, pp. 3–7.

[8] M. Potkonjak, A. Nahapetian, M. Nelson, and T. Massey, "Hardware TROJAN horse detection using gate-level characterization," in *Design Automation Conference*, 2009, pp. 688–693.

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

[10] R. Rad, X. Wang, M. Tehranipoor, and J. Plusquellic, "Power supply signal calibration techniques for improving detection resolution to hardware trojans," in *International Conference on Computer-Aided Design*, 2008, pp. 632–639.

[11] W. Huang, S. Ghosh, S. Velusamy, K. Sankaranarayanan, K. Skadron, and M. Stan, "HotSpot: A Compact Thermal Modeling Methodology for Early-Stage VLSI Design," *IEEE Transactions onVery Large Scale Integration Systems*, vol. 14, no. 5, pp. 501 – 513, 2006.

[12] J. Yang, D. Zhang, A. Frangi, and J. yu Yang, "Two-dimensional pca: a new approach to appearance-based face representation and recognition," *Pattern Analysis and Machine Intelligence*, vol. 26, no. 1, pp. 131 – 137, 2004.

[13] A. Agarwal, "Statistical timing analysis using bounds and selective enumeration," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 22, no. 9, pp. 1243 – 1261, 2003.

[14] A. Srivastava, R. Bai, D. Blaauw, and D. Sylvester, "Modeling and analysis of leakage power considering within-die process variations," in *Low Power Electronics and Design*, 2002, pp. 64 – 67.