Gate-Level Characterization: Foundations and Hardware Security Applications

Sheng Wei Saro Meguerdichian Miodrag Potkonjak
Computer Science Department
University of California, Los Angeles (UCLA)
Los Angeles, CA 90095
{shengwei, saro, miodrag}@cs.ucla.edu

ABSTRACT

Gate-level characterization (GLC) is the process of characterizing each gate of an integrated circuit (IC) in terms of its physical and manifestation properties. It is a key step in the IC applications regarding cryptography, security, and digital rights management. However, GLC is challenging due to the existence of manufacturing variability (MV) and the strong correlations among some gates in the circuit. We propose a new solution for GLC by using thermal conditioning techniques. In particular, we apply thermal control on the process of GLC, which breaks the correlations by imposing extra variations concerning gate level leakage power. The scaling factors of all the gates can be characterized by solving a system of linear equations using linear programming (LP). Based on the obtained gate level scaling factors, we demonstrate an application of GLC, hardware Trojan horse (HTH) detection, by using constraint manipulation. We evaluate our approach of GLC and HTH detection on several ISCAS85/89 benchmarks. The simulation results show that our thermally conditioned GLC approach is capable of characterizing all the gates with an average error less than the measurement error, and we can detect HTHs with 100% accuracy on a target circuit.

Categories and Subject Descriptors

K.6.5 [**Management of Computing and Information Systems**]: Security and Protection—*Physical Security*

General Terms

Security

Keywords

Gate-level characterization, thermal conditioning, hardware Trojan horse, manufacturing variability.

DAC '10, June 13-18, 2010, Anaheim, California, USA

1. INTRODUCTION

The consequences of deep submicron technologies include exponentially increasing leakage energy, ever increasing substrate noise, profound and intrinsic manufacturing variability (MV), increased susceptibility to environmental (e.g. thermal) and operational (e.g. supply voltage) variation, and device aging. Among them, MV has emerged as the most profound and essentially redefined synthesis and analysis flow. It has formed a natural basis for conceptually new types of cryptography, security, and digital rights management [1][2][3][4].

However, MV is a suitable and plausible explanation for any discrepancy against the nominal design in terms of delay, switching or leakage energy. Therefore, MV greatly complicates the detection of hardware Trojan horses (HTHs), which are malicious alterations of designs. The alterations may be done by untrusted synthesis or FPGA configuration tools, untrusted hardware intellectual property, and even untrusted members of the design team.

Gate-level characterization (GLC) is the process of characterizing each gate of an integrated circuit (IC) in terms of its physical properties, such as gate width and length, or its manifestation properties, such as leakage power and switching power. It is important to note that GLC has a strong impact beyond hardware security. For example, Intel regularly adjusts supply and threshold voltages on its microprocessors in order to maximize yield and adapt to needs of desktop (speed) and mobile (energy) computing. GLC is also the starting point for post-silicon optimization [9]. Furthermore, GLC is a universal HTH defense technique that can be used for detection of very small HTHs (e.g. a single inverter). Therefore, effective GLC is our primary objective.

In this paper, we have two strategic goals: (i) to advance GLC state-of-the-art; and (ii) to develop generic HTH detection techniques. Our three technical contributions include development of coordinated GLC flows, thermal conditioning, and constraint manipulation of equations. We found that during the process of GLC, regardless of the number of measurements and their accuracy, often a significant number of gates in many designs cannot be characterized due to linear dependencies and limited controllability. Our solution is to use thermal conditioning, which is intentional nonuniform heating of an IC. The crucial observation is that leakage energy increases exponentially with temperature. Therefore, it provides a simple and practical way to conduct GLC accurately regardless of the structure and functionality of the design. To the best of our knowledge, it is the first use of conditioning techniques in both synthesis and security.

2. RELATED WORK

GLC is essential for many architectural and synthesis tasks, and has been applied in various hardware security applications. For example, techniques and applications based on GLC have been developed in HTH detection [1], digital rights management [2], hardware metering [3], physically unclonable functions (PUFs) [4], and PUF reverse engineering [5]. Also, many other hardware-based security applications have been motivated by GLC [6] [7].

There are two main and orthogonal approaches for GLC. The first one focuses on direct measurement of physical parameters using sophisticated microscopes [8]. The second one measures global delays between flip-flops or leakage/switching power for different input vectors and uses various techniques for solving systems of equations under various assumptions to find individual gate characteristics [9] [10] [11]. The advantages of the first approach is that one can directly measure all gates on each IC regardless of design structure. However, the approach is very expensive and slow and requires wafer-level inspection, where there is significant potential for damage. On the other hand, the second approach is fast, inexpensive, and can be applied on packaged ICs, but sometimes a percentage of gates can not be characterized due to correlations.

Recently, there has been an exponentially increasing interest in HTH detection. A comprehensive survey of HTH techniques is presented in [12]. Probably one of the first to explore HTH detection is the IBM paper [13], where side channels are used for circuit fingerprinting. This technique works well, but only if it is assumed that there is no MV, which is unfortunately intrinsic for all deep submicron silicon technologies. Jie and Lach [14] were the first to address HTH detection in the presence of MV. Recent UCLA research [15] [16] proposed HTH detection using GLC, a technique which is effective in the presence of MV. However, it is rather often the case that one cannot characterize all gates due to collinearity and therefore cannot detect collinear HTHs.

3. PRELIMINARIES

The manufacturing process of ICs may introduce two types of variations on gate characteristics: intra-chip variations and inter-chip variations. Intra-chip variations only impact the gates within a single chip, where spatial correlations exist and take effect. We use the same equation as in the work of [9] to model the intra-chip variations:

$$s(x, y) = s(0, 0) + \delta_x x + \delta_y y + \epsilon \tag{1}$$

where $s(x, y)$ is the expected scaling factor of the gate at location(x,y); δ_x and δ_y are parameters indicating the spatial variance along the x and y directions; and ϵ is the random intra-chip variation, which is represented by a multivariate normal distribution (MVN). Inter-chip variations are the variations among different chips, which have the same impact on the gates within the same chip, but behave differently on different chips. We represent inter-chip variations in our model by altering the parameter $s(0, 0)$ in (1) for each chip, and the variations follow MVN.

The power measured from the external pins is by no means accurate, due to environmental variations, random noise, or hardware inaccuracies. We model the measurement errors as the following:

$$\tilde{p} = (1 + e_s + e_r)\, p \tag{2}$$

where $\tilde{p}$ is the measured power; p is the actual power; e_s is the systematic error imposed on each gate, which we assume to be consistent over all gates; and e_r is the random error, which is caused by some random factors in the measurement. For e_r, we consider the triangular distribution in this paper.

We will be using leakage power in characterizing the scaling factors. In order to take the effect of MV into account, we define a MV scaling factor s_i for each gate, and model the leakage power in the following way:

$$p_j = \sum_{\forall gate\ i=1,\ldots,n} K_{ij}\, s_i \tag{3}$$

where p_j is the measured full-chip leakage power at input state j, as specified in (2); s_i is the MV scaling factor of gate i that we are characterizing; and K_{ij} is the nominal leakage power for the gate at input state j, which is dependent on the subthreshold leakage and the gate tunneling leakage. The values of K_{ij} can be found in [18].

The modeling of switching power is similar to that of leakage power, except that the coefficients K_{ij} are now changed to the nominal values of switching power, and the gates which are considered only include those that switch states when the primary input vector switches from one to another.

4. GATE LEVEL CHARACTERIZATION

Our approach for GLC is to keep taking power measurements while changing the primary input states of the circuit. Then, we can generate a system of equations in the form of (3). Next, we can formulate a LP in which the objective function is to minimize the measurement errors. After solving the LP, we obtain results for the characterized scaling factors. Specifically, the system of equations which serves as the constraints in the LP is the following:

$$K \cdot s = \tilde{p} + e \tag{4}$$

where $K \in R^{m \times n}$ is the matrix of coefficients for leakage power based on gate types and input states, with m the number of measurements and n the number of gates on the chip. s, $\tilde{p}$, and e are one-dimensional vectors representing the scaling factor of each gate, the measured power, and the measurement error in each measurement, respectively. The format of (4) meets that of linear constraints in a LP, in which we are minimizing the $l1$-norm of the measurement errors. The objective function is the following:

$$min \quad \sum_{i=1,\ldots,m} |e_i| \tag{5}$$

We propose a systematic way of formulating and solving the LP. We first pre-process the input vectors so that good coefficients can be found which help make the equations more independent from each other. This would be a regressive process since we need to detect the correlations in the formulated equations, in order to find those gates that are not differentiable by the LP solver. We then take measurements for leakage power and generate a system of equations based on the power model. After getting results from the LP solver, we do post-processing using maximum likelihood estimation (MLE) to improve the accuracy.

4.1 Leakage Power vs. Switching Power

As mentioned earlier, there are two types of power models that we can utilize in GLC: leakage power and switching power. The leakage power measurement accounts for all the gates in the target circuit, while the switching power measurement only takes the switching gates into consideration. In most cases, the switching power model could help reduce the number of variables, due to the fact that the number of switching gates is much less than the number of gates in the entire circuit. However, from the perspective of HTH detection, we should consider using leakage power, because it covers all the gates in the circuit and thus makes the HTH impossible to hide from our measurement.

4.2 Correlation Detection

The matrix K in (4) and thus the formulation of the LP is highly dependent on the choice of input vectors. In order to characterize the scaling factors accurately, our goal is to minimize the dependencies among the system of equations, because there are gates which are correlated with each other in the circuit. We define two types of correlation: (i) between gates that always have the same ratio of coefficients (TYPE1 correlation); and (ii) between gates that are not correlated in nature, but that we are not able to obtain enough independent equations to make differentiable by the solver (TYPE2 correlation). Figure 1 shows some examples of TYPE2 correlations in Benchmark C499 and C880.

For the detection of TYPE1 correlation, we add one more constraint which sets one of the suspicious correlated gates to a very large value, and if correlations exist, the solution of LP would show that some other variables become very small. For TYPE2 correlations, the detection is not trivial, because the number of subparts of the circuit that can possibly have TYPE2 correlations is huge. We solve the problem by manipulating the objective function. In particular, we change the objective function to maximize one single variable which is suspected to be the leading gate in some correlated subparts, such as gates x69 and x70 in Figure 1(a). If the gates in the subpart of the circuit do have TYPE2 correlation, the other variables would become very small.

4.3 Maximum Likelihood Estimation

In order to improve the accuracy of GLC, we apply statistical methods during and after the GLC process. First, we improve the objective function by assuming that errors are independent and by maximizing the ML function of the error distribution instead of the $l1$-norm. Then, we apply piecewise linear approximation which approximates the nonlinear ML function with piecewise linear segments. Second, we do post-processing using MLE. In particular, we take k different subsets of measurements and obtain k different sets of characterization results. We then select the best result for each variable using MLE. The probability density functions were obtained from a learning set of the characterized MV scaling factors.

5. GLC USING THERMAL CONDITIONING

We break the detected correlations using conditioning techniques, by which we expect to bring extra variations to the current power measurement model. We have the following observation: the leakage power grows exponentially as the temperature increases. The leakage power follows [17]:

$$I_{leakage} = \mu_0 \cdot C_{OX} \cdot \frac{W}{L} \cdot e^{b(V_{dd}-V_{dd0})} \cdot v_t^2 \cdot (1 - e^{\frac{-V_{dd}}{v_t}}) \quad (6)$$

where thermal voltage(v_t) and threshold voltage(v_{th}) are variables dependent on the temperature. The other parameters are constants and can be derived using transistor-level simulation.

Our solution to thermal conditioning is shown in Figure 2. We first calculate the generated heat per switch for each gate through switching power characterization. Meanwhile, we select our expected temperatures for each unit of the target IC. By applying these temperatures, some good independent coefficients can be obtained. We plug in the expected temperatures to our thermal control model which emulates the heat transfer process using LP, and provides us with the total amount of heat that is needed for some specific gates in the circuit. We then heat up the specific gates, for the amount of heat, based on their switching power characteristics. Finally, with the new temperatures generated from thermal conditioning, we come up with the new leakage coefficients by doing leakage power characterization.

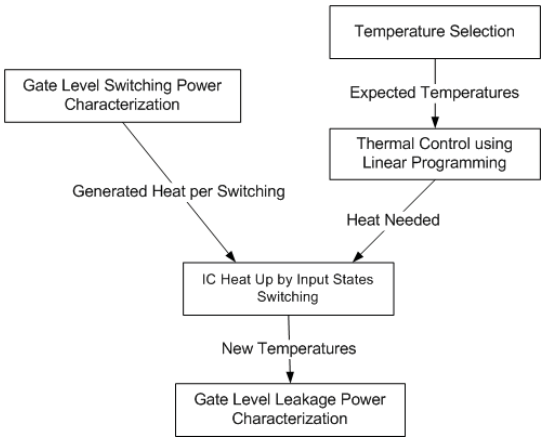
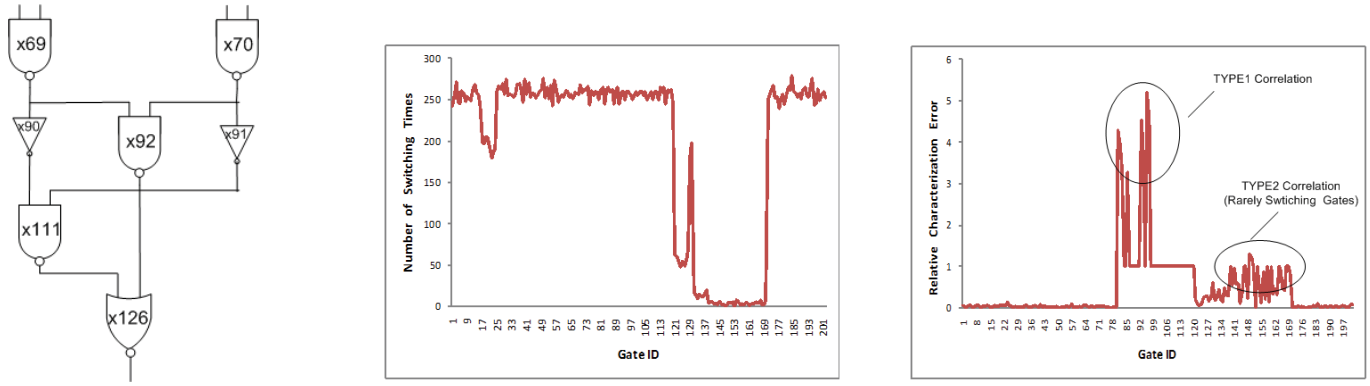


Figure 2: Flow of Thermal Conditioning for GLC

5.1 Switching Power Characterization

The way we heat up the circuit is by switching the input vectors in an organized way so that some gates in the circuit switch many times and their temperatures increase. In this way, we can take some specific gates to higher temperatures, which will serve as the sources of thermal conditioning for the entire circuit. The problem is that we must decide how many times we need to switch the input states in order to reach our expected temperature. It depends on two factors: the generated heat per switch and the total amount of necessary heat. We get the former from gate level switching power characterization and the latter from the thermal control process.

The switching power can be characterized from the characterization results of scaling factors, which have been discussed in Section 4 using the switching power model. The set of specific gates we would use as the sources of thermal conditioning is determined by the primary input vector. We use equation (3) to calculate the switching power (i.e. the generated heat per switch) for each gate. In particular, the switching power is formulated as follows:



(a) TYPE2 Correlations (b) Number of Switches (c) Characterization Errors

Figure 1: Examples of TYPE2 Correlations ((a) in the leakage power model; (b)(c) in the switching power model): (a) shows a subpart of C880 circuit, in which the two outputs of x69 and x70 drive five gates: x90, x91, x92, x111, x126. There are not enough independent equations that can be achieved for solving the five gates. (b) shows the number of switches of each gate in benchmark C499, when 1024 switches of input vectors are applied (gates 118-171 are rarely switching gates compared to others); (c) shows the characterization error for each gate. The large errors in gate 81-120 are due to TYPE1 correlation; the inaccuracies in gates 118-171 are due to TYPE2 correlation.

$$\Delta Q_i = K_{ij} \cdot s_i \tag{7}$$

where ΔQ_i is the switching power for gate i; K_{ij} is the leakage coefficient for the gate i at input state j; and s_i is the characterized scaling factor of gate i.

5.2 Heat Dissipation Characterization

Heat dissipation in a circuit is the transition of thermal energy from hotter gates to cooler gates; eventually, all the gates reach the static state temperatures. The process follows Fourier's law as described in [19]. Here we consider using the static state temperature because the initial temperature of the circuit is unknown, and there is no way to predict the dynamic state temperature even if we know about the generated heat.

We expect to calculate the total amount of heat needed for setting up our expected temperatures. In order to obtain this information from the heat transfer model, we formulate the heat transfer process as a LP according to Fourier's law. The constraints in the LP are the following:

$$\begin{aligned}
&\Delta Q_i = \Delta Q_{out_i} + \Delta Q_{in_i} + \Delta Q_{i,d} \\
&\Delta Q_{out_i} = H \cdot A_{surface} \cdot (\theta_{avg_i} - \theta_{air}) \cdot \Delta t \\
&\Delta Q_{in_i} = m \cdot c \cdot (\Delta \theta_i) \cdot \Delta t \\
&\Delta Q_{i,d} = -k \cdot A_{side} \cdot \frac{\theta_{avg_i} - \theta_{avg_{i,d}}}{\Delta x} \cdot \Delta t
\end{aligned} \tag{8}$$

The set of equations comes from conservation of energy and Fourier's law [19], where H and k are coefficients regarding heat transfer and conductivity; m and c are coefficients regarding the silicon in the circuit. ΔQ_i is the switching power of gate i; ΔQ_{out_i} and ΔQ_{in_i} stand for the energy exchanged between the gate and the air; $\Delta Q_{i,d}$ means the energy exchanged between neighboring gates, in which index d represents a certain direction of the neighbor. θ_{avg_i} ($\theta_{avg_{i,d}}$) denotes the average temperature of gate i (neighbor of gate i on the d direction) before and after heat transfer. The objective of LP is to get as close to the expected temperatures as possible. In other words, we need to minimize the discrepancy between the generated temperature and expected temperature.

After obtaining outputs from the above two steps, we can calculate the number of switches that are needed for heating up the circuit. We then apply the exact number of switches onto the circuit. Our observation is that the time needed for switching is in the level of nanoseconds, compared to the level of seconds for heat transfer. Therefore, it is possible that we can have the heated gates as expected before the heat transfer begins. Then, we can follow (6) to set the new coefficients in the linear equations based on the input states and expected temperatures. In this way, we are able to make much more independent linear equations which help break the correlations.

6. HTH DETECTION USING THERMALLY CONDITIONED GLC

A hardware Trojan horse (HTH) [12] is a malicious modification on an IC, which is intentionally made by adversaries in order to attack the target hardware. By modifying the circuitry of an IC, a HTH may alter the functionality of the circuitry, change the original characteristics (propagation delay or leakage power), or even leak confidential information.

HTHs have a huge impact on and pose a significant threat to the IC industry. Nowadays, outsourcing has become a trend for IC companies to increase their revenues. As a matter of fact, today's IC design and manufacturing is a global business which spreads all over the world. However, due to the existence of HTHs, hardware security is not always guaranteed, especially for those IC designs from untrusted factories. It is difficult to address this issue during the manufacturing process, because in the current manufacturing model of ICs, the manufacturing process is exposed to everyone who is in charge. Therefore, HTH detection after manufacturing is of high necessity and has become a

main concern in the IC industry. There are typically two types of HTH attacks: 1) gate resizing, by which the power or delay characteristics of the gate can be modified; and 2) adding additional gates to the circuit, which may not only change the characteristics but also leak confidential information from the design.

We are able to do HTH detection based on the thermally conditioned GLC. HTH detection is to tell whether any HTHs exist on the circuit or not. Our approach for HTH detection is to use constraint manipulation based on GLC. The key idea is that the leakage power of HTHs will cause variation in the power measurement, which will change the characterization results of MV scaling factors. In order to clearly capture the impact of HTH, we first assume some HTHs exist somewhere in the circuit. Since we do not know any information about their types, locations, or input signals, we just use a single variable (called the HTH variable) to represent them in the LP formulation. Then we solve the LP and check the value of the HTH variable in the solution, which would serve as an indicator for the existence of HTHs. In particular, if the characterization result of the HTH variable is close to 0, we conclude that no HTHs are on the chip; otherwise, we assume some HTHs exist.

The equation after constraint manipulation is the following, as modified from (4):

$$var_{hth} + K \cdot s = \tilde{p} + e \tag{9}$$

where var_{hth} is the HTH variable as the indicator for HTHs. By solving the LP with updated constraints, the existence of HTHs can be inferred from the characterized HTH variable.

7. SIMULATION RESULTS

We evaluate our thermally conditioned GLC approach, as well as the HTH detection scheme, by a set of simulations on ISCAS85/89 benchmarks. We also apply thermal conditioning in order to break the correlations and characterize as many gates as possible. We use the triangular distribution as our measurement error model. The leakage coefficients are obtained from [18]. The LP solver we use is lp_solve 5.5.

7.1 Thermally Conditioned GLC

Our simulation results for thermal conditioning are shown in Figure 3 and Figure 4, in which we use thermal conditioning to break the correlations. Figure 3 indicates that the TYPE1 correlation is broken after thermal conditioning: the ratios of coefficients between gate x97 and x99 now have 8 distinct values compared to only 1 value before thermal conditioning. Figure 4 demonstrates that the TYPE2 correlation discussed in Figure 1(a) is removed; there are 36 combinations of coefficients for the 5 gates compared to 4 combinations before thermal conditioning.

We simulate the thermally conditioned GLC on several ISCAS85/89 benchmarks, in which we apply 32 thermal conditions on each benchmark, with 1024 leakage power measurements, and compare the characterization results to those without thermal conditioning. The average measurement error is modeled as 1% of the measured power. The characterization results are shown in Table 1. Our thermally conditioned approach characterizes 100% of the gates with an average error less than 1%, while the approach without thermal conditioning can only handle a subset of the gates (27.4% to 95.0%) due to correlations.

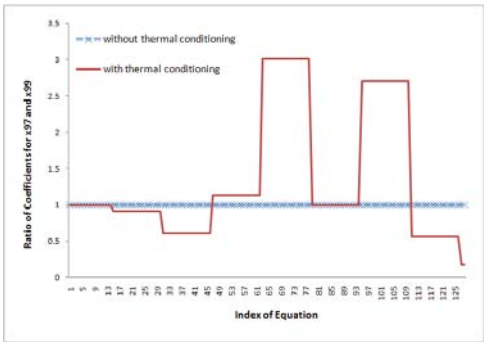


Figure 3: Breaking TYPE1 Correlations

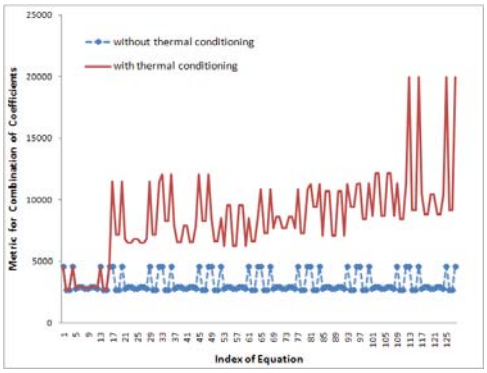


Figure 4: Breaking TYPE2 Correlations

Table 1: Accuracy of GLC on ISCAS85/89 Benchmarks with 1% Leakage Power Measurement Error

Benchmark	Gates	Using Thermal	Characterized Gates	Result Error (%)
C17	6	No	6 (100%)	0.00572
		Yes	6 (100%)	
C432	160	No	152 (95.0%)	0.108
		Yes	160 (100%)	
C499	202	No	162 (80.2%)	0.255
		Yes	202 (100%)	
C880	383	No	299 (78.1%)	0.339
		Yes	383 (100%)	
C1355	546	No	442 (81.0%)	0.398
		Yes	546 (100%)	
S526	214	No	149 (69.6%)	0.330
		Yes	214 (100%)	
S832	292	No	80 (27.4%)	0.726
		Yes	292 (100%)	

7.2 HTH Detection

We evaluate our HTH detection approach on the ISCAS85 and ISCAS89 benchmarks. For each benchmark, we simulate two cases where the HTHs do not exist or are embedded at some random locations on the target circuit. Our HTH detection scheme uses an extra HTH variable as the indicator of HTHs. We repeat the leakage power measurement for all the benchmarks 50 times and plot the probability density function (PDF) of the HTH variable in Figure 5. We observe a large enough difference between the two cases in terms of the probability distribution of the HTH variable. It enables us to draw a decision line between the two situations, with which we can achieve zero false positives and zero false negatives in HTH detection.

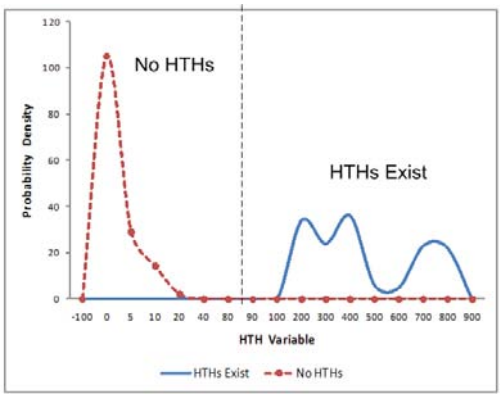


Figure 5: PDF of the HTH variable in HTH detection, integrated with all the ISCAS85/89 benchmarks in Table 1.

8. CONCLUSIONS

We propose a gate level characterization approach based on thermal conditioning. By utilizing the extra variances obtained from the thermal control process, we are able to break all the correlations in the target circuit. It enables us to characterize the scaling factors for all the gates in the circuit, which is done by solving a system of power measurement equations using LP. We further improve the accuracy of the characterization by applying statistical methods in the formulation of the objective function as well as the post-processing stage. Based on the obtained gate level characteristics, we design a HTH detection scheme by using constraint manipulation techniques. The simulation results on several ISCAS85 and ISCAS89 benchmarks show that we are able to characterize all the gates with an average error less than the measurement error, and the HTHs can be detected with 100% accuracy by our approach.

9. ACKNOWLEDGMENTS

This research is partially supported by the Center for Domain-Specific Computing (CDSC) funded by the NSF Expedition in Computing Award CCF-0926127.

10. REFERENCES

[1] M. Banga, M. Hsiao. A Region Based Approach for the Identification of Hardware Trojans. HOST 2008, pp. 40-47.

[2] G. Qu, M. Potkonjak. Intellectual Property Protection in VLSI Designs: Theory and Practice. Kluwer Academic Publishers, 2003.

[3] F. Koushanfar, G. Qu, M. Potkonjak. Intellectual Property Metering. Information Hiding 2001, pp. 81-95.

[4] N. Beckmann, M. Potkonjak. Hardware-Based Public-Key Cryptography with Public Physically Unclonable Functions. Information Hiding 2009, pp. 206-220.

[5] M. Majzoobi, F. Koushanfar, M. Potkonjak. Techniques for Design and Implementation of Secure Reconfigurable PUFs. ACM TRETS, Vol.2 No.1, 2009, pp. 1-33.

[6] F. Koushanfar, M. Potkonjak. CAD-based Security, Cryptography, and Digital Rights Management. DAC 2007, pp. 268-269.

[7] Y. Alkabani, F. Koushanfar. Consistency-based Characterization for IC Trojan Detection. ICCAD 2009, pp. 123-127.

[8] P. Friedberg, Y Cao, J. Cain, R. Wang, J. Rabaey, C. Spanos. Modeling Within-Die Spatial Correlation Effects for Process-Design Co-Optimization. ISQED 2005. pp. 516-521.

[9] Y. Alkabani, T. Massey, F. Koushanfar, M. Potkonjak. Input Vector Control for Post-silicon Leakage Current Minimization in the Presence of Manufacturing Variability. DAC 2008, pp. 606-609.

[10] Y. Alkabani, F. Koushanfar, N. Kiyavash, M. Potkonjak. Trusted Integrated Circuits: A Nondestructive Hidden Characteristics Extraction Approach. Information Hiding 2008, pp. 102-117.

[11] F. Koushanfar, P. Boufounos, D. Shamsi. Post-silicon Timing Characterization by Compressed Sensing. ICCAD 2008, pp. 185-189.

[12] M. Tehranipoor, F. Koushanfar. A Survey of Hardware Trojan Taxonomy and Detection. IEEE Design and Test of Computers, Vol. 27, No. 1, 2010, pp. 10-25.

[13] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, B. Sunar. Trojan Detection Using IC Fingerprinting. S&P 2007, pp. 296-310.

[14] J. Li, J. Lach. At-Speed Delay Characterization for IC Authentication and Trojan Horse Detection. HOST 2008, pp. 8-14.

[15] M. Nelson, A. Nahapetian, F. Koushanfar, M. Potkonjak. SVD-Based Ghost Circuitry Detection. Information Hiding 2009, pp. 221-234.

[16] M. Potkonjak, A. Nahapetian, M. Nelson, T. Massey. Hardware Trojan Horse Detection Using Gate-level Characterization. DAC 2009, pp. 688-693.

[17] K. Skadron, M. Stan, W. Huang, S. Velusamy, K. Sankaranarayanan, D. Tarjan. Temperature-aware Microarchitecture. ISCA 2003, pp. 2-13.

[18] L. Yuan, G. Qu. A Combined Gate Replacement and Input Vector Control Approach for Leakage Current Reduction. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol. 14, No. 2, 2006, pp. 173-182.

[19] J. Lienhard IV, J. Lienhard V. A Heat Transfer Textbook, 3rd edition, Phlogiston Press, 2003.