Integrated Circuit Security Techniques Using Variable Supply Voltage

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

ABSTRACT

This paper addresses integrated circuit (IC) security issues by using supply voltage based gate-level characterization (GLC). Our GLC scheme is capable of characterizing both manifestation and physical level properties of an IC accurately using variable supply voltage. We demonstrate that the proposed scheme can detect three types of IC attacks with low false positives and false negatives.

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, integrated circuit security, process variation, supply voltage control

1. INTRODUCTION

With the fast growth of IC outsourcing, hardware security has become a major concern and has drawn a great deal of attention in the IC industry [1]. IC products from untrusted foundries must be fully tested to ensure that no malicious alterations have been made. However, due to the consequences of deep submicron technologies, process variation (PV) [2] becomes an unavoidable component in the manifestation and physical properties of ICs. Adversaries can easily hide their malicious attacks under the unrecognized PV, since it is difficult to distinguish the variation caused by PV from malicious attacks.

Efforts have been made to characterize the impact of PV and address the resulting security issues. PV modeling [2] develops statistical models to predict PV. The models can be very accurate, but they only work for a population of ICs and cannot address the security issues for a specific IC instance. Physical inspection [3] focuses on direct measurements of physical parameters using sophisticated microscopes. It can measure the physical properties of all gates regardless of the design structure, but it is very expensive and has a potential to damage the target IC. Side channel-based approaches [4][5][6] characterize ICs in terms of their manifestational properties. However, the manifestational properties are impacted by many factors (e.g. temperatures), which may reduce the accuracy of detection.

We propose a gate-level characterization (GLC) approach to uncover the impact of PV and address the IC security issues in an inexpensive way. In order to avoid the high instrumentation in physical methods and the instability in manifestation-level side channel analysis, we characterize the gate-level physical properties, such as effective length (L_{eff}) and threshold voltage (V_{th}), in a nondestructive way and use them as indicators for malicious attacks on the ICs. Our approach is based on the manipulation of supply voltage (V_{dd}), which provides us with an accurate control over the manifestation-level properties and enables us to characterize the physical-level properties accurately. We further improve our characterization accuracy by applying statistical analysis on the obtained results. For demonstration and evaluation purposes, we analyze three types of IC security attacks and show how our V_{dd}-based GLC scheme resolves them.

Our main contributions include: (i) a manifestation-level GLC (M-GLC) and a physical-level GLC (P-GLC) approach using supply voltage control, which solves the correlation issues in the characterization process and provides us with accurate characterization results; (ii) the use of statistical methods, namely maximum likelihood estimation (MLE), to improve the GLC accuracy; and (iii) a systematic way to detect gate resizing attacks, aging attacks, and power supply network attacks using our proposed GLC methods.

2. RELATED WORK

Management of supply voltage has been a popular and important energy minimization technique for more than two decades [7]. However, it has not been used until now as a tool for the detection of a variety of hardware attacks.

In the last five years, gate characterization emerged as one of the most important enabling steps during circuit synthesis and analysis. There are two schools of thought. The first advocates direct measurements of transistor parameters such as channel length or thickness of oxide [3]. More recently, several efforts have been undertaken to use measurements of delay, leakage, and/or switching power in or-

DAC'11, June 5-10, 2011, San Diego, California, USA.

der to characterize the gates [8][9][10][11]. To the best of our knowledge, we for the first time analyze three non-functional circuit alterations that have significant detrimental impact on the operation of the pertinent ICs. Specifically, we consider gate resizing, aging, and power supply network attacks. Interestingly, all three attacks can be treated using the same framework of GLC using V_{dd} manipulation.

Gate resizing has been a crucial task for accomplishing simultaneous optimizations of delay, power, and area since very early beginnings of CAD [12]. In the mid-80s, Fishburn and Dunlop proposed a provably optimal approach to transistor sizing [13]. Phenomena such as negative-bias temperature instability (NBTI) are causing significant alterations of both delay and leakage. For example, aging can increase delay by 10% and leakage energy by several times [14]. Our novelty in this domain is that we expect that the attacker will intentionally produce such input vectors to the circuit that delay degradation will be maximized in terms of overall negative impact. Power supply networks (PSNs) are crucial for correct operations of ICs [15][16]. Power supply and ground voltage variations have significant impact on the performance of ICs and recently became a research topic of great interest [17]. For the first time, we explain not just how the attacker can launch PSN attacks but also techniques for detecting these malicious changes.

3. PRELIMINARIES

3.1 Process Variation, Power and Delay Model

PV in IC manufacturing is the deviation of IC parameter values from nominal specifications [2]. It causes major variations in gate-level physical properties such as L_{eff} and V_{th}, which are two major sources of PV. For example, due to the impact of PV, the actual L_{eff} of a manufactured gate can be expressed by Equation (1), where L_{nom} is the nominal design value of the effective length, and ΔL is the variation in the manufacturing process.

$$L_{eff} = L_{nom} + \Delta L \tag{1}$$

We use leakage power, switching power and delay as manifestational properties of an IC, which we expect to connect with the physical properties such as L_{eff} and V_{th}. Equation (2) is the gate-level leakage power model [18], where L is effective channel length, V_{th} is threshold voltage, W is gate width, V_{dd} is supply voltage, n is substreshold slope, μ is mobility, C_{ox} is oxide capacitance, D is clock period, ϕ_t is thermal voltage $\phi_t = kT/q$, and σ is drain induced barrier lowering (DIBL) factor.

$$P_{leakage} = 2 \cdot n \cdot \mu \cdot C_{ox} \cdot \frac{W}{L} \cdot \phi_t^2 \cdot D \cdot V_{dd} \cdot e^{\frac{\sigma \cdot V_{dd} - V_{th}}{n \cdot \phi_t}} \tag{2}$$

The gate-level switching power model [18] is described by Equation (3), where α is the switching probability.

$$P_{switching} = \alpha \cdot C_{ox} \cdot W \cdot L \cdot V_{dd}^2 \tag{3}$$

We use the delay model in [18] that connects the gate delay to its sizing and operating voltages:

$$Delay = \frac{k_{tp} \cdot k_{fit} \cdot L^2}{2 \cdot n \cdot \mu \cdot \phi_t^2} \cdot \frac{V_{dd}}{(ln(e^{\frac{(1+\sigma)V_{dd} - V_{th}}{2 \cdot n \cdot \phi_t}} + 1))^2} \cdot \frac{\gamma_i \cdot W_i + W_{i+1}}{W_i} \tag{4}$$

where subscripts i and $i+1$ represent the driver and load gates, respectively; γ is the ratio of gate parasitic to input capacitance; and k_{tp} and k_{fit} are delay-fitting parameter and model-fitting parameter, respectively.

We observe from the above models that the manifestational properties are dependent on L_{eff} and V_{th} in a non-linear manner and can be controlled via V_{dd} manipulation.

3.2 Manifestation-Level GLC

At the manifestation level [4][6], the power and delay models can be expressed in a linear format assuming that the variation of all the physical-level properties is represented by a single PV scaling factor K. Equation (5) shows the linear model at the manifestation level (using leakage power as an example).

$$\tilde{p_j} = e_{sj} + e_{rj} + \sum_{\forall gate\ i=1,\ldots,n} K_{ij}\ s_i \tag{5}$$

where $\tilde{p_j}$ is the full-chip leakage power at input state j; s_i is the PV scaling factor of gate i; K_{ij} is the nominal leakage power for the gate at input state j, which is dependent on the parameters in Equation (2) and the input vectors; and e_{sj} and e_{rj} are systematic and random measurement errors, respectively. We can obtain a set of linear equations by varying the input vectors and measuring the leakage power of the entire circuit. After that, by solving the system of equations with an objective function of minimizing the measurement errors, we can characterize the gate level PV scaling factors and thus obtain the leakage power for each gate.

4. GATE-LEVEL CHARACTERIZATION

4.1 Overall Flow

We characterize both the manifestation-level and physical-level properties of an IC using supply voltage manipulation. Our approach is based on the fact that the manifestational properties (delay and power) are dependent on the supply voltage V_{dd} in a non-linear manner, as shown in Equations (2) to (4). Therefore, V_{dd} brings extra variation to the manifestational properties and can serve as a correlation breaker to both the collinearity and insufficient controllability correlations, which are the major issues in M-GLC [4]. Also, the extra variation enables the formulation of multiple non-linear equations following Equations (2) to (4) so that the physical-level properties (L_{eff} and V_{th}) can be obtained by characterizing the manifestational properties and solving the non-linear equations.

Our overall flow of V_{dd}-based GLC is shown in Fig. 1. We first conduct manifestation-level GLC on the target circuit. During this process, we vary the input vector and the V_{dd} of the circuit, in order to obtain different power/delay values. Next, we formulate a system of linear equations based on the power/delay measurements and the abstraction of the PV impact using a PV scaling factor (discussed in Section 3.2). By solving the system of equations using linear programming (LP), we obtain the manifestation-level properties of each gate. Then, we begin the process of P-GLC, in which we follow Equations (2) to (4) to formulate a non-linear equation that connects the manifestational properties we obtained from M-GLC and the physical properties we are characterizing in P-GLC. In order to make the variables L_{eff} and V_{th} solvable, we manipulate the V_{dd} of the circuit and formulate a system of non-linear equations. After that,

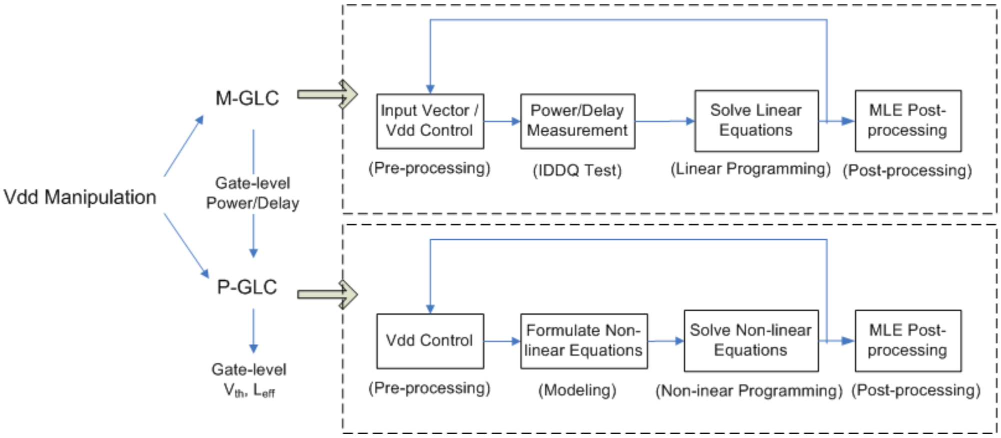


Figure 1: Flow of V_{dd}-based GLC scheme.

we solve the non-linear equations to obtain L_{eff} and V_{th} values for each gate.

4.2 Solving the Correlation Issues in M-GLC

As pointed out in [4], one of the major issues in M-GLC is the correlations in the system of linear equations. In particular, two types of correlations have been studied: (i) collinearity, where gates have the same ratio of K_{ij} values as appearing in Equation (5); and (ii) insufficient controllability, where no enough equations can be obtained due to the lack of controllability over the circuit. Both types of correlations make the system of linear equations unsolvable. [4] proposed a thermal conditioning method to break the correlation. However, it requires a long time for conditioning and has to suffer the instability of temperature due to heat transfer both on and off the circuit.

We instead use V_{dd} for resolving correlations. The idea is based on the non-linear relation between power/delay values and V_{dd} as shown in Equations (2) to (4). Taking leakage power as an example, we first select a range of V_{dd} values for the M-GLC process. The selected V_{dd} values are different from the nominal V_{th} values for a threshold we define, in order not to make the exponential part in Equation (2) too small and thus the leakage power value change too little when V_{dd} varies. Then, we apply the selected V_{dd} values to Equation (2) together with the input vector manipulation, and formulate the system of linear equations shown in Equation (5). The collinearity and insufficient controllability correlations are removed because of the non-linear relation between leakage power and V_{dd}. Note that the nominal leakage power value K_{ij} must be changed to reflect the changes in V_{dd}. We calculate and update the values of K_{ij} using Equation (2).

4.3 Physical-Level GLC

Based on the characterization results of M-GLC, we are able to formulate a non-linear equation based on Equation (2). It correlates L_{eff} and V_{th} with the leakage power. Also, we obtain leakage power from the M-GLC process as discussed in Section 3.2. However, with only one non-linear equation, we are not able to solve for both variables L_{eff} and V_{th}. Therefore, we must find a way to add additional variations to the leakage power model so that a system of equations can be obtained. We solve this problem by manipulating V_{dd} of the circuit. In particular, we select a set of V_{dd} values for the circuit and apply each of them to all the gates in M-GLC. The M-GLC provides us with the leakage power of each gate under each V_{dd} value, which enables us to formulate the following system of equations:

$$P_{leakage_i} = \frac{a}{L_{eff_i}} \cdot V_{dd_i} \cdot e^{\frac{bV_{dd_i} - V_{th_i}}{c}} \tag{6}$$

where index i indicates the case where the ith V_{dd} value is applied to all the gates on the circuit; a, b and c are constant parameters in the leakage power model. We can obtain the L_{eff} and V_{th} values for all the gates on the circuit by solving the system of non-linear equations.

4.4 Post-processing

The obtained characterization results in both M-GLC and P-GLC are subject to multiple sources of errors. The errors may come from power/delay measurements, approximation errors in linear/non-linear program solvers, and approximation errors in the power/delay model.

In order to reduce the impact of the errors and improve the characterization results, we conduct post-processing in the following way. First, we repeat the M-GLC and P-GLC processes multiple times in order to obtain a large enough sample of data. For M-GLC, the repeated experiments are from varying the selected input vectors and the V_{dd} values; for P-GLC, the variations in the repeated experiments are from the corresponding M-GLC results, as well as the different starter values in the Gauss-Newton method that we use for solving the system of non-linear equations. Second, we conduct maximum likelihood estimation (MLE) on the repeated GLC results in order to find out the most likely property value for each gate. We apply goodness-of-fit tests on the data from each run and estimate the statistical distribution of the predicted results over different runs. We take the value of L_{eff} (or V_{th}) as the one that maximizes the likelihood function ($p(L)$ is the probability density function of the L_{eff} distribution):

$$\tilde{L} = argmax_L \; log \; p(L) \tag{7}$$

5. HARDWARE SECURITY APPLICATIONS

With the accurate characterization of the gate-level properties, our P-GLC approach is capable of supporting various hardware security applications. In this section, we show how we detect several security attacks that are difficult to address using other methods.

5.1 Gate Resizing Attack

In a gate resizing attack, the attackers alter the sizing parameters (e.g. L_{eff}) of one or more gates on the circuit intentionally, with the goal of making the IC malfunction or leak more energy. In order to hide the attack under common detection schemes such as functional testing and timing analysis, the attackers tend to alter the sizes of gates in such a way that the ICs can still pass all the standard tests. For example, the attacker may reduce the L_{eff} of the gates that are rarely on the critical path, so that it is not detectable by a timing analysis but would cause the target IC to consume more leakage energy.

We use our V_{dd}-based P-GLC scheme to address the gate resizing attack. We characterize the value of L_{eff} for each gate on the circuit and compare it with the nominal design value. Since the characterization is now on the physical level, there are no other sources of variations to the nominal values, except the PV and possible gate resizing attacks imposed by the adversary. We can further exclude the impact of PV by comparing the P-GLC results with the nominal design values, from which the PV model for the IC instance can be achieved. We set a threshold value for each gate based on its PV property in the PV model. The threshold value is then used to check whether a specific L_{eff} value from the P-GLC process should be considered as a gate-resizing attack.

5.2 Gate Aging Attack

IC aging [14] is a physical process where the V_{th} values of the gates keep increasing while the gates are being used. As a result, there is a degradation in the speed of the IC because of the increase of gate delay according to Equation (4). The adversary may intentionally speed up the aging process by stressing one or more gates on the circuit. Such an attack can easily bypass a normal functional test or timing analysis because the functionality of the circuit stays the same, and the alteration in delay is not observable in the case that the attacked gates are not on the critical path. We are able to detect the gate aging attack based on P-GLC in terms of V_{th}. We set the threshold value in a similar manner as that in Section 5.1.

5.3 Power Supply Network Attack

PSNs provide a constant supply voltage to IC applications [15][16]. In the modern submicron technologies, ICs become more and more sensitive to the noise in PSNs, and consequently PSNs have become another possible source of attack. The attackers may intentionally reduce the resistance of a certain part of the circuit. As a result, the current through the PSN becomes higher and may make the PSN suffer from early time failure, due to the effect of electromigration [19].

The attack to PSN is not detectable unless a profile of the supply voltage drop down can be obtained and analyzed. We modify our GLC model under the assumption that the supply voltage of each gate may vary from its nominal value due to the noise from the PSN and possible attacks made by adversaries. Our modified P-GLC model from Equation (6) is the following:

$$P_{leakage_i} = \frac{a}{L_{eff_i}} \cdot V_{dd_i}(1-r_i) \cdot e^{\frac{bV_{dd_i}(1-r_i)-V_{th_i}}{c}} \qquad (8)$$

where r_i is the drop down rate of V_{dd_i}. By varying V_{dd} and solving the non-linear equations with three variables r_i, L_{eff_i}, and V_{th_i}, we can characterize r_i. If it exceeds our defined threshold, we conclude that the PSN has been attacked.

6. SIMULATION RESULTS

6.1 Gate Resizing Attack

We simulate the gate resizing attack by randomly resizing one gate on the circuit. Next, we use our V_{dd}-based GLC approach to detect the resized gate. Fig. 2 shows the distribution of relative characterization error of L_{eff} on ISCAS benchmark C432, in which we use 40 distinct V_{dd} values for the entire circuit in the P-GLC process. The results show that we have maximumly ±2% characterization errors, and the most likely error in the distribution is close to 0.

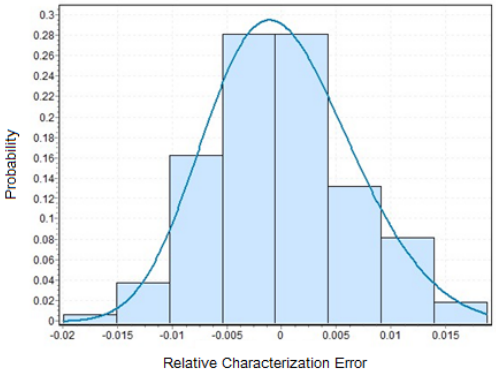
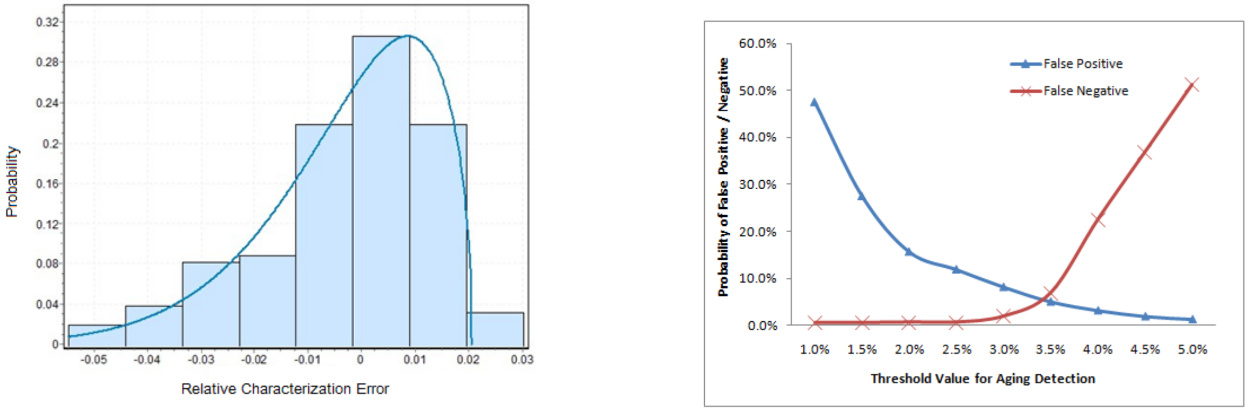


Figure 2: Accuracy of L_{eff} characterization in benchmark C432 for gate resizing detection.

Table 1: Probability of false positives and false negatives in gate resizing detection.

Resizing Rate	Threshold	False Positive	False Negative
-5%	1%	11.9%	0
	2%	0	0
	3%	0	0
	4%	0	5%
	5%	0	51.2%
5%	1%	11.9%	0
	2%	0	0
	3%	0	0
	4%	0	6.88%
	5%	0	48.8%

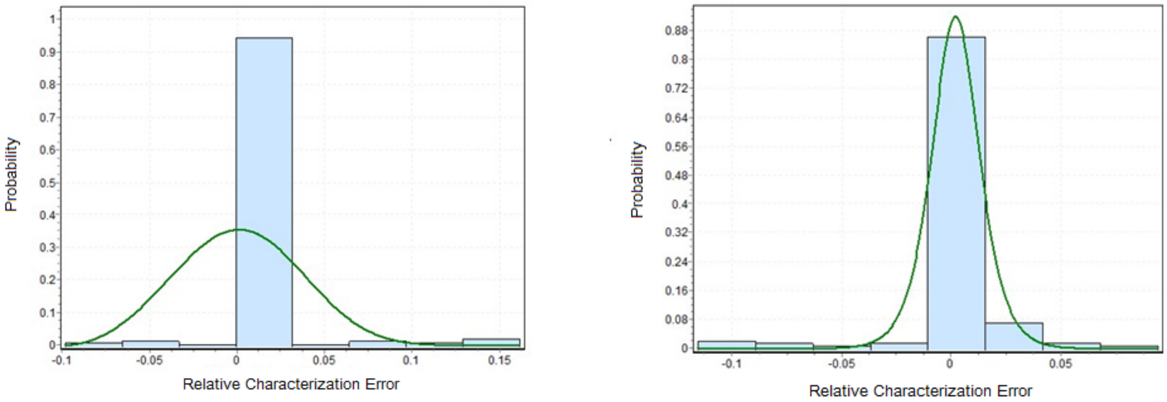
Based on the above L_{eff} characterization, we conduct gate resizing detection on the same benchmark circuit. We simulate the gate resizing attack for a random gate on the



(a)

(b)

Figure 3: Gate aging detection: (a) accuracy of threshold voltage (V_{th}) characterization; (b) probability of false positives and false negatives in aging detection (with an aging rate of 5%).



(a) Characterization *without* post-processing

(b) Characterization *with* post-processing

Figure 4: Accuracy of V_{dd} drop down characterization in power supply networks.

Table 2: Probability of false Positives and false negatives for gate resizing/aging detection, with a 5% resizing or aging rate and 3% threshold value for detection.

Benchmark	Resizing Attack		Aging Attack	
	False Positive (%)	False Negative (%)	False Positive (%)	False Negative (%)
C432	0	0	8.13	1.88
C499	0.495	0.495	3.47	5.94
C880	0.261	1.04	7.83	2.35
C1355	0.733	0.733	5.31	4.95
C1908	0.795	0.682	4.55	5.23
C2670	0.587	4.11	6.54	1.26
C3540	0.659	1.02	7.67	4.37
C5315	0.607	1.34	7.8	2.08
C6288	0.538	0.869	6.33	2.73
C7552	0.683	0.997	6.38	3.08

circuit with a ±5% resizing rate. For each of the resizing attacks, we simulate 5 threshold values (1% to 5%) in order to evaluate our approach under different parameter settings. We show in Table 1 the probability of false positives and false negatives resulting from the detection; the former indicates the cases where a certain gate has not been attacked but our scheme detects it as having been resized, and the latter represents the opposite. The results show that when the threshold value is properly selected (2% to 3%), our GLC approach can achieve both zero false positives and zero false negatives in the resizing detection. Table 2 shows our simulation results ragarding resizing attack on the ISCAS85 benchmarks, with a 5% resizing rate and a 3% threshold value. The false positives and false negatives are below 5% for all the benchmark circuits.

6.2 Gate Aging Attack

We simulate the gate aging attack by randomly selecting one gate on the benchmark circuit and increasing its V_{th} value by 5%. Next, we use our V_{dd}-based GLC scheme to characterize V_{th} for all gates and detect the aging attack. Fig. 3 shows our characterization and detection results on benchmark C432, in which we use 40 different V_{dd} values in the P-GLC process. Fig. 3(a) shows the accuracy of V_{th} characterization, which has relative errors of -5% to +3%. Fig. 3(b) shows the probabilities of false positives and false negatives in the aging detection, which are both below 10% if the threshold value is selected in the range of 3% to 4%. Table 2 shows our simulation results on the ISCAS85 benchmarks. All the false postives and false negateives are below 10%.

6.3 Power Supply Network Attack

We characterize the supply voltage drop down of the target IC in order to detect the possible PSN attacks. Fig. 4 shows our simulation results in terms of the characterization accuracy of the V_{dd} drop down. In Fig. 4(a) we demonstrate the results without using MLE post-processing, where the error ranges from -10% to +15% with a mean value around 0. The results are further improved by using MLE post-processing as shown in Fig. 4(b).

7. CONCLUSION

We develop a systematic way of conducting M-GLC and P-GLC using variable supply voltage. The correlation issues in M-GLC are resolved by varying the supply voltage. Also, we are able to characterize the physical-level properties L_{eff} and V_{th} by solving a system of non-linear equations. With the characterized physical properties, we demonstrate three IC attacks that can be addressed by our GLC approach (gate resizing attacks, gate aging attacks, and power supply network attacks). Our simulation results show that the proposed GLC scheme is capable of detecting IC security attacks with low false positives and false negatives.

8. ACKNOWLEDGMENTS

This work was supported in part by the NSF under awards CNS-0958369 and CNS-1059435.

9. REFERENCES

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

[2] B. Cheng, S. Roya, A. Browna, C. Millara, A. Asenov. Evaluation of Statistical Technology Generation LSTP MOSFETs. Solid-State Electronics, Vol. 53, 2009. pp. 767-772.

[3] 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.

[4] S. Wei, S. Meguerdichian, M. Potkonjak. Gate-level characterization: foundations and hardware security applications. DAC 2010, pp. 222-227.

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

[6] S. Wei, M. Potkonjak. Scalable Segmentation-Based Malicious Circuitry Detection and Diagnosis. ICCAD 2010, pp. 483-486.

[7] A. Chandrakasan, M. Potkonjak, R. Mehra, J. Rabaey, R. Brodersen. Optimizing Power Using Transformations. IEEE Transactions on CAD, Vol. 14, No. 1, 1995, pp. 12-31.

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

[9] S. Reda, S. Nassif. Analyzing the Impact of Process Variations on Parametric Measurements: Novel Models and Applications. DATE 2009, pp. 375-380.

[10] S. Wei, S. Meguerdichian, M. Potkonjak. Malicious Circuitry Detection Using Thermal Conditioning, accepted for publication in IEEE Transactions on Information Forensics and Security, 2011.

[11] S. Wei, M. Potkonjak. Scalable Hardware Trojan Diagnosis, accepted for publication in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2011.

[12] A. Ruehli, P. Wolff, G. Goertzel. Power and Timing Optimization of Large Digital Systems. ISCAS 1976, pp. 402-405.

[13] J. Fishburn, A. Dunlop. TILOS: A Posynomial Approach to Transistor Sizing. ICCAD 1985, pp. 326-328.

[14] M. Agarwal, B. Paul, M. Zhang, S. Mitra. Circuit Failure Prediction and Its Application to Transistor Aging, VTS 2007, pp. 277-286.

[15] K. Wang , M. Marek-Sadowska, On-chip Power Supply Network Optimization Using Multigrid-based Technique, DAC 2003. pp. 113-118.

[16] S. Sapatnekar, H. Su. Analysis and Optimization of Power Grids. IEEE Design & Test. Vol.20, No. 3, 2003, pp. 7-15.

[17] D. Li, S. Tan, Statistical Analysis of Large On-chip Power Grid Networks by Variational Reduction Scheme. Integration, the VLSI Journal, Vol. 43, No. 2, 2010. pp. 167-175.

[18] D. Markovic, C. Wang, L. Alarcon, T. Liu, J. Rabaey. Ultralow-Power Design in Near-Threshold Region. Proceedings of the IEEE, Vol. 98, No. 2, 2010. pp. 237-252.

[19] C. Tan, A. Roy. Electromigration in ULSI interconnects. Materials Science and Engineering, Reports 58, pp. 1-75.