Robust Passive Hardware Metering

Sheng Wei[‡] Ani Nahapetian[‡,*] Miodrag Potkonjak[‡]

[‡]Computer Science Department, University of California, Los Angeles (UCLA), Los Angeles, CA 90095

*Computer Science Department, California State University, Northridge (CSUN), Northridge, CA 91330

{shengwei, ani, miodrag}@cs.ucla.edu

ABSTRACT

Current hardware metering techniques, which use manifestational properties of gates for ID extraction, are weakened by the non-uniform effects of aging in conjunction with variations in temperature and supply voltage. As an integrated circuit (IC) ages, the manifestational properties of the gates change, and thus the ID used for hardware metering can not be valid over time. Additionally, the previous approaches require large amounts of costly measurements and often are difficult to scale to large designs.

We resolve the deleterious effects of aging by going to the physical level and primarily targeting the characterization of threshold voltage. Although threshold voltage is modified with aging, we can recover its original value for use as the IC identifier. Another key aspect of our approach involves using IC segmentation for gate-level characterization. This results in a cost effective approach by limiting measurements, and has a significant effect on the approach scalability. Finally, by using threshold voltage for ID creation, we are able to quantify the probability of coincidence between legitimate and pirated ICs, thus for the first time quantitatively and accurately demonstrating the effectiveness of a hardware metering approach.

Keywords

Passive hardware metering, usage metering, gate-level characterization.

1. INTRODUCTION

Since semiconductor manufacturing demands a large capital investment, the role of contract foundries has dramatically grown, increasing exposure to mask theft and unauthorized excess fabrication. Hence hardware metering approaches have been proposed and implemented for identifying pirated integrated circuits (ICs).

Hardware metering is the process of differentiating legitimate ICs from pirated ICs, by verifying a unique identifier associated with the IC. There exist two general classes of hardware metering approaches: active and passive. In active hardware metering, either new hardware or a programmable model is inserted into the IC to generate unique identifiers (IDs) [17]. In the more sophisticated passive metering schemes [1][3], the inherent uniqueness of the ICs, which is a result of intrinsic process variation, is leveraged to determine a unique ID for the IC, without modifying the IC design or manufacturing process.

Current passive hardware metering techniques extract IC IDs using manifestational properties, such as leakage power, switching power, and delay, of gates. We describe four drawbacks with the current state-of-the-art passive metering approaches.

First, manifestational properties have been shown to vary and age non-uniformly under the combination of switching and variations in temperature and supply voltage. IDs extracted after a gate has aged will be different from previously calculated and stored IDs, and thus IDs from legitimate ICs will be deemed invalid, undermining the whole approach. As a result, we argue that previous hardware metering techniques will malfunction as aging modifies the manifestational characteristics of gates.

Secondly, previously proposed approaches are cost prohibitive, due to their requirement to characterize all the gates of an IC, with a high level of precision. The process of extracting the manifestational characteristics of gates requires a great deal of input vector application to the IC, thus making the approach costly and impractical.

Reciprocally, the approaches become difficult to scale to large ICs, as solving the large system of linear equations can be prohibitively time-consuming.

Finally, manifestational characteristics of gates are correlated across an IC. Thus it is not possible to quantify the uniqueness of the IDs extracted, which practically prevents the approach's feasability from being evaluated quantitatively.

These four challenges are overcome in the current work using two main advances. First, manifestational properties, which can be extracted using side-channel measurements, are used to go to the physical level, primarily to extract the threshold voltage of gates. Other physical properties can also be extracted such as the channel length. Even though the threshold voltage will degrade with age, we provide a procedure for extracting the original threshold voltage of a gate, from two or more non-original threshold voltage values. The original threshold voltage is independent of

variations caused by aging, temperature, and supply voltage instability, and hence can serve as an effective IC identifier.

A second major advance to passive hardware metering presented in this work is use of IC segmentation, which results in a hardware metering approach that is inherently cheaper, faster, and more scalable than previous approaches. IC segmentation involves selecting only a small subset of gates for the purpose of physical level gate characterization, instead of all the gates of the IC. By freezing a subpart of the primary inputs and varying other parts, a large circuit can be segmented into small pieces. Even for the case of characterizing all the gates of an IC, segmentation provides an efficient and scalable technique for accomplishing this goal.

The low probability of coincidence obtained from our simulation results demonstrates that the number of gates used to carry out metering can be limited. With a small number of gates required for calculating the probability of coincidence, the remaining gates can be turned off during the metering process and smaller numbers of measurements need to be taken from the IC.

Segmentation also provides the flexibility to vary the level of precision of hardware metering. The size and number of the segments provides a parameter that can be varied to minimize the false negative rate of pirated ICs, depending on the cost or availability of IC measurements.

To summarize, our approach has four main advantages over the previous work. (1) Its functionality is maintained despite IC aging. (2) It is more cost-effective, as it minimizes the number of measurements that need to be carried out for characterization. Also, the use of segments provides the flexibility to tune the probability of false negatives, using measurement cost as a parameter. (3) It is substantially more scalable, as it uses segments of the IC for gate characterization. (4) The probability of coincidence between legitimate and pirated ICs is fully quantifiable, whereas the previous work was hampered by the correlation of manifestational gate characteristics.

To verify our hardware metering process, the probability of coincidence of a pirated IC with a legitimate IC is calculated. With simulations we are able to demonstrate that threshold voltage can be used as the gate property on which the IC identifier is based, as the probability of coincidence between ICs is highly unlikely. Additionally, the results show that process variation indeed allows threshold voltage to serve as a unique identifier for ICs. Further simulations are carried out in this work to ensure that the threshold voltage can be recovered with enough accuracy to differentiate legitimate ICs from pirated ones.

The key contributions of the paper are highlighted below.

- Successfully using persistent properties of gates for passive hardware metering;
- Using far fewer gates for identifier extraction, which results in a faster and more economical metering approach;
- Providing an algorithm for picking segments, efficiently and robustly;
- Explaining how the probability of coincidence of pirated ICs and legitimate ICs is quantitatively calculated;
- Demonstrating extremely low and favorable probabilities of coincidence between ICs, when using threshold for gate characterization.

2. RELATED WORK

Passive hardware metering generates unique IDs without having to modify the IC design. Instead, it characterizes the gate-level characteristics of an IC and uses them to uniquely identify the chip. This approach leverages the presence of process variation, which naturally exists in the IC manufacturing process and which makes all ICs unique and different from their nominal design properties. Koushanfar et al [1] propose a CAD-based passive hardware metering approach, which characterizes each gate of an IC in terms of its delay on the critical path and uses the delay value as a unique identifier for an IC. Alkabani et al [3] provide a nondestructive approach for gate-level characterization which analyzes the probability of collision of IDs in presence of intra- and inter-chip correlations. A hardware metering protocol is also introduced based on the proposed ID generation scheme. These passive metering approaches require a high degree of accuracy in the gate-level characterization results, and as we argue they are prone to malfunction, as gates exhibit changes to their manifestational properties over time.

Gate level characterization (GLC) under the impact of process variation has been assumed as a key step in many hardware security applications [10][13][14][15][16][18][20]. The basic approaches which have been proposed [3][11][19] characterize the manifestational properties of each gate by measuring the overall properties of the entire IC. Then, a system of linear equations is obtained from multiple measurements, based on the relationship between the physical and manifestational properties of each gate. A linear programming approach can be used to solve the system of equations and to obtain the characterization results. We leverage manifestational GLC for our robust hardware metering approach.

3. PRELIMINARIES

3.1 Process Variation Model

Process variation is due to the intense industrial CMOS feature scaling. With the scaling of feature sizes, the physical limits of the devices are reached and uncertainty in the device size increases [5]. Variations in transistor feature

sizes and thus, in gate characteristics, e.g., delay or power, are inevitable. In present and pending technologies, the variation is large compared to the device dimensions. As a result, VLSI circuits exhibit a high degree of variability in both delay and power consumption. Process variation is the major underpinning of all passive hardware metering approaches, as it introduces a distinction between ICs of the same design.

3.2 Measurement Model

To carry out passive hardware metering using gate level characterization, a limited number of nondestructive or side-channel measurements are taken. After fabrication it is possible to provide input vectors to the input pins of the manufactured chip and obtain the respective outputs from the output pins. Additionally, it is possible to measure the IC's leakage and switching power consumption [21].

We assume a zero measurement error in our simulations, as modern $3000 powering instruments have accuracy close to 0. In the specific case of Power SMU device, the measurement error is reported to be on the order of 10^{-5} [12], and thus highly accurate power measurements can be made. It should be noted that the approach used for threshold voltage extraction is robust enough to handle higher amounts of measurement error.

3.3 Aging Model

We use the aging model proposed in paper [2] for our threshold voltage (V_{th}) recovery scheme. The time dependence of V_{th} shift due to negative bias temperature instability (NBTI) follows the fractional power law, as shown in the following equation:

$$\Delta V_{th} = A \exp(\beta V_G) \exp(-E_\alpha / kT)\, t^{0.25} \qquad \text{(Eq.1)}$$

where V_G is the applied gate voltage; A and β are constants; E_α is the measured activation energy of the NBTI process; T is the temperature; and t is the current time.

4. APPROACH TO ROBUST HARDWARE METERING

In subsection 4.1 and section 4.2, we provide an overview of our new passive hardware metering approach. The specifics of each phase of the approach are detailed in the remaining subsections, including how to carry out IC segmentation, physical level GLC, original threshold voltage recovery, and probability of coincidence calculation.

4.1 New Hardware Metering Approach

Figure 1 gives an overview of the overall procedure for carrying out robust hardware metering using physical and persistent characteristics of gates. Manifestational characteristics are used to derive threshold voltage values, as well as effective channel length (L). Then through threshold voltage (V_{th}) recovery, the original threshold voltage is determined. The original threshold voltage values for an IC are individually or aggregately compared to the known threshold voltage values for legitimate ICs. If there is a match, the hardware is deemed to be legitimate, otherwise the IC is deemed to a pirated and an unauthorized IC.

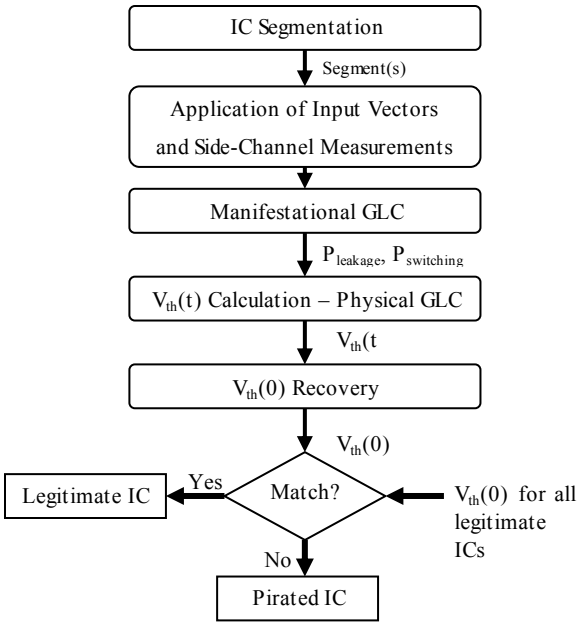

Figure 1. Provides an overview of the proposed hardware metering technique, for the differentiation of legitimate and pirated ICs.

Algorithm 1 **– Robust Hardware Metering**

Input: IC and IC segment netlist
Output: $V_{th}(t_0)$ for all selected gates
1: **For** all or selected segments in IC
2: **For**(all pairs of applied input vectors)
3: Obtain IC leakage and power measurements
4: Solve LP to determine gate level leakage and power
5: **End For**
6: **For**(all gates in a segment)
7: Solve NLP to determine gate-level $V_{th}(t_i)$
8: $V_{th}(t_0) = V_{th}\_Recovery(V_{th}(t_1), V_{th}(t_2), \ldots V_{th}(t_n))$
9: **End For**
10: **End For**

The procedure for the robust hardware metering approach is summarized in the pseudocode given in Algorithm 1. It carries out two types of gate level characterization. First, known manifestational GLC [3][11] is carried out. Side-hannel measurements of leakage power and switching power are made, which are then evaluated using linear programming to derive individual gate level values of leakage power and switching power. These values are then used for physical level GLC, to determine the current threshold voltage of the gates. Two or more measurements separated by gate aging are required to derive at least two different threshold voltage values per gate. The original threshold voltage of the gate, before any aging or switching

took place, can then be determined using a threshold voltage recovery scheme, presented below.

As the threshold voltage (and/or effective channel length) values for all legitimate ICs are recorded after manufacturing, the derived persistent gate characteristics can be used to verify and meter ICs.

4.2 Example

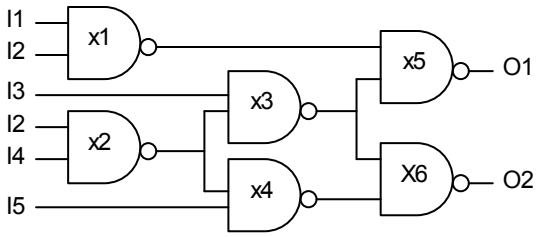

Figure 2. c17 example from ISCAS 85 benchmark used as an example to demonstrate the three main phases of our new hardware metering approach.

Consider the simple benchmark c17 from the ISCAS 85 suite, given in Figure 2, for the purpose of demonstrating three main phases in our new metering approach. Figure 3 provides the derived values for each gate of the example, from each phase.

First, at two different time instances, labeled t=1 and t=2, side-channel measurements are by applying vectors pairs to the IC. Using manifestational GLC the normalized leakage and switching power of each gate is derived. Then in the second phase, using the recovered values for switching and leakage power, physical level GLC is carried out. With physical level GLC, threshold voltages at t=1 and t=2 are recovered. From these two data values, the original threshold voltage can be recovered using original threshold voltage recovery, given in phase 3. The example given in Figure 3 demonstrates that some characterization error is possible, however as our simulation results show these errors tend to be very small and hence do not affect the metering scheme effectiveness.

4.3 Segmentation

One of the major difficulties in physical GLC-based hardware metering is that there are large numbers of gates in the pertinent ICs, which require a long running time for characterization. With our approach, since we use the combination of gate IDs (threshold voltage) for hardware metering, a small number of gates would suffice to distinguish different ICs. Therefore, we develop a segmentation based approach to select only a small subset of gates for the purpose physical level characterization and hardware metering. We define a segment *S* in a circuit as a group of gates that are the transitive fan-out of a certain set of inputs *I*. Therefore, by varying the input vectors for *I* and freezing any other inputs, we are able to change the input/output signals of the gates in S while freezing the other gates in the circuit. In this way, we can narrow down the gates for manifestational and physical GLC to only the gates in a few segments.

Gate	t=1		t=2	
	Normalized Leakage Power	Normalized Switching Power	Normalized Leakage Power	Normalized Switching Power
1	16.10	3.85	16.10	3.85
2	14.91	3.80	14.91	3.80
3	13.28	3.80	13.28	3.80
4	20.97	3.90	20.97	3.90
5	13.08	3.85	13.08	3.85
6	24.59	4.03	24.59	4.03

(a) Manifestational GLC

Gate	t=1	t=2
	Characterized $V_{th}(1)$ (Normalized)	Characterized $V_{th}(2)$ (Normalized)
1	0.56	0.61
2	0.56	0.61
3	0.59	0.65
4	0.51	0.56
5	0.49	0.54
6	0.51	0.56

(b) Physical Level GLC

Gate	Recovered $V_{th}(0)$ (Normalized)	Actual $V_{th}(0)$ (Normalized)
1	0.39	0.39
2	0.39	0.39
3	0.43	0.43
4	0.34	0.34
5	0.32	0.32
6	0.34	0.34

(c) Original Threshold Voltage Recovery

Figure 3. Data values for the simple example benchmark c17, given in Figure 2, for all three phases of the new hardware metering approach, namely (a) manifestational GLC, (b) physical level GLC, and (c) original threshold voltage recovery.

Consider the segmentation example in Figure 4. We first partition the circuit into two segments. We obtain Segment 1 (gates X1, X2, and X5) by freezing inputs 3 and 4 and applying different input vectors to inputs 1 and 2. Similarly, we obtain Segment 2 (gates X3, X4, and X5) by freezing inputs 1 and 2.

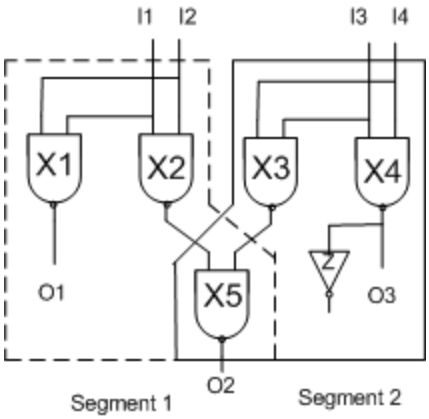

Figure 4. Simple IC segmentation example. Where segment 1 is represented with a dotted line and segment 2 is represented with a solid line.

Our goal in selecting the segments is to lower the cost of physical GLC while maintaining GLC accuracy. Since the major cost in GLC is the power measurement, we aim to select those gates that require a small number of equations in GLC. In other words, the selected inputs must have good controllability over the gates in the segments. We quantify controllability using a ratio of the number of inputs and the number of gates, or the controllability ratio (CR). Furthermore, our observation is that the running time of GLC explodes with the number of gates being characterized; therefore, we tend to select small segments for GLC. With these underlying motivations for our approach, we develop a segment selection algorithm as shown in Algorithm 2.

We first identify the unit segment $S(I_i)$ which is controlled by each single input I_i. Next, we keep inserting $S(I_i)$ into the selected segment set (*Seg*) in such a way that the increased number of gates in *Seg* is minimal in each step. This ensures that the number of overlapping gates between the selected segments is minimized, and the CR is maximized. The algorithm terminates when the total number of selected gates in *Seg* reaches *s*, which is a constant we define to indicate the number of needed gates for hardware metering.

Algorithm *2*– **Segment Selection for Hardware Metering**
Input: netlist of the target IC Output: selected segments set *Seg* for hardware metering 1: **For** each input I_i in IC 2: $S(I_i) = S_i$, where S_i is transitive fanout gate set of I_i 3: **End For** 4: **While** (size (*Seg*) < s) 5: Insert $S(I_k)$ into *Seg*, where size(S_k U *Seg*) < size(S_t U Seg), for any t!=k 6: **End While** 7: **Return** *Seg*

4.4 Physical GLC for Hardware Metering

To carry out threshold voltage characterization, leakage power and switching power measurements are made. Then the equations for gate-level leakage power, Equation (2), and switching power, Equation (3), [24] are used to solve for the current threshold voltage.

$$I_{leakage} = 2 \cdot n \cdot \mu \cdot C_{ox} \cdot \frac{W}{L} \cdot \phi_t^{\,2} \cdot e^{\frac{\sigma \cdot V_{dd} - V_{th}}{n \cdot \phi_t}} \quad \text{(Eq.2)}$$

$$P_{switching} = \alpha \cdot C_L \cdot W \cdot L \cdot V_{dd}^2 \quad \text{(Eq.3)}$$

where α is the switching probability, n is the subthreshold slope, μ is the mobility, C_{ox} is the oxide capacitance, C_L is the load capacitance, W is the gate width, L is the effective channel length, φ_t is the thermal voltage, σ is the drain induced barrier lowering (DIBL) factor, V_{dd} is the supply voltage, and V_{th} is the threshold voltage.

There are two variables in the gate-level leakage power and switching power formulas that are subject to process variation: threshold voltage (V_{th}) and effective channel length (L). We first conduct manifestation-level GLC to characterize gate-level leakage power and switching power. Then, we formulate two non-linear equations according to Equation (2) and (3). By solving these two equations for each gate, we can characterize the gate-level physical properties, threshold voltage and effective channel length.

4.5 Threshold Voltage as IC ID

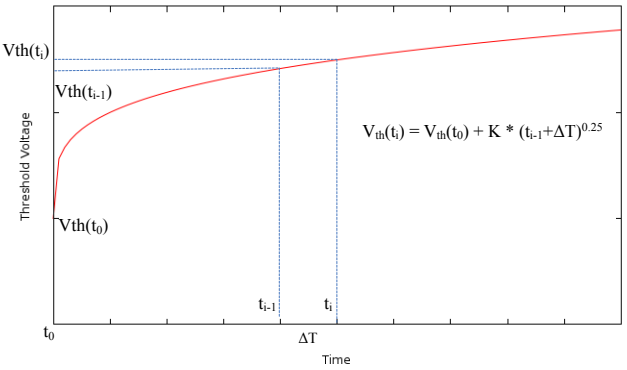

Figure 5 Threshold voltage recovery using Gauss-Newton method for solving the system of nonlinear equations.

We are able to recover the threshold voltage of gate, even after aging. Following the aging model, given in Equation (1) [2], we solve for the original threshold voltage, $V_{th}(t_0)$. To accomplish original threshold voltage recovery, we start our metering from time t_1 when the threshold voltage of the gate is $V_{th}(t_1)$. We age the gate for time ΔT and measure the increased threshold voltage as $V_{th}(t_2)$. By repeating this process, we can formulate a system of non-linear equations of the following type, where m is the number of threshold voltage measurements:

$$V_{th}(t_1) = V_{th}(t_0) + K * t_1^{\,0.25} \quad \text{(Eq.4)}$$

$$V_{th}(t_i) = V_{th}(t_0) + K * (t_{i-1}+\Delta T)^{0.25},\ 1<i<=m \quad \text{(Eq.5)}$$

By solving these non-linear equations, we can obtain $V_{th}(t_0)$,

the original threshold voltage that we use as the ID. As shown in Figure 5, we solve the system of non-linear equations using the Gauss-Newton method.

4.6 Probability of Coincidence Calculation

To quantify the feasibility of the passive hardware metering approach, we evaluate the likelihood that a pirated IC will be falsely classified as a legitimate ID. Reciprovally, we must consider the likelihood that a legitimate IC will be classified as pirated. To quantify the probability of coincidence between legitimate and pirated ICs, we can take advantage of the fact that threshold voltage follows an independent Gaussian distribution. This enables an upper bound on the probability of coincidence to be obtained.

With a Bayesian-based probability analysis [22] to calculate the probability of coincidence, we can first calculate the false positive case, where a pirated IC is classified as legitimate. We have the following equation representing the probability that a gate's threshold voltage matches a gate's threshold voltage in another IC for a certain set of measurements.

$$P(H \mid D) = \frac{P(D \mid H) - P(H)}{P(D)} \qquad \text{(Eq. 6)}$$

where H is the event that a gate matches at least one other gate's threshold voltage measurement; D is the event that we have a certain set of threshold voltage measurements for the N sampled chips; P(D|H) is the probability of having the certain set of measurements under the condition that a gate matches with some other gates.

Using the well-known approach in the birthday paradox problem [23], we can calculate P(H).

$$P(H) = 1 - \prod_{1}^{N} (1 - P_i) \qquad \text{(Eq. 7)}$$

where P_i is the probability that a certain gate, i, matches another gate, j.

Assuming that P(D|H)/P(D) does not vary with the variation in D, we have the following estimate for P(H|D).

$$P(H \mid D) \propto 1 - \prod_{1}^{N} (1 - P_i) \qquad \text{(Eq. 8)}$$

In our coincidence calculation, the value of P_i is approximated as the highest possible P_i, for all the P_i's, and in this way, we overestimate the probability of coincidence and obtain an upper bound value for worst case analysis.

To determine whether two ICs match, the accuracy and hence the measurement cost of the coincidence calculation can be varied according the threshold of overlap required when comparing probability distributions from the two ICs.

5. SIMULATION RESULTS

5.1 Simulation Set-up

Simulations were performed on the ISCAS 85 and ISCAS 89 benchmark circuits. Matlab 7.1's fsolve function served as the non-linear solver used for physical GLC. For manifestation-level (switching power or leakage power) characterization, we used 1024 measurements per segment. For large test cases, segmentation was used [6][7]. For V_{th} characterization, we utilized the results from leakage power and switching power characterization. For V_{th} recovery, we used two measurements of V_{th}, $V_{th}(t_1)$ and $V_{th}(t_2)$, before and after our aging operation, respectively.

5.2 Enhancements to Manifestational Gate-Level Characterization

Table 1 presents our results from manifestational GLC for select benchmarks. It demonstrates the accuracy with which gate-level characterization using IC segmentation is carried out, even for benchmarks with over 19,000 gates.

Segmentation has previously been showed to improve gate-level characterization techniques, by allowing much larger numbers of gates to be characterized in shorter period of time. As with our hardware metering technique, we do not need to characterize the entire IC, but just enough gates to meet a threshold set for an acceptable probability of coincidence. Thus segmentation approaches can be appropriately applied to this realm.

Table 1. Demonstrates the accuracy with which gates can be characterized, for benchmarks with up to 19,000 gates.

Benchmark	# of Gates	Characterized Gates	GLC Accuracy (%)
C499	202	162	0. 18
C880	383	369	1.01
C1355	546	500	0. 91
C1908	880	355	0. 086
C2670	1193	598	0. 13
C3540	1669	878	0.29
C5315	2307	1334	0.073
S38584	19253	12861	0.36

5.3 Physical GLC and Original Threshold Voltage Recovery

The physical GLC approach is based on leakage power, and switching power values being used to solve non-linear equations for each gate. With the procedure both threshold voltage (V_{th}) and effective channel length (L) can be calculated. In the simulations, we generated the IC instances using the quad-tree model [8] for effective channel length and the Gaussian model [9] for threshold

voltage. The simulation results are shown in Table 2. The error rate for V_{th} recovery is less than 1.3% even for the largest of benchmarks attempted, with over 19,000 gates. Effective channel length is even more accurate with the worst results being better than .06% error.

We went on to carry out threshold voltage recovery, using the results of physical GLC. The results are given in Table 3, and even in the largest circuits of around 19,000 gates, the error in V_{th} recovery is less than 1.7% in the worst case.

Table 2. Simulation results for threshold voltage and effective channel length recovery during physical level GLC, for a series of benchmarks.

Benchmark	# of Gates	V_{th} Accuracy (%)	L Accuracy (%)
C499	202	0. 36	0. 019
C880	383	0. 58	0. 026
C1355	546	0. 48	0. 023
C1908	880	0. 46	0. 024
C2670	1193	0. 51	0. 024
C3540	1669	0. 59	0. 026
C5315	2307	0. 65	0. 028
S38584	19253	1.22	0. 053

Table 3. Recovery accuracy results from threshold voltage recovery for benchmarks from the ISCAS 85 and ISCAS 89.

Benchmark	# of Gates	V_{th} Accuracy (%)
C499	202	1.30
C880	383	1.22
C1355	546	1.52
C1908	880	1.47
C2670	1193	1.28
C3540	1669	1.44
C5315	2307	1.36
S38584	19253	1.62

5.4 Probability of Coincidence

As shown in the simulation results in Table 4 and Table 5, we find an extremely low probability of coincidence among ICs, when characterizing all gates or even a single small segment of the IC, respectively. The likelihood of coincidence decreases dramatically in larger ICs, as the number of original threshold values increases.

From the results in Table 4 and Table 5 we can conclude that the worst case probability of coincidence is small enough to hold huge population of chips (i.e. in the millions), and the false positive and false negative are close to 0. This conclusion enables us to assume that all the chips are distinguishable from each other and we can label them uniquely without overlaps.

Table 4. Demonstrates the low probability of coincidence when using threshold voltage for hardware metering.

Benchmark	# of Gates	Prob. of Coincidence Using V_{th}
C499	202	6.67E-80
C880	383	1.63E-218
C1355	546	3.19E-349
C1908	880	3.85E-546
C2670	1193	2.56E-809
C3540	1669	6.08E-1132
C5315	2307	9.31E-1518
S38584	19253	3.03E-11264

Table 5. Demonstrates the low probability of coincidence between ICs is still maintained when a single small segment is used hardware metering using threshold voltage.

Benchmark	# of Gates	# Gates in Selected Segments	Prob. of Coincidence Using Segments
C499	202	22	5.68E-14
C880	383	40	8.27E-25
C1355	546	43	1.29E-26
C1908	880	21	2.27E-13
C2670	1193	27	5.55E-17
C3540	1669	47	5.04E-29
C5315	2307	26	2.22E-16
S38584	19253	18	1.46E-11

6. EXTENSION TO USAGE METERING

Usage metering is similar to hardware metering, with the exception that legitimate ICs can become illegitimate after some amount of usage and gate activity. With usage metering, an IC's functionality can be halted or payment can be demanded, after some number of IC uses. We demonstrate how our use of physical level gate characterization provides a solution to the related problem of usage metering, as well are hardware metering.

In the process of extracting the original threshold voltage from the current threshold voltage values, the activity of the gate can also be determined. However, aging can be accelerated under increased temperature during switching activity. To determine IC usage, the buffer gates of the clock tree are used for characterization as they have the same switching activity by definition. To determine the baseline activity without the contributory effects of

temperature, we chose a region of the clock tree with the smallest amount of aging, implying that it was the least effected by temperature increases. Then we extract the original threshold voltage values for that gate. Using the aging model [2], we can derive the amount of switching activity that the gate underwent, thus providing its usage history.

7. CONCLUSION

With this work we have highlighted existing weaknesses with current passive hardware metering techniques, namely the fact that IC aging will prevent proper manifestational GLC. Instead, we have presented a robust hardware metering scheme that leverages persistent properties of gates for gate-level characterization. The simulation results with benchmarks as small as 200 and up to 19,000 gates demonstrate the effectiveness of the proposed approach.

8. ACKNOWLEDGEMENTS

This work was supported in part by the NSF under Award CNS-0958369, Award CNS-1059435, and Award CCF-0926127.

9. REFERENCES

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

[2] S. Chakravarthi, et al. A Comprehensive Framework for Predictive Modeling of Negative Bias Temperature Instability. IEEE International Reliability Physics Symposium April 2004, pp. 273- 282.

[3] Y. Alkabani, et al. Trusted Integrated Circuits: A Nondestructive Hidden Characteristics Extraction Approach. Information Hiding 2008, pp. 102-117.

[4] A. Caldwell, et al. Effective Iterative Techniques for Fingerprinting Design IP. IEEE Transactions on CAD, Vol. 23, No. 2, 2004. pp. 208-215.

[5] S. Borkar, T. Karnik, S. Narendra, J. Tschanz, A. Keshavarzi, V. De. Parameter Variations and Impact on Circuits and Microarchitecture. DAC 2003, pp. 338-342.

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

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

[8] B. Cline, et al. Analysis and Modeling of CD Variation for Statistical Static Timing. ICCAD 2006, pp. 60-66.

[9] A. Asenov. Random Dopant Induced Threshold Voltage Lowering and Fluctuations in Sub-0.1 um MOSFET's: A 3-D Atomistic Simulation Study. IEEE Transactions on Electron Devices, Vol. 45, No. 12, 1998, pp. 2505-2513.

[10] M. Potkonjak, A. Nahapetian, M. Nelson, T. Massey. Hardware Trojan horse detection using gate-level characterization. DAC 2009, pp. 688-693.

[11] A. Srivastava et al. Statistical Analysis and Optimization for VLSI: Timing and Power. Springer, 2005.

[12] NI PXI-4130 Power SMU: http://sine.ni.com/nips/cds/view/p/lang/en/nid/204239.

[13] M. Nelson, A. Nahapetian, F. Koushanfar, M. Potkonjak,. SVD-Based Ghost Circuitry Detection. IH 2009, pp. 229-237.

[14] S. Wei, S. Meguerdichian, M. Potkonjak, Gate-Level Characterization: Foundations and Hardware Security Applications, DAC 2010, pp. 222-227.

[15] S. Wei, M. Potkonjak, Integrated Circuit Security Techniques Using Variable Supply Voltage, DAC 2011, pp. 248-253.

[16] S. Wei, S. Meguerdichian, M. Potkonjak, Malicious Circuitry Detection Using Thermal Conditioning, IEEE Transactions on Information Forensics and Security (TIFS), 2011.

[17] G. Qu, M. Potkonjak, Intellectual Property Protection in VLSI Design Theory and Practice, Kluwer Publishing, 2003.

[18] M. Potkonjak, S. Meguerdichian, A. Nahapetian, S. Wei. Differential Public Physically Unclonable Functions: Architecture and Applications. DAC 2011.

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

[20] F. Dabiri, M. Potkonjak, Hardware aging-based software metering, DATE 2009, pp. 460-465.

[21] A. G. Bayrak, F. Regazzoni, P. Brisk, F-X. Standaert, and P. Ienne, A First Step Towards Automatic Application of Power Analysis Countermeasures. DAC 2011.

[22] M. Mitzenmacher, E. Upfal. Probability and Computing: Randomized Algorithms and Probabilistic Analysis. Cambridge, 2005.

[23] P. Flajolet, D. Gardy, L. Thimonier. Birthday Paradox, Coupon Collectors, Caching Algorithms and Self-organizing search. Discrete Applied Mathematics, Vol. 39, No. 3, 1992. pp. 207-229.

[24] D. Markovic, et al, Ultralow-Power Design in Near-Threshold Region, Proceedings of the IEEE, Vol. 98, No.2, 2010. pp. 237-252.