Quantitative Intellectual Property Protection Using Physical-Level Characterization

Sheng Wei, *Student Member, IEEE*, Ani Nahapetian, *Member, IEEE*, and Miodrag Potkonjak, *Member, IEEE*

***Abstract*—Hardware metering, the extraction of unique and persistent identifiers (IDs), is a crucial process for numerous integrated circuit (IC) intellectual property protection tasks. The currently known hardware metering approaches, however, are subject to alternations due to device aging, since they employ unstable manifestational IC properties. We, on the other hand, have developed the first robust hardware metering approach by using physical-level gate proprieties for ID generation. By using effective channel length, which is resilient to aging, and threshold voltage, which is essentially independent across gates and suitable for calculating the uniqueness of the IDs, we overcome the limitations of the existing approaches. Also, despite the increase in threshold voltage that occurs with aging, the original threshold voltage value can be extracted through intentional IC aging. Our ID generation procedure first employs two types of side channels, namely switching power and leakage power, to extract metering results for each gate. Next, we show that localized delay measurements alone are sufficient for accurate characterization of large sets of gates. Finally, by using threshold voltage for ID creation, we are able to obtain low probabilities of coincidence between legitimate and pirated ICs. The application of the approach to a set of benchmarks quantitatively establishes the effectiveness of the new hardware metering approach.**

***Index Terms*— Intellectual property protection, hardware metering, gate-level characterization.**

I. Introduction

WITH the rapid growth of integrated circuit (IC) outsourcing, hardware metering has become an important procedure in identifying any unauthorized IC manufacturing carried out by untrusted foundries [2], [13]–[15]. Hardware metering [1], [16] 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) [5], [18]. In passive metering schemes [4], [16], the inherent uniqueness of the ICs, which is a result of intrinsic process variation, is leveraged to determine the IDs, without modifying the IC design or manufacturing process.

Current passive hardware metering techniques [4], [16] extract IC IDs using manifestational properties, such as leakage power, switching power, and delay of gates. There are two significant drawbacks to the current state-of-the-art passive metering approaches. First, manifestational properties have been shown to vary and age nonuniformly under the combination of gate switching and variations in temperature and supply voltage [3]. IDs extracted after a gate has aged will be different from previously calculated and stored IDs, and thus IDs from legitimate ICs may be deemed invalid, undermining the entire approach. As a result, we argue that previous hardware metering techniques will malfunction as aging modifies the manifestational characteristics of gates. Second, previously proposed approaches are cost prohibitive, due to their requirement for characterizing 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 [12], thus making the approach costly and difficult to scale to large designs.

We overcome these two challenges using two main advances. First, we employ two orthogonal sets of manifestational properties, namely power and delay, to uniquely identify the ICs and address the robustness issue caused by aging. In particular, we characterize the gate-level physical properties, such as the original threshold voltage, and use them as the IC IDs instead of the delay and power that were considered in the previous approaches. Even though threshold voltage will degrade with aging, we provide a procedure for extracting the original threshold voltage of a gate from two or more nonoriginal 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 of the passive hardware metering presented in this work is the cost reduction of the metering approach and the way it addresses the issue of scalability. We note that the major cost associated with the hardware metering process, which affects the scalability of the approach to large industrial-scale designs, is the number of power or delay measurements. In order to solve for gate-level properties, a large number of measurements is required comparable to the number of gates (variables) in the system of linear equations. This is considered infeasible for a design with millions of gates, especially when the measurements have to be conducted for each single

Manuscript received January 27, 2013; revised May 25, 2013; accepted July 22, 2013. Date of publication August 15, 2013; date of current version September 26, 2013. This work was supported in part by the NSF under Awards CNS-0958369 and CNS-1059435. An earlier version of this paper was presented at the 2011 IEEE/ACM International Conference on Computer-Aided Design (ICCAD 2011). The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Jiangtao Li.

S. Wei and M. Potkonjak are with the Computer Science Department, University of California, Los Angeles (UCLA), Los Angeles, CA 90095 USA (e-mail: shengwei@cs.ucla.edu; miodrag@cs.ucla.edu).

A. Nahapetian is with the Computer Science Department, California State University, Northridge (CSUN), Northridge, CA 91330 USA, and also with the Computer Science Department, University of California, Los Angeles (UCLA), Los Angeles, CA 90095 USA (e-mail: ani@cs.ucla.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2013.2277976

1556-6013 © 2013 IEEE

chip in the postsilicon stage considering the impact of process variation [6].

We have two approaches to reduce the measurement cost and address the scalability issue. Firstly, for the power characterization, we use IC segmentation [44], [45], which partitions the circuit into small independent regions and 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, instead of all the gates of the IC, for the purpose of physical gate-level characterization. By freezing a subpart of the primary inputs and varying the 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 the goal. Secondly, we employ timing (delay) of the IC as an alternative source for side channel measurements. The key observation is that each delay measurement only relates to a small number of gates that are on the delay path, which significantly reduces the size of the problem.

The low probability of coincidence obtained from our simulation results demonstrates that the number of gates used to carry out metering can be reduced. With only a small number of gates required for ID generation, all remaining gates can be turned off during the metering process, and thus a smaller number of measurements of the IC is required. Also, segmentation provides the flexibility to vary the level of precision of hardware metering procedure. The size and number of the segments act as parameters to be varied to minimize the false negative rate of identifying pirated ICs, depending on the cost or availability of the IC measurements.

We are able to demonstrate that threshold voltage can serve as an effective basis for ID generation, by showing that the probability of coincidence that two different ICs have identical IDs is extremely low. Additionally, the results show that process variation indeed allows threshold voltage to serve as a unique identifier for ICs. To summarize, the key contributions of the paper are the following.

- Successful use of persistent gate properties for passive hardware metering;
- Use of far fewer gates for identifier extraction, which results in a faster and more economical metering approach;
- Employment of delay as an alternative source of side channel measurements, helping to address the issue with scaling to larger designs; and
- Demonstration of extremely low and favorable probabilities of coincidence between ICs, when using threshold voltage for ID generation.

II. Related Work

In this section, we summarize the related work in hardware metering and gate-level characterization, with an emphasis on the novelty of our proposed approach.

A. PUF-Based Active Hardware Metering

Physically unclonable functions (PUFs) is a multi-input multi-output device whose input-output mapping is difficult to predict and reverse engineer and thus impossible to clone. Recently, PUF-based approach has been adopted as an active means of identifying the IC and conducting hardware metering [29]–[40]. For example, Maes *et al.* [21] proposed a secure device activation protocol based on PUFs; Alkabani *et al.*, [22] proposed a novel PUF-based active metering approach based on the manipulation of the original finite state machine; and Koeberl *et al.*, [23] evaluated several PUF-based approaches, including memory-based [24]–[27] and delay-based PUFs [28]. The major difference between PUF-based approach and our approach is that the former is active IC metering, which requires additional hardware (i.e., PUFs) to be embedded in the IC. However, our approach does not introduce hardware instrumentations or area overhead and, more importantly, it applies to legacy ICs that have already been manufactured. It is important to note that, with the trend of transistor scaling, the legacy ICs often contain a large number of gates and thus IC segments that can serve as the candidates of IC metering.

B. Passive Hardware Metering

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 [6], which naturally exists in the IC manufacturing process and which makes all ICs unique and different from their nominal design properties. Koushanfar *et al.* [16] 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.* [4] 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. Related hardware metering techniques can also be found in [46]. These passive metering approaches require a high degree of accuracy in the gate-level characterization results, and as we argue, are prone to malfunction, as gates exhibit changes to their manifestational properties over time.

C. Gate-Level Characterization

Gate-level characterization (GLC) has been adopted as a postsilicon step in quantifying the process variations, which has been employed by several hardware security applications [9], [11], [12]. The existing approaches [4], [10], [12], [16] characterize the manifestational properties of each gate by measuring the overall properties of the entire IC. Then, a system of linear equations can be obtained from multiple measurements. Finally, a linear programming approach can be employed to solve the system of equations and to obtain the characterization results.

III. Preliminaries

In this section, we introduce the system and analytical models that we employ in the discussion of our hardware metering approach, including process variation model, delay model, and device aging model.

A. Process Variation Model

Process variation is the major underpinning of all passive hardware metering approaches, as it introduces a distinction between ICs of the same design. It is due to the intense feature scaling of industrial CMOS. With the scaling of feature sizes, the physical limits of the devices are reached and uncertainties in the device sizes are increased [6]. Variations in transistor feature sizes and thus, in gate characteristics such as delay and power, are inevitable. In present and pending technologies, the variation is relatively large compared to the device dimensions. As a result, VLSI circuits exhibit a high degree of variability in both delay and power consumption.

In the discussion of this paper, we refer to the process variation models introduced by Asenov *et al.*, [8] and Cline *et al.*, [7], where threshold voltage and effective channel length are considered as the two major sources of process variation. In addition, we note that load capacitance (C_L) and oxide capacitance (C_{ox}) are also subject to process variation. According to Boning *et al.* [41] and Markovic *et al.* [17], the variation of load capacitance is proportional to the variation of the channel length (L). Therefore, we evaluate the impact of process variation in C_L together with L. As for C_{ox}, according to Iniewski *et al.* [42], the variation of C_{ox} is negligible compared to that of V_{th}.

B. Delay Model

The delay of a single logic gate can be expressed as

$$d = gh + p \tag{1}$$

where g and h are logical effort and electrical effort, respectively; and p is parasitic delay. In particular, we use the delay model in [17] that connects the gate delay to its sizing and operating voltages:

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

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 fitting parameters.

C. Aging Model

We use the aging model proposed in paper [3] 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:

$$\Delta V_{th} = A\cdot e^{\beta V_G}\cdot e^{-E_\alpha/kT}\cdot t^{0.25} \tag{3}$$

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.

We age a logic gate by applying input vectors that stress the transistors that consist of the gates. Due to the NBTI effects, the transistors that are under stress will be aged following the aging model shown in (3). Also, a higher operating temperature and stress voltage will further accelerate the V_{th} shift. For example, Schroder *et al.* [43] reported that the threshold voltage can be increased by 10 mV under approximately 10^4 sec stress time, with $V_G = -2.3$ V and $T = 100°$C. As prior work, researchers from our group have conducted aging on Xilinx FPGAs. The method to age a specific LUT on a specific slice is to instantiate the LUT in HDL with a constant value to its inputs (i.e., the aging input vector that stresses the PMOS transistors), and apply location constraint in the synthesis tool to map it to a specific cell.

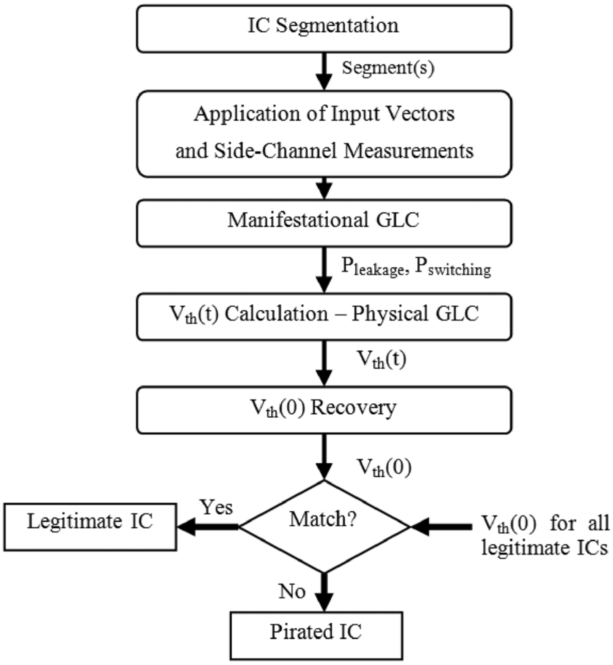
IC Segmentation
Segment(s)
Application of Input Vectors and Side-Channel Measurements
Manifestational GLC
$P_{leakage}$, $P_{switching}$
$V_{th}(t)$ Calculation – Physical GLC
$V_{th}(t)$
$V_{th}(0)$ Recovery
$V_{th}(0)$
Match?
Yes
Legitimate IC
No
Pirated IC
$V_{th}(0)$ for all legitimate ICs

Fig. 1. Overall procedure of the proposed hardware metering approach, for the differentiation of legitimate and pirated ICs.

IV. Approach to Robust Hardware Metering

In Sections IV-A and IV-B, 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, and original threshold voltage recovery.

A. Robust Hardware Metering Approach

Fig. 1 shows the overall procedure of our hardware metering approach using physical and persistent IC characteristics. Manifestational characteristics are used to derive threshold voltage (V_{th}) values, as well as effective channel length (L). Then, the original threshold voltage can be determined through a threshold voltage recovery scheme. Next, 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 be pirated or unauthorized.

We summarize the procedure of the robust hardware metering approach in Algorithm 1. First, we conduct manifestational GLC [4], [12], which derives the side channels (e.g., leakage

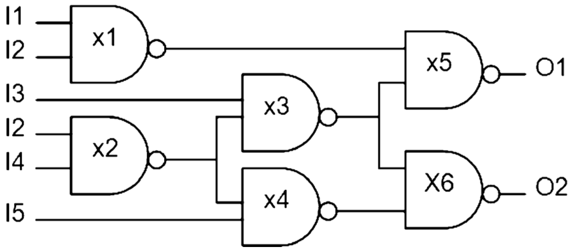

Fig. 2. c17 example from ISCAS benchmark used as an example to demonstrate the three main phases of our new hardware metering approach.

power and switching power) of individual gates from power measurements using linear programming (LP). Second, we use the manifestational GLC results to determine the current threshold voltage of the gates via nonlinear programming (NLP). Finally, we conduct two or more measurements separated by gate aging, which enables us to calculate the original threshold voltage before any aging effects take place. As the original 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 the ICs.

Algorithm 1 Robust Hardware Metering.

```
Input: Netlists of IC and IC segments;
Ouput: $V_{th}(t_0)$ for all selected gates;
for all or selected segments in the IC do
    for all pairs of applied input vectors do
        Measure IC leakage and switching power;
        Solve LP to determine gate-level leakage and switching power;
    end for
    for all gates in a segment do
        Solve NLP to determine gate-level $V_{th}(t_i)$;
        $V_{th}(t_0) = V_{th}\_recovery(V_{th}(t_1), V_{th}(t_2), \ldots, V_{th}(t_n))$;
    end for
end for
```

B. Example of Hardware Metering

We demonstrate the three main phases of our new hardware metering approach using an example of ISCAS benchmark c17, as shown in Fig. 2. First, at two different time instances, labeled $\mathrm{t} = 1$ and $\mathrm{t} = 2$, we conduct side-channel measurements while applying specific input vectors to the IC. We derive the normalized leakage and switching power of each gate using manifestational GLC [12], as shown in Table I(a). Then, in the second phase, we conduct physical level GLC using the characterized switching and leakage power values. The threshold voltages at $\mathrm{t} = 1$ and $\mathrm{t} = 2$ can be obtained from the physical level GLC results, as shown in Table I(b). Finally, in the third phase, we recover the original threshold voltage based on the threshold voltages at $\mathrm{t} = 1$ and $\mathrm{t} = 2$ following the aging model (i.e., (3)), as shown in Table I(c).

TABLE I
GLC AND RECOVERY RESULTS OF THE ISCAS BENCHMARK c17
(NORMALIZED VALUES)

(a) Manifestational GLC

Gate	t=1		t=2	
	Leakage Power	Switching Power	Leakage Power	Switching Power
1	16.10	3.85	12.36	3.85
2	14.91	3.80	11.51	3.80
3	13.28	3.80	10.22	3.80
4	20.97	3.90	16.08	3.90
5	13.08	3.85	10.40	3.85
6	24.59	4.03	18.65	4.03

(b) Physical GLC

Gate	t=1	t=2
	Characterized $V_{th}(1)$	Characterized $V_{th}(2)$
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

(c) Original Threshold Voltage Recovery

Gate	Recovered $V_{th}(0)$	Actual $V_{th}(0)$
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. IC 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 metering. With our approach, since we use the combination of gate IDs for hardware metering, a small number of gates would suffice to differentiate ICs from each other. Therefore, we develop a segmentation-based approach to select only a small subset of gates for the purpose of 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's of a certain set of inputs I. By varying the input vectors for I and freezing any other inputs, we are able to switch 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.

Fig. 3 shows an example of IC segmentation. 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 $X3$, $X4$, $X5$, and z) by freezing inputs 1 and 2 and varying inputs 3 and 4.

Our goal in selecting the segments is to reduce 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 measurements

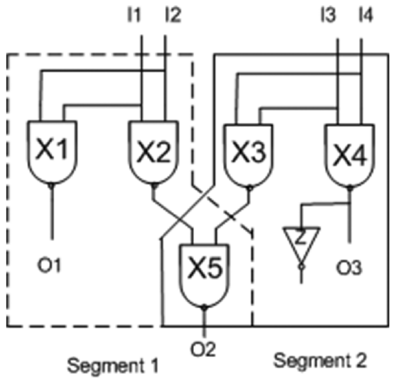

Fig. 3. Simple IC segmentation example, where segment 1 is represented with a dotted line and segment 2 is represented with a solid line.

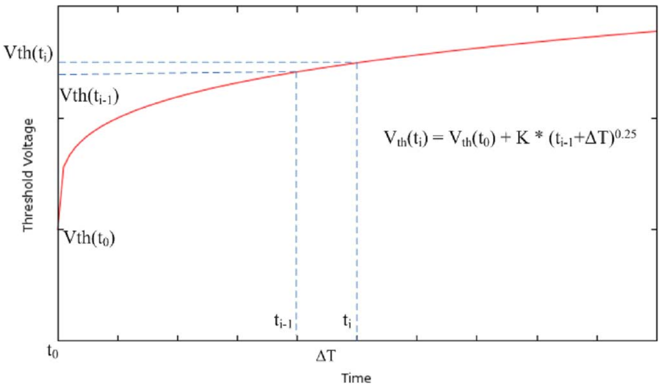

Fig. 4. Threshold voltage recovery using the Gauss-Newton method for solving the system of nonlinear equations.

(equations) for 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, based on our observation that the GLC running time dramatically grows with the addition of more gates for characterization, we select relatively small segments for GLC. These GLC characteristics motivate our segment selection algorithm shown in Algorithm 2.

Algorithm 2 Segment Selection for Hardware Metering.

```
Input: Netlists of the target IC;
Ouput: Selected segment set $Seg$ for hardware metering;
for each input $I_i$ in the target IC do
    $S(I_i) = S_i$, where $S_i$ is the transitive fanout gate set of $I_i$;
end for
while $size(Seg) < s$ do
    Insert $S_{I_k}$ into $Seg$, where $size(S_k \cup Seg) < size(S_t \cup Seg)$, for any $t \neq k$;
end while
Return $Seg$;
```

In segment selection, 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 number of additional 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 parameter we define to indicate the number of required gates for hardware metering.

D. Physical GLC for Hardware Metering

In Physical GLC, we conduct leakage and switching power measurements in order to characterize gate-level threshold voltage values. Then, we employ the equations for gate-level leakage power (i.e., (4)) and switching power (i.e., (5)) [17] to solve for the current threshold voltage.

$$P_{leakage} = 2 \cdot n \cdot \mu \cdot C_{ox} \cdot \frac{W}{L} \cdot \phi_t^2 \cdot V_{dd} \cdot e^{\frac{\sigma \cdot V_{dd} - V_{th}}{n \cdot \phi_t}} \quad (4)$$

$$P_{switching} = \alpha \cdot C_L \cdot W \cdot L \cdot V_{dd}^2 \quad (5)$$

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 nonlinear equations according to (4) and (5). By solving these two equations for each gate, we can characterize the gate-level physical properties, i.e., V_{th} and L.

E. Threshold Voltage Recovery

We are able to recover the original threshold voltage of gate, despite gate aging. Following the aging model, given in (3) [3], we solve for the original threshold voltage, $V_{th}(t_0)$. To accomplish the 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 nonlinear equations of the following type, where m is the number of threshold voltage measurements:

$$V_{th}(t_1) = V_{th}(t_0) + K * t_1^{0.25} \quad (6)$$

$$V_{th}(t_i) = V_{th}(t_0) + K * (t_{i-1} + \Delta T)^{0.25}, \quad 1 < i \leq m \quad (7)$$

By solving these nonlinear equations, we can obtain $V_{th}(t_0)$, the original threshold voltage that we use as the ID. As shown in Fig. 4, we solve the system of nonlinear equations using the Gauss-Newton method.

V. Hardware Metering Using Timing Characterization

In this section, we discuss the details of our timing-based hardware metering approach, which serves as an alternative to

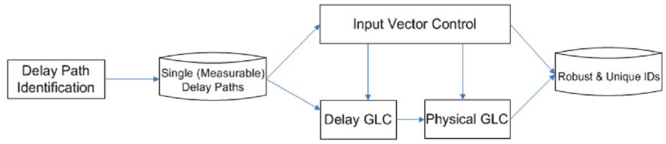

Fig. 5. Flow of hardware metering using timing characterization.

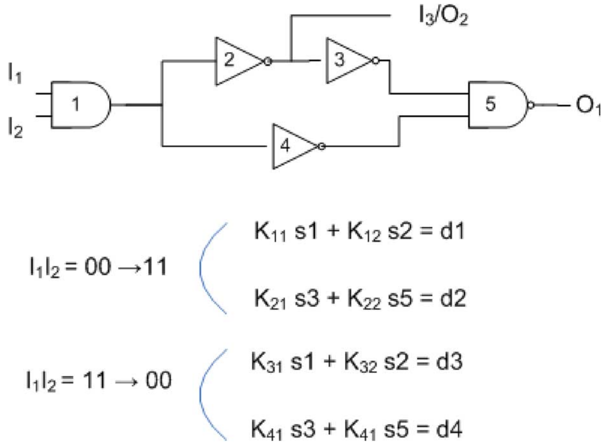

Fig. 6. Example of hardware metering using timing characterization.

the power-based approach and has the potential to reduce the metering costs.

A. Motivation

Power-based GLC can recover the physical properties of all the gates in an IC and leverage them for uniquely identifying each individual chip for the purpose of metering. Furthermore, since there are huge numbers of gates on each chip in modern IC technologies, the resulting IC IDs have extremely low probabilities of colliding with each other and yielding identical IDs for two different chips. However, the GLC approach can be made more efficient in practice, if the following issues are addressed:

- *Cost of measurements*. The cost of leakage power measurements is high when many measurements are made for each individual chip in the postsilicon stage.
- *Scalability*. With the power-based approach, all the gates are involved and contributing to the total leakage power. Consequently, the linear programs for manifestational GLC are huge, which present issues when scaling to millions of transistors.

In order to address these two challenges associated with the power-based GLC, we leverage circuit delay for identifying each chip. We argue that the delay-based detection methods are more scalable, as only a small subset of gates are considered on a measured delay path. Also, delay measurement techniques, such as delay fault based methods [20], have been well studied and require less cost and overhead when applied to large numbers of ICs postsilicon.

One of the traditional drawbacks of using delay-based methods is that it is difficult to characterize all the gates in the circuit. However, this is not an issue for the purposes of hardware metering, since not all gates are required in order to obtain a low probability of coincidence.

B. Flow for Delay-Based ID Generation

Fig. 5 shows the flow of using delay as the side channel in the hardware metering process. In order to reduce the number of delay measurements and to avoid additional hardware instrumentation, we first identify the delay paths in the circuit that are easy to measure and characterize. For example, we take into account of the following factors to evaluate the difficulty of conducting the delay measurements: (1) whether the source and destination of the path are observable for delay fault-based measurements using existing inputs, outputs, or flip-flops in the circuit; (2) whether there are any other paths in parallel with the measured path that cannot be distinguished; and (3) whether the number of gates on the measured delay path is small enough to be handled by an linear programming solver.

After finding the measurable delay paths, we vary the input vectors and formulate systems of linear equations for the total path delay and the individual gate delays (as discussed in Section V-C). Then, we characterize the physical properties of individual gates (e.g., V_{th} and L) based on the characterized delays using the delay model. Finally, we obtain unique IC IDs using the physical properties of all characterized gates.

C. Gate-Level Delay Characterization

Process variation (PV) manifests itself as a scaling factor multiplying the gate-level manifestational properties of delay, and it is what is extracted during the GLC. In particular, a system of linear equations can be obtained by summing the gate-level properties and measuring the delay:

$$d_j = e_{sj} + e_{rj} + \sum_j K_{ij} s_i \tag{8}$$

where d_j is the path delay at input state j; s_i is the PV scaling factor of gate i; K_{ij} is the nominal delay for the gate at input state j; and e_{sj} and e_{rj} are systematic and random delay measurement errors, respectively. We formulate a set of linear equations by varying the input vectors (i.e., input state j). Then, we measure the delay along the input/output path using delay fault approach [20]. We characterize the gate level PV scaling factors and thus the delay for each gate on the path by solving the system of equations. Finally, we employ the delay model in (2) to characterize the physical level properties (i.e., V_{th} and L).

D. Example of Delay Characterization

We demonstrate the procedure of timing characterization using a small example shown in Fig. 6. In the circuit with 5 gates, we are able to measure the delay of gates 1 and 2, as well as the delay of gates 3 and 4. Also, by switching the input vectors $I_1 I_2$ from low to high and from high to low, we obtain two sets of equations concerning the gate-level delays under process variation and the measured delay following (8). By solving the 4 equations that involve 4 variables, we are able to characterize the delays of gates 1, 2, 3, and 5. Note that in this example, we are not able to characterize the delay of gate 4, since the path 1-4-5 is subject to reconvergence with path 1-2-3-5 and cannot be measured for delay using the delay fault-based method. However, for our hardware

TABLE II
ACCURACY OF MANIFESTATIONAL GLC

Benchmark	Gates	Solved 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

metering purpose, it is sufficient to have the 4 characterized gates for generating the ID, which ensures low probability of coincidence.

E. Delay- Versus Power-Based Characterization

The main advantage of using delay over power as the side channel measurements is that each delay measurement, and thus each equation in the linear program, only covers a small number of gates (e.g., less than 10). This results in a small-size linear program that in turn requires relatively few measurements. Furthermore, delay by itself is easier to measure compared to leakage/switching power. For example, there exist well studied and applied delay fault methods to measure the delays of individual paths accurately [20].

On the other hand, the delay-based approach has one major limitation that it cannot characterize all the gates in the circuit due to the presence of reconvergent paths [19]. As shown in a small example in Fig. 2, the delay of path $X2 - X3 - X6$and path $X2 - X4 - X6$cannot be measured using the existing delay fault methods, since it is difficult to determine whether the measured delay is for the first path or the second. Also, in Fig. 6, path 1-2-3-5 and path 1-4-5 are subject to reconvergence as well.

We argue that this limitation does not impact the effectiveness of our hardware metering approach for the following two reasons. First, we note that not all the gates are required to be characterized in order to achieve low probability of coincidence on IC IDs. The probability of coincidence will be exponentially low based on the number of characterized gates. This enables us to bypass the gates that are subject to reconvergent paths and still obtain enough gates for the ID creation. Second, in certain extreme examples where the majority of gates are not measurable due to reconvergence, we can insert limited number of test points (i.e., flip-flops) to make the delay measurable [19].

VI. SIMULATION RESULTS

In this section, we introduce our simulation results that evaluate the power-based and timing-based hardware metering approaches. In particular, we evaluate the accuracy of the gate-level characterization and the resulting probability of coincidence in the generated IDs. We performed simulations on the ISCAS 85 and ISCAS 89 benchmark circuits. In physical GLC, we employ the Matlab fsolve function as the nonlinear solver.

TABLE III
SIMULATION RESULTS FOR THRESHOLD VOLTAGE AND EFFECTIVE CHANNEL LENGTH RECOVERY DURING PHYSICAL LEVEL GLC, FOR A SERIES OF BENCHMARKS

Benchmark	Gates	$V_{th}(\%)$	L (%)
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 IV
RECOVERY ACCURACY RESULTS FROM THRESHOLD VOLTAGE RECOVERY FOR BENCHMARKS FROM THE ISCAS 85 AND ISCAS 89

Benchmark	# Gates	Recovery 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

TABLE V
PROBABILITY OF COINCIDENCE WHEN USING POWER FOR HARDWARE METERING

Benchmark	# Gates	Prob. of Coincidence
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 VI
PROBABILITY OF COINCIDENCE WHEN USING POWER AND SEGMENTATION FOR HARDWARE METERING

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

A. Manifestational Gate-Level Characterization

Table II presents our results from manifestational GLC. It demonstrates the accuracy of GLC and the number of gates that can be characterized in each benchmark. Although not all the gates can be characterized, we argue that it is not necessary to characterize the entire IC, and only the minimum number of gates is required to ensure an acceptable probability of coincidence (presented in Section VI-C.).

TABLE VII
HARDWARE METERING USING TIMING CHARACTERIZATION

Benchmark	# Gates	# Characterized Gates	Delay Accuracy (%)	V_{th} Accuracy (%)	L Accuracy (%)	Prob. of Coincidence
C499	202	122	0.0031	0.35	0.018	4.25E-61
C880	383	178	0.1	0.4	0.022	6.06E-102
C1908	880	141	0.1	0.34	0.019	4.07E-88
C2670	1193	262	0.98	0.8	0.033	2.64E-178
C3540	1669	127	0.95	0.91	0.039	8.35E-87
C5315	2307	383	0.11	0.66	0.029	1.41E-252
C7552	3512	960	0.51	0.59	0.027	1.05E-578
S38584	19253	3022	0.24	1.43	0.061	1.12E-1768
Best	-	-	0.0031	0.34	0.018	1.12E-1768
Median	-	-	0.18	0.63	0.028	2.64E-178
Worst	-	-	0.98	1.43	0.061	4.25E-61

B. Physical GLC and Original Threshold Voltage Recovery

The physical GLC approach is based on leakage power, and switching power values being used to solve nonlinear equations for each gate. With this 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 [7] for effective channel length and the Gaussian model [8] for threshold voltage. The simulation results are shown in Table III. 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 0.06% error.

We conduct threshold voltage recovery using the results of physical GLC. The results are given in Table IV. The error in V_{th} recovery is below 1.7% even in the largest circuits of over 19,000 gates.

C. Probability of Coincidence

As shown in the simulation results in Table V and Table VI, we observe extremely low probabilities of coincidence (i.e., two different ICs having identical IDs) 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 V and Table VI, we can conclude that the worst case probability of coincidence is small enough to hold the false positive and false negative rates among huge population of chips (i.e. in the millions) 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.

D. Hardware Metering Using Timing Characterization

In Table VII we evaluate the effectiveness of the timing-based hardware metering approach. We employ the same set of metrics as in the power-based approach, including the number of characterized gates, the characterization accuracy of delay, V_{th}, and L, and the probability of coincidence in the generated IDs. The results indicate a need for a smaller number of characterized gates, compared to the power-based approach shown in Table I. However, the probability of coincidence remains extremely low, validating the effectiveness of the approach.

VII. CONCLUSION

With this work we have highlighted the existing weaknesses with current passive hardware metering techniques, namely the fact that IC aging will prevent the metering approach from yielding the original recorded IDs. To address this issue, we have presented a robust hardware metering scheme that leverages the persistent gate properties for gate-level characterization. The simulation results obtained using benchmarks as small as 200 and up to 19,253 gates demonstrate the effectiveness of the proposed approach.

REFERENCES

[1] S. Wei, A. Nahapetian, and M. Potkonjak, “Robust passive hardware metering,” in *Proc. ICCAD 2011*, pp. 802–809.

[2] F. Koushanfar *et al.*, “CAD-based security, cryptography, and digital rights management,” in *Proc. DAC 2007*, pp. 268–269.

[3] S. Chakravarthi *et al.*, “A comprehensive framework for predictive modeling of negative bias temperature instability,” in *Proc. IEEE Int. Reliability Physics Symp.*, 2004, pp. 273–282.

[4] Y. Alkabani *et al.*, “Trusted integrated circuits: A nondestructive hidden characteristics extraction approach,” in *Proc. Information Hiding 2008*, pp. 102–117.

[5] A. Caldwell *et al.*, “Effective iterative techniques for fingerprinting design IP,” *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 23, no. 2, pp. 208–215, Feb. 2004.

[6] S. Borkar, T. Karnik, S. Narendra, J. Tschanz, A. Keshavarzi, and V. De, “Parameter variations and impact on circuits and microarchitecture,” in *Proc. DAC 2003*, pp. 338–342.

[7] B. Cline *et al.*, “Analysis and modeling of CD variation for statistical static timing,” in *Proc. ICCAD 2006*, pp. 60–66.

[8] A. Asenov, “Random dopant induced threshold voltage lowering and fluctuations in sub-0.1 um MOSFET’s: A 3-D atomistic simulation study,” *IEEE Trans. Electron Devices*, vol. 45, no. 12, pp. 2505–2513, Dec. 1998.

[9] M. Potkonjak, A. Nahapetian, M. Nelson, and T. Massey, “Hardware trojan horse detection using gate-level characterization,” in *Proc. DAC 2009*, pp. 688–693.

[10] A. Srivastava *et al., Statistical Analysis and Optimization for VLSI: Timing and Power*. New York, NY, USA: Springer, 2005.

[11] M. Nelson, A. Nahapetian, F. Koushanfar, and M. Potkonjak, “SVD-based ghost circuitry detection,” in *Proc. Information Hiding 2009*, pp. 229–237.

[12] S. Wei, S. Meguerdichian, and M. Potkonjak, “Gate-level characterization: Foundations and hardware security applications,” in *Proc. DAC 2010*, pp. 222–227.

[13] G. Qu and M. Potkonjak*, Intellectual Property Protection in VLSI Design Theory and Practice*. Norwell, MA, USA: Kluwer, 2003.

[14] J. Lach, W. Mangione-Smith, and M. Potkonjak, “Fingerprinting techniques for field programmable gate array intellectual property protection,” *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 20, no. 10, pp. 1253–1261, Oct. 2011.

[15] G. Qu and M. Potkonjak, “Hiding signatures in graph coloring solutions,” in *Proc. Information Hiding 1999*, pp. 348–367.

[16] F. Koushanfar, G. Qu, and M. Potkonjak, "Intellectual property metering," in *Proc. Information Hiding 2001*, pp. 81–95.

[17] D. Markovic *et al.*, "Ultralow-power design in near-threshold region," *Proc. IEEE*, vol. 98, no. 2, pp. 237–252, Feb. 2010.

[18] A. Kahng, D. Kirovski, S. Mantik, M. Potkonjak, and J. Wong, "Copy detection for intellectual property protection of VLSI designs," in *Proc. ICCAD 1999*, pp. 600–604.

[19] S. Wei, K. Li, F. Koushanfar, and M. Potkonjak, "Provably complete hardware trojan detection using test point insertion," in *Proc. ICCAD 2012*, pp. 569–576.

[20] M. Majzoobi, E. Dyer, A. Elnably, and F. Koushanfar, "Rapid FPGA characterization using clock synthesis and signal sparsity," in *Proc. ITC 2010*, pp. 1–10.

[21] R. Maes, D. Schellekens, P. Tuyls, and I. Verbauwhede, "Analysis and design of active IC metering schemes," in *Proc. HOST 2009*, pp. 74–81.

[22] Y. Alkabani and F. Koushanfar, "Active hardware metering for intellectual property protection and security," in *Proc. USENIX Security 2007*, pp. 291–306.

[23] P. Koeberl, R. Maes, V. Rozic, V. Van der Leest, E. Van der Sluis, and I. Verbauwhede, "Experimental evaluation of physically unclonable functions in 65 nm CMOS," in *Proc. ESSCIRC 2012*, pp. 486–489.

[24] J. Guajardo, S. Kumar, G. Schrijen, and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," in *Proc. CHES 2007*, pp. 63–80.

[25] P. Simons, E. van der Sluis, and V. van der Leest, "Buskeeper PUFs, a promising alternative to D flip-flop PUFs," in *Proc. HOST 2012*, pp. 7–12.

[26] Y. Su, J. Holleman, and B. Otis, "A 1.6 pJ/bit 96% stable chip-ID generating circuit using process variations," in *Proc. ISSCC 2007*, pp. 406–408.

[27] R. Maes, P. Tuyls, and I. Verbauwhede, "Intrinsic PUFs from flip-flops on reconfigurable devices," in *Proc. 3rd Benelux Workshop on Information and System Security*, Eindhoven, The Netherlands, Nov. 13–14, 2008.

[28] J. Lee, D. Lim, B. Gassend, G. Suh, M. van Dijk, and S. Devadas, "A technique to build a secret key in integrated circuits for identification and authentication application," in *Proc. Symp. VLSI Circuits*, 2004, pp. 176–179.

[29] J. Anderson, "A PUF design for secure FPGA-based embedded systems," in *Proc. ASP-DAC 2010*, pp. 1–6.

[30] J. Huang *et al.*, "IC activation and user authentication for security-sensitive systems," in *Proc. HOST 2008*, pp. 76–80.

[31] A. Baumgarten *et al.*, "Preventing IC piracy using reconfigurable logic barriers," *IEEE Design Test Comput.*, vol. 27, no. 1, pp. 66–75, Jan./Feb. 2010.

[32] Y. Alkabani *et al.*, "Active control and digital rights management of integrated circuit IP cores," in *Proc. CASES 2008*, pp. 227–233.

[33] Maes *et al.*, "Analysis and design of active IC metering schemes," in *Proc. HOST 2009*, pp. 74–81.

[34] F. Koushanfar, *Hardware Metering: A Survey, Introduction to Hardware Security and Trust*. New York, NY, USA: Springer, 2012.

[35] W. Griffin *et al.*, "CLIP: Circuit level IC protection through direct injection of process variations," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 20, no. 5, pp. 791–803, May 2012.

[36] J. Zheng *et al.*, "Securing netlist-level FPGA design through exploiting process variation and degradation," in *Proc. FPGA 2012*, pp. 129–138.

[37] Maes *et al.*, "A pay-per-use licensing scheme for hardware IP cores in recent SRAM-based FPGAs," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pt. 1, pp. 98–108, Feb. 2012.

[38] J. Kim, "Toward reliable SRAM-based device identification," in *Proc. ICCD 2010*, pp. 313–320.

[39] M. Majzoobi, F. Koushanfar, and M. Potkonjak, "Lightweight secure PUFs," in *Proc. ICCAD 2008*, pp. 670–673.

[40] M. Majzoobi, F. Koushanfar, and M. Potkonjak, "Techniques for design and implementation of secure reconfigurable PUFs," *ACM Trans. Reconfig. Technol. Syst. (TRETS)*, vol. 2, no. 1, 2009, Article 5.

[41] Boning *et al., Models of Process Variations in Device and Interconnect, Design of High Performance Microprocessor Circuits*. Piscataway, NJ, USA: IEEE Press, 1999, ch. 6.

[42] K. Iniewski, *Advanced Circuits for Emerging Technologies*. Hoboken, NJ, USA: Wiley, 2012, p. 283.

[43] D. Schroder *et al.*, "Negative bias temperature instability: Road to cross in deep submicron silicon semiconductor manufacturing," *J. Appl. Phys.*, vol. 94, no. 1, pp. 1–18, 2003.

[44] S. Wei and M. Potkonjak, "Scalable segmentation-based malicious circuitry detection and diagnosis," in *Proc. ICCAD 2010*, pp. 483–486.

[45] S. Wei and M. Potkonjak, "Scalable hardware trojan diagnosis," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 20, no. 6, pp. 1049–1057, Jun. 2012.

[46] S. Wei, "Consistency-based system security techniques," Ph.D. dissertation, University of California, Los Angeles, CA, USA, 2013, ProQuest/UMI.

Sheng Wei (S'13) is a Ph.D. candidate in computer science at the University of California, Los Angeles. His research interests include hardware security, computer-aided design of VLSI circuits, and wireless networking.

Ani Nahapetian (S'03–M'07) is an Assistant Professor with the California State University, Northridge Computer Science Department, and an Assistant Adjunct Professor with the UCLA Computer Science Department. She received the Ph.D. and M.S. degrees in computer science and the B.S. degree in computer science and engineering from UCLA. Her research interests include hardware security, mobile and wireless health systems, and algorithm design for embedded systems.

Miodrag Potkonjak (M'02) received the Ph.D. degree in electrical engineering and computer science from the University of California, Berkeley, in 1991. He is a professor with the Computer Science Department at UCLA.