CACI: Dynamic Current Analysis Towards Robust Recycled Chip Identification

Yu Zheng, Abhishek Basak and Swarup Bhunia
Case Western Reserve University, Department of EECS, Cleveland, Ohio 44106
{yu.zheng3, axb594, skb21}@case.edu

ABSTRACT

Rising incidences of counterfeit chips in the supply chain have posed a serious threat to the semiconductor industry. Recycling of used chips constitutes a major form of counterfeiting attacks. If undetected, they can lead to serious consequences including system performance/reliability issues during field operation and potential revenue/reputation loss for a trusted manufacturer. Existing validation approaches based on path delay analysis suffer from reduced robustness and sensitivity under large process variations. On the other hand, existing design solutions based on aging sensors require additional design/verification efforts and cannot be applied to legacy chips. In this paper, we present a novel recycled chip identification approach, *CACI*, that exploits differential aging in self-similar modules (e.g., different parts of an adder) to isolate aged chips under large inter- and intra-die process variations. It compares dynamic current (I_{DDT}) signatures between two adjacent similar circuit structures in a chip. We derive an isolation metric based on multiple current comparisons to provide high level of confidence. *CACI* does not rely on any embedded structures for authentication, thus it comes at virtually zero design overhead and can be applied to chips already in the market. Through extensive simulations, we show that for 15% inter- and 10% intra-die variations in threshold voltage for a 45nm CMOS process, over 97% of recycled chips can be reliably identified.

Categories and Subject Descriptors

K.6.5 [**Security and Protection**]: Physical security

General Terms

Design, Security

Keywords

Hardware security, Recycled chip, Counterfeiting attack, BTI

1. INTRODUCTION

A counterfeit integrated circuit (IC) is an electronic component with discrepancy on the material, performance or characteristics, but sold as a genuine one. Counterfeit ICs include an unauthorized copy, remarked/recycled die (e.g., selling a used chip as new), cloned design through piracy or reverse engineering or failed real part [1]. Fig. 1 shows the typical life cycle of an IC from the design (by a manufacturer) to the deployment in a system (by a system designer). The IC supply chain, marked in red in Fig. 1, consists of multiple untrusted entities and is vulnerable to a potential compromise by an attacker, who can insert counterfeit chips at any level in the chain. The cost of counterfeiting and piracy is estimated to rise to 1.2 to 1.7 trillion dollars by 2015 [1]. In addition to the revenue and reputation loss to the genuine IC manufacturer, a counterfeit chip in electronic equipment may lead to severe consequences with potentially degraded quality, reliability, and performance in field operation [2]. In particular, it poses serious threats in many mission-critical applications. As a result, counterfeit chips have emerged as a major concern in the semiconductor industry. Among all counterfeit types, the recycled (i.e., aged/used) chip, often scavenged from used electronic goods, is the most common one, with over 80% share in total counterfeit chips, according to [3]. This is primarily because reselling used chips from old discarded electronics is relatively easy low-cost process, which, unlike cloning and other forms of counterfeiting attacks, requires little or no complex infrastructure. Due to aging effect, these chips suffer from degraded device threshold voltage (V_{th}) and hence reliability issues compared to new chips.

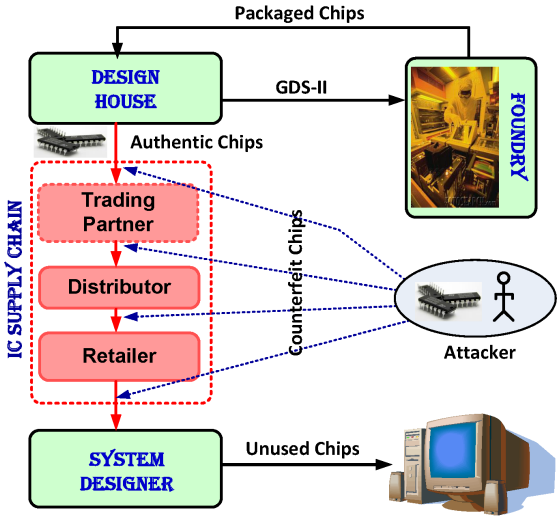

Figure 1: Typical stages in an IC supply chain, which are vulnerable to counterfeit chip insertion.

Existing industry-standard methods and tools, such as [4], [5], primarily depend on functional or parametric tests, which are typically not effective in isolating recycled or cloned chips under process variations. To address this growing need, new approaches are emerging from academia and industry. The active metering approach that minimally alters a design for authentication and remotely activates it before use has been explored to identify counterfeit chips [6]. For

DAC'14, June 01 - June 05 2014, San Francisco, CA, USA.
http://dx.doi.org/10.1145/2593069.2593102.

detecting recycled chips, researchers have proposed inserting one or more aging sensor(s) in a chip to track the change of device V_{th} shift due to aging [7]. However, both [6] and [7] add to the design overhead and cannot be used for legacy chips in the market. An emerging paradigm of IC authentication based on Physical Unclonable Function (PUF) [8] has been considered as an effective mechanism for counterfeit chip isolation by producing unique identifier for each chip. Besides the extra hardware/design cost of embedded PUF structure, it is not effective for detecting recycled chips due to the required robustness of the identifier under aging. Moreover, PUF cannot work for the chips already in the market. Other detection methods are based on the extraction of circuit parameters in authentic chips, such as path delay, to identify recycled ones [9], [10]. However, the target parameters are often difficult to measure and the detection accuracy is a concern under large process/temporal variations.

In this paper, we propose a novel recycled chip identification approach, referred to as ***C**urrent **A**nalysis based **C**ounterfeit chip **I**dentification (CACI)*, to efficiently isolate recycled chips from new ones. The key idea is that different self-similar logic blocks in a datapath (e.g., parts of adder, comparator, decoder, logical unit) experience different stress due to widely varying level of activities. For example, the functional units in a processor operate on $> 50\%$ of narrow-width operands (i.e., <16 bits in a 32-bit adder) [11]. It leads to different levels of aging in two parts of a datapath. *CACI* utilizes the correlation of dynamic supply current (I_{DDT}) of two self-similar modules with unbalanced aging to construct a process-invariant signature for each chip. Fig. 2 illustrates the overall approach. Two test vector pairs (transitions) are used to measure dynamic current $I_{DDT}^{(i)}$ and $I_{DDT}^{(i')}$ from two identical structures (i and i') for each suspect chip from a supply chain. The distance pair (d_1, d_2) of the measured currents from an expected trend line is calculated for each chip. Based on the probability density function (PDF) of (d_1, d_2) of authentic chips, we transform the distance to an isolation metric. A chip is judged as recycled when its isolation metric exceeds a pre-defined threshold.

The effectiveness of *CACI* is validated through extensive circuit-level simulation under a realistic process variation model for a 45nm CMOS process. We consider inter- and intra-die variations in V_{th} for Hspice simulation. In our evaluation, among various aging effects, we consider the effect of negative biased temperature instability (NBTI) in V_{th} using MOSRA tool from Synopsys integrated with Hspice [12]. It is well accepted that NBTI poses the most critical reliability issue that largely determines the lifetime of a circuit in nanoscale CMOS processes. The proposed approach, however, can work under other aging effects. We consider a 32-bit carry lookahead adder and equality comparator as case study, since they are common components in modern digital circuits (e.g., processor). In particular, the paper makes the following major contributions:

- It presents a low-cost robust validation approach for identifying recycled chips from an untrusted supply chain. It works for diverse chips including processor, digital signal processors (DSP), and other ASICs. A major challenge in detecting recycled chip using parametric analysis is that intrinsic process variations can easily mask the effect of aging in circuit parameters (e.g., delay or current). *CACI* addresses this challenge by taking advantage of differential aging in adjacent self-similar logic blocks. Such an analysis automatically eliminates the effect of inter-die and intra-die systematic variations. However, to effectively eliminate intra-die random variations effect (e.g., due to random dopant fluctuations) and detect recycled chips with high sensitivity, the proposed approach requires minimal process characterization. Thus, it imposes low burden and validation cost for both designer and system integrator.

- It proposes relevant metrics for I_{DDT} based analysis to detect recycled chip. It derives an isolation metric that combines the differential aging effects for multiple vectors into one consolidated metric. It provides high level of confidence to detect recycled chips with high sensitivity. A method is presented to maximize the sensitivity of detection by increasing unbalanced aging effect on I_{DDT}.

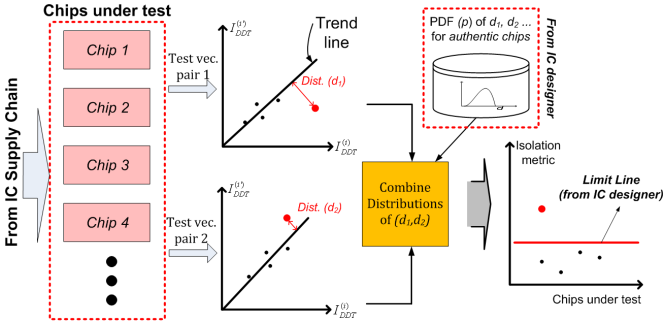

Figure 2: Illustration of the proposed recycled chip isolation process.

The rest of the paper is organized as follows. Section 2 describes the related work and motivation. The theoretical foundation is presented in Section 3. The methodology is described in Section 4. Section 5 presents the simulation results. The discussion on several important issues is provided in Section 6. We conclude in Section 7.

2. RELATED WORK AND MOTIVATION

In case of recycled chips, V_{th} is elevated due to aging effect (e.g., NBTI). The detection methods can be classified into two broad categories: (1) the circuit parameter characterization based validation, and (2) aging sensor based design approach. Among circuit parameters, [9] and [10] employ path delay. However, for [9], a large number of test vectors are required to measure path delays by using the commercial CAD tools (e.g., Tetramax) on the netlist of a chip. As a result, it cannot be applied when the netlist or test vectors are difficult to obtain. It also relies on accurate characterization of all forms (inter- and intra-die) of process variations. The effectiveness of [10] is severely limited considering the difficulty to find two paths among vast set of available ones with sufficient aging-induced path delay discrepancy. Aging sensors are embedded into a chip for tracking the V_{th} shift due to aging, with which recycled chips can be identified [7]. However, aging sensors are well-known to suffer in accuracy under large process variations. More importantly, they require design modification (also incur hardware overhead), and cannot be applied to chips already in market.

Modern digital ICs usually include many regular self-similar structures. Depending on application scenarios, PMOS transistors in each structure would have different stress/recovery duration, thus experiencing variable V_{th} shift. We used MOSRA in Hspice to observe NBTI effect in a 32-bit carry lookahead adder. Since more than 50% operands in a processor for benchmark applications are narrow-width [11], upper 16-bit are mostly all zero or one. We apply 16-bit random inputs with activity 0.5 for the lower 16-bit, while all-zero and all-one with activity 0.2 for the upper 16-bit. Fig. 3 shows a significant difference on V_{th} increase between the

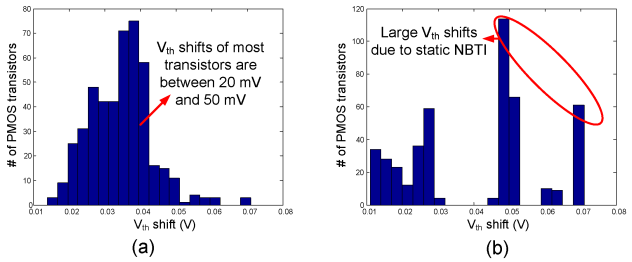

Figure 3: The histogram of V_{th} shift of a 32-bit carry lookahead adder: (a) lower 16-bit part, and (b) upper 16-bit part.

upper and lower 16-bit for a five-year aging. On the other hand, major components of process variations (inter-die and intra-die systematic) induce uniform shift in V_{th}. Hence, in *CACI*, we isolate aged chip under process variations by observing the nature of V_{th} shift in two similar and adjacent structures.

3. THEORETICAL BASIS

Fundamentally, *CACI* exploits the correlation of I_{DDT} in similar and adjacent circuit structures to differentiate between the authentic and recycled chips by observing aging-induced V_{th} shift. Both inter-die and intra-die V_{th} variations are considered in the CMOS processes. The inter-die V_{th} variation is shared by transistors on the same die and varies from die to die. The intra-die variation results in a random as well as systematic V_{th} shift among transistors within a die. Assume the nominal V_{th} is $V_{th}^{(nom)}$, the inter-die shift for chip c is $\Delta V_{th}^{(c)}$ and the intra-die shift for gate g in chip c is $\Delta V_{th}^{(c,g)}$. The gates in module i activated by test vector pair j is in set $G_{i,j}$. According to [13], the average I_{DDT} induced by test vector pair j in chip c is

$$I^{(c)}(G_{i,j}) = \sum_{g \in G_{i,j}} \beta_g (V_{DD} - V_{th}^{(c)} - \Delta V_{th}^{(c,g)})^{\alpha} \quad (1)$$

where β_g is a gate-dependent constant and $V_{th}^{(c)} = V_{th}^{(nom)} + \Delta V_{th}^{(c)}$. By Taylor's expansion, (1) can be re-written as

$$I^{(c)}(G_{i,j}) = \sum_{g \in G_{i,j}} \beta_g ((V_{DD} - V_{th}^{(c)})^{\alpha} - \gamma_g \Delta V_{th}^{(c,g)}) \quad (2)$$

where $\gamma_g = \alpha (V_{DD} - V_{th}^{(c)})^{\alpha - 1}$. Assuming i' as a similar and adjacent module of i, we can obtain the linear correlation as

$$I^{(c)}(G_{i',j}) = I^{(c)}(G_{i,j}) + S_{rand}(G_{i,j}, G_{i',j}) \quad (3)$$

$S_{rand} = \sum_{g \in G_{i,j}} \beta_g \gamma_g \Delta V_{th}^{(c,g)} - \sum_{g \in G_{i',j}} \beta_g \gamma_g \Delta V_{th}^{(c,g)}$ is associated with intra-die variation of V_{th}. The subtraction in S_{rand} cancels out intra-die systematic variation due to the strong spatial correlation for adjacent similar modules. The summation and hence averaging on S_{rand} helps to mitigate the effects of intra-die random variation, if more gates are activated simultaneously (e.g., activate short paths parallely). The influence on I_{DDT} of an unbalance-aged module pair $\{i, i'\}$ can be modeled as $S_{recycled} = \sum_{g \in G_{i,j}} \beta_g \gamma_g \delta V_{th}^{(c,g)} - \sum_{g \in G_{i',j}} \beta_g \gamma_g \delta V_{th}^{(c,g)}$, where $\delta V_{th}^{(c,g)}$ corresponds to the aging-induced V_{th} shift for gate g in chip c. Hence, the unbalanced aging effect is incorporated into (3) as

$$\begin{aligned} I^{(c)}(G_{i',j}) =& I^{(c)}(G_{i,j}) + S_{rand}(G_{i,j}, G_{i',j}) \\ &+ S_{recycled}(G_{i,j}, G_{i',j}) \end{aligned} \quad (4)$$

Under no intra-die variation, similar module i and i' should have approximately the same I_{DDT} under the same test vector pair. Hence, the trend line of (3) will be $y = x$. From (4) we can observe that the inter-die variation causes the shift of point $(I^{(c)}(G_{i,j}), I^{(c)}(G_{i',j}))$ along the trend line; the intra-die variation and aging effect leads to its deviation from the trend line. The detection of recycled chip is formulated as identifying $S_{recycled}$ in average I_{DDT}. To improve accuracy, we enhance the sensitivity of $S_{recycled}$ to I_{DDT} of similar and adjacent module i and i' in Section 3.1 and 3.2.

3.1 I_{DDT} Averaging Window

The location and size of a time window (TW) should be selected properly when measuring the average value of I_{DDT}. Fig. 4(a) shows the shape of I_{DDT} in time domain, as well as a proper TW to average it. TW is represented as a time interval $[t_0, t_1]$ $(t_1 \geq t_0)$ that captures a large fraction of dynamic power for a test vector pair, and satisfies

$$\begin{aligned} &min \;\; t_1 - t_0 \\ &s.t. \int_{t_0}^{t_1} I_{DDT}(t)dt \geq \eta V_{DD} C_{L,t} \end{aligned} \quad (5)$$

where $C_{L,t}$ is the overall capacitance of $G_{i,j}$ and $G_{i',j}$; η is a control factor for charging (e.g., 0.9). In (5), we minimize $t_1 - t_0$ to increase the sensitivity of I_{DDT} to V_{th}. Algorithm A is proposed to implement (5). In step 1, the time t_{max} is the maximum transient current $I_{DDT}^{(i)}(t_{max})$. Hence, $t_0 = t_{max} - \Delta t_0$ and $t_1 = t_{max} + \Delta t_1$ are employed to form a proper TW for computing average I_{DDT} in step 2-4.

Fig. 4(b) shows the I_{DDT} shape of module pair $\{i, i'\}$ with different aging profiles under the same test vector pair. The gates activated in module i' has larger V_{th} shift. Hence, I_{DDT} of $\{i, i'\}$ (blue and black triangle) in Fig. 4(b) do not completely overlap, creating a small shift in the time of the maximum I_{DDT} and the charge/discharge duration. If TW is changed to track such shift, the average I_{DDT} may only show small discrepancy between i and i'. The difference of V_{th} shift is not fully reflected on I_{DDT} measurement.

Algorithm A: Measure Average I_{DDT} under $G_{i,j}$ and $G_{i',j}$

Input: $I_{DDT}^{(i)}(t)$ and $I_{DDT}^{(i')}(t)$ for module $\{i, i'\}$

1. Find the time t_{max} with max. $I_{DDT}^{(i)}(t)$
2. Specify Δt_0 and Δt_1 for $\int_{t_{max}-\Delta t_0}^{t_{max}+\Delta t_1} I_{DDT}^{(i)}(t)dt \geq \eta V_{DD} C_{L,t}$
3. Compute the average I_{DDT} of module i in chip c as $I^{(c)}(G_{i,j}) = \frac{1}{\Delta t_0 + \Delta t_1} \int_{t_{max}-\Delta t_0}^{t_{max}+\Delta t_1} I_{DDT}^{(i)}(t)dt$
4. Compute the average I_{DDT} of module i' in chip c as $I^{(c)}(G_{i',j}) = \frac{1}{\Delta t_0 + \Delta t_1} \int_{t_{max}-\Delta t_0}^{t_{max}+\Delta t_1} I_{DDT}^{(i')}(t)dt$

Output: $I^{(c)}(G_{i,j})$ and $I^{(c)}(G_{i',j})$

Based on such analysis, Algorithm A also amplifies the sensitivity of average I_{DDT} on different V_{th} shifts of $\{i, i'\}$. A proper TW is specified in step 2 for module i (not i'). The average I_{DDT} is calculated in step 3 and 4 using the same TW found in step 2 to enhance the difference.

3.2 Effect of Supply Voltage (V_{DD})

V_{DD} affects I_{DDT}, and thus the effectiveness of Algorithm A. Fig. 5(a) shows the change on I_{DDT} with a load of total capacitance $C_{L,t}$, when V_{DD} is increased. The charging duration $t_2 - t_1$ can be approximately written as

$$(t_2 - t_1) \propto \frac{C_{L,t} V_{DD}}{\beta (V_{DD} - V_{th})^{\alpha}} \quad (6)$$

In (6), the increase in V_{DD} leads to smaller $t_2 - t_1$. Hence, dynamic power is more concentrated around the time when maximum I_{DDT} occurs, as shown in Fig. 5(b). The effectiveness of step 3 and 4 in Algorithm A is therefore enhanced

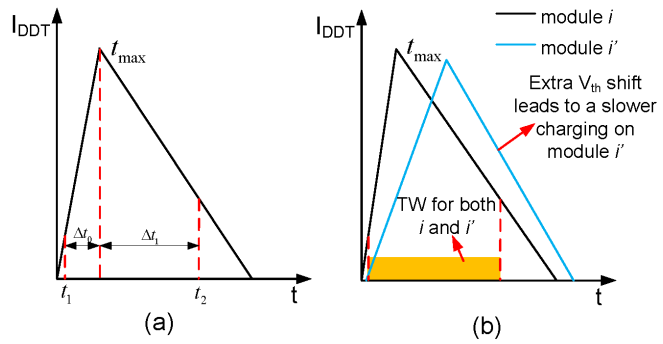

Figure 4: (a) An appropriate time window (TW) to measure average I_{DDT}, and (b) shift in TW with V_{th} change due to aging.

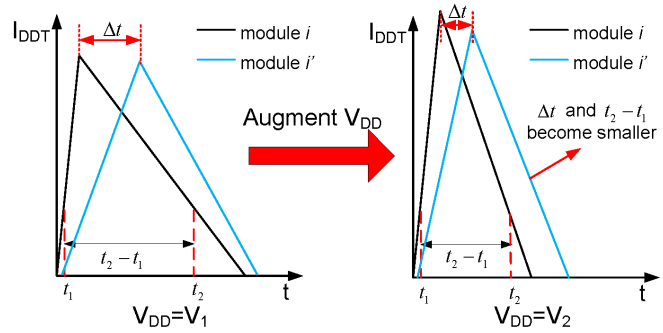

Figure 5: I_{DDT} of module $\{i, i'\}$ for (a) $V_{DD} = V_1$, and (b) $V_{DD} = V_2$ $(V_1 < V_2)$.

with the increase of V_{DD} until it achieves a certain value. Δt decreases with a larger V_{DD} ($\Delta t \to 0$ as $V_{DD} \to \infty$). We analyze the influence of V_{DD} on detecting recycled chip with Hspice simulation in Section 5.2.

4. METHODOLOGY

In this section, we describe the steps in *CACI* to detect a recycled chip during system integration. It exploits differential aging in self-similar circuit blocks to isolate aged chips from new ones in presence of both inter- and intra-die process variations. *CACI* extracts the information of authentic chips by IC designer as illustrated in Fig. 6(a); and a suspect chip is authenticated by system designer as depicted in Fig. 6(b).

Assume the authentic and suspect chips constitute set N and U, respectively; test vector pairs are in set T to activate a similar module pair $\{i, i'\}$. In Fig. 6(a), the test vector pairs in T are input into $\{i, i'\}$ of chips in N to compute average I_{DDT} by Algorithm A. The distance set $\{d_{i,j}^{(c)}\}$ to the trend line $(y = x)$ for points $(I^{(c)}(G_{i,j}), I^{(c)}(G_{i',j}))$ $(c \in N)$ $(1 \le j \le |T|)$ is computed to estimate the probability density function (PDF) family $\{p_j(\cdot)\}$. An isolation metric is formulated from log-likelihood of $\{d_{i,j}^{(c)}\}$ in a chip, along with the threshold Th_R of recycled chip. Here, T, $\{p_j(\cdot)\}$ and Th_R are produced and shared by IC designer for authentication. As shown in Fig. 6(b), the isolation metric of each suspect chip is calculated and compared with Th_R to decide whether it is recycled or not.

4.1 Measurement of Average I_{DDT}

Average I_{DDT} is measured for a chip by following steps in Algorithm A. The time/magnitude accuracy should be considered, especially when I_{DDT} varies rapidly with switching test vector pairs. In [14], we observe that photoconductive semiconductor switches can yield time accuracy as high as

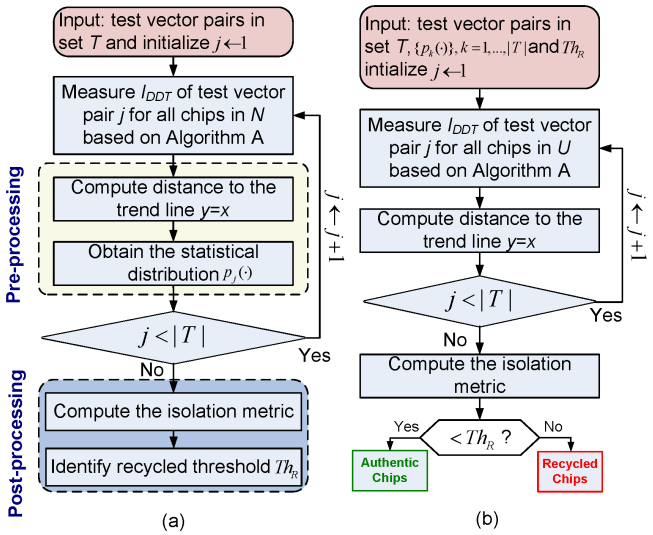

Figure 6: The procedure of *CACI*: (a) information extraction for authentic chips, and (b) authentication of chips under test.

10 ps. Moreover, small current can be measured with the accuracy up to pA level [15]. Such resolution is enough to implement *CACI* for chips. In non-ideal environment, temporal noises (e.g., temperature and V_{DD} fluctuations) can decrease the measurement accuracy. However, we can minimize these effects through multiple measurements. In our simulation, average I_{DDT} is directly estimated through Hspice.

4.2 Pre-processing

Based on $(I^{(c)}(G_{i,j}), I^{(c)}(G_{i',j}))$ for $c \in N$ and $j \in T$, we proceed with the steps of pre-processing to extract the information for identifying authentic chips. $(I^{(c)}(G_{i,j}), I^{(c)}(G_{i',j}))$ is projected on the trend line $y = x$ with coordinate $(a_j^{(c)}, a_j^{(c)})$. It can be derived that $|I^{(c)}(G_{i,j}) - a_j^{(c)}| = |I^{(c)}(G_{i',j}) - a_j^{(c)}|$. Considering the sign of $I^{(c)}(G_{i',j}) - a_j^{(c)}$ that shows the location of $(I^{(c)}(G_{i,j}), I^{(c)}(G_{i',j}))$ relative to the trend line, the distance $d_{i,j}^{(c)}$ is calculated as

$$d_{i,j}^{(c)} = (\sqrt{2}/2)(I^{(c)}(G_{i',j}) - I^{(c)}(G_{i,j})) \quad (7)$$

Due to the process/aging effect on V_{th}, $d_{i,j}^{(c)}$ can be processed as a random variable with PDF $p_j(\cdot)$. From (3) and (7), we derive $d_{i,j}^{(c)} = (\sqrt{2}/2)S_{rand}$. Hence, $p_j(\cdot)$ depends on the distribution of intra-die variation. Particularly, $p_j(\cdot)$ can be modeled as a Gaussian distribution, if the intra-die variation of V_{th} follows a Gaussian distribution.

4.3 Post-processing and Authentication

Based on the data set $\{d_{i,j}^{(c)}\}$ and PDF family $\{p_j(\cdot)\}$, $c \in N$, $j \in T$, we derive the isolation metric for each authentic chip, as well as the detection threshold for recycled chip. Since the gates in $G_{i,j}$ activated by test vector pair j can be different from $G_{i,j'}$ $(j \neq j')$, the random variables of PDF $p_j(\cdot)$ and $p_{j'}(\cdot)$ are approximated as statistically independent. Hence, the log-likelihood of authentic chip c is:

$$B_{i,i'}^{(c)} = -log_{10}(\prod_{j=1}^{|T|} p_j(d_{i,j}^{(c)})) = -\sum_{j=1}^{|T|} log_{10}(p_j(d_{i,j}^{(c)})) \quad (8)$$

Here, $B_{i,i'}^{(c)}$ is called *isolation metric* of chip c. In the presence of process variation, $B_{i,i'}^{(c)} \neq B_{i,i'}^{(c')}$ for $c \neq c'$. The recycled-chip threshold is set as $Th_R = \overline{B_{i,i'}} + \gamma \cdot \Delta B_{i,i'}$, where $\overline{B_{i,i'}}$

and $\Delta B_{i,i'}$ are the mean value and standard deviation of set $\{B_{i,i'}^{(c)}\}$ $(c \in N)$ and γ is a tunable positive factor to adjust Th_R for lower error rate.

Fig. 6(b) shows the major steps to identify a suspect chip c in set U by system designer. First, $d_{i,j}^{(c)}$ is computed as (7). The isolation metric $B_{i,i'}^{(c)}$ is obtained according to (8). If $B_{i,i'}^{(c)} \leq Th_R$, it is judged as an authentic chip in N ('hit'); otherwise a recycled chip in C ('reject'), i.e.,

$$auth_c = \begin{cases} hit & if \quad B_{(i,i')}^{(c)} < Th_R \\ reject & otherwise \end{cases} \tag{9}$$

In the ideal situation, if a chip in U is authentic, its $B_{(i,i')}^{(c)}$ should be less than Th_R and $auth_c$ is 'hit'; Similarly, if it is recycled, $auth_c$ should be 'reject'. However, a misjudgement occurs due to the existence of process variations. Hence, the error rate e is calculated as

$$e = Pr(hit, \ recycled) + Pr(reject, \ new) \tag{10}$$

where $Pr(hit, \ recycled)$ and $Pr(reject, \ new)$ mean the probability of misjudging a recycled and authentic chip.

5. SIMULATION RESULTS

5.1 Simulation Setup

To validate *CACI*, we use the transistor-level netlist of 32-bit lookahead adder and 32-bit equality comparator, since they are common in modern digital circuits. The simulation is carried out in Hspice for PTM 45nm CMOS process [16]. MOSRA in Hspice is used to generate the profile of V_{th} shift due to NBTI. Considering narrow-width operands, most test vectors into upper 16-bit part have at least one all-zero (or all-one) operand with low flipping probability (e.g., 0.2), while the lower 16-bit has the random vectors with flipping probability 0.5. Next, we incorporate an aging profile into process variation of V_{th}, which is modeled as 15% inter-die and 10% random intra-die variation and a Gaussian distribution. We use 16 test vector pairs for measuring average I_{DDT} in Algorithm A. We simulate 200 authentic adders (and comparators) under the process variation, as well as two aged versions with one year and five years of use. Next, the procedures of *CACI* are carried out for $B_{i,i'}^{(c)}$ of each chip and we make a judgement using (9). Assuming equal probability for authentic and recycled chip, we calculate $Pr(hit, \ recycled)$ and $Pr(reject, \ new)$ to obtain e.

5.2 Analysis

For one-year aging, the histograms of V_{th} shifts in the adder and equality comparator are shown in Fig. 7 and Fig. 8. The mean V_{th} shifts of the lower/upper 16-bit part in the adder are 23.2 mV and 27.2 mV, while 24.1 mV and 26.4 mV for the comparator. The V_{th} shifts of lower and upper part have a different histogram and thus a recycled version can be differentiated. For a given test vector pair, the average I_{DDT} correlations of upper/lower 16-bit part in adder and comparator are shown in Fig. 9. The points of recycled chips are slightly lower than that of authentic chips due to Algorithm A. Hence, $\{d_{i,j}^{(c)}\}$ of recycled chip has a different distribution. Fig. 9(b) shows the histograms of $\{d_{i,j}^{(c)}\}$ to estimate $p_j(\cdot)$. They follow the Gaussian distribution that matches the derivation in Section 4.2.

A proper γ should be selected to minimize e. In the simulation, γ is set as one and two for adder and comparator, respectively with the result shown in Fig. 11. The isolation metric of recycled chip for one-year usage is larger than that of authentic chip in Fig. 11. The error rate e is 6.25% for both the adder and comparator.

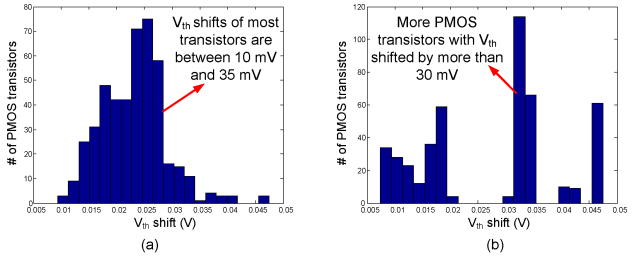

Figure 7: The V_{th} shifts of adder used for one year: (a) lower 16-bit part, and (b) upper 16-bit part.

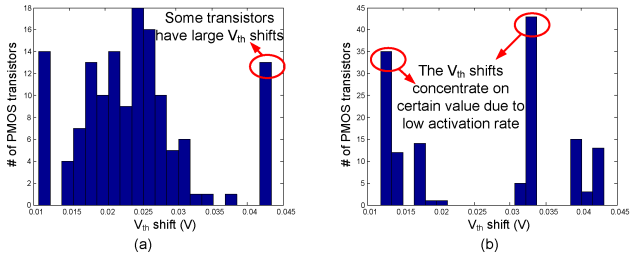

Figure 8: The V_{th} shifts of comparator used for one year: (a) lower 16-bit part, (b) upper 16-bit part.

We also apply *CACI* to detect recycled chip for five-year usage. e with the same γ as one-year age is reduced to 2.5% and 3% for the adder and comparator, respectively. Hence, *CACI* works effectively to identify recycled chips. Moreover, e is reduced with the increase in usage duration. It is useful for recycled-chip detection, since older chips are more dangerous once integrated into electronic systems.

In Section 3.2, choice of an optimal V_{DD} is analyzed for a circuit structure. The average I_{DDT} is measured under different V_{DD} after one-year aging. Fig. 12 shows the error rate e when γ is one and two for adder and comparator. $V_{DD} = 1.0$ V is the best choice for the adder, since it achieves the minimum $e = 0.0625$. When V_{DD} becomes 1.1 V or 0.9 V, e rises up to 0.2875 and 0.3, respectively. However, comparator shows a different trend. e is 0.2175 for $V_{DD} =$ 0.9 V. With the increase of V_{DD}, e decreases to 0.045 when $V_{DD} = 1.1$ V. Hence, it is helpful to select a proper value of V_{DD} for each type of circuit structure for a smaller e.

6. DISCUSSION

6.1 Extensions of *CACI*

SRAM is common component in modern SoCs, which includes an array of cells (e.g., 6-T, 8-T) organized in a regular structure. Due to abundance of narrow-width operands in real applications [11], most significant bits (MSBs) in a word store '0' (or '1') in most time. The contents in least significant bits are altered more frequently. Hence, the aging effect is unbalanced for MSBs and LSBs. Furthermore, an embedded memory usually has separate power grid that simplifies I_{DDT} measurement for memory core with reduced noise. Hence, it can be a good candidate to determine aging of a chip by employing *CACI*.

In addition to digital circuits, *CACI* is also promising for mixed-signal circuits. For example, pipelined analog-to-digital converter (ADC) includes several stages of similar structure. The aging effect of each stage is different, since ADC works in the middle of transfer function in a major time to reduce the influence of differential nonlinearity (DNL). As a result, the activity of MSBs is lower than LSBs, which leads to aging discrepancy.

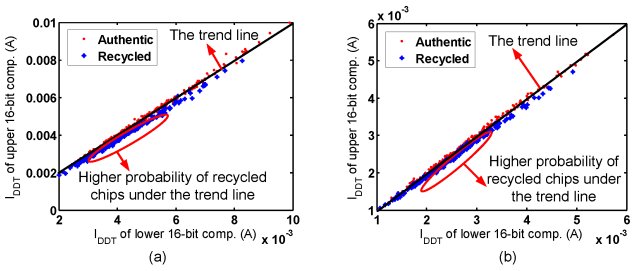

Figure 9: Average I_{DDT} correlation for: (a) the adder, and (b) the comparator.

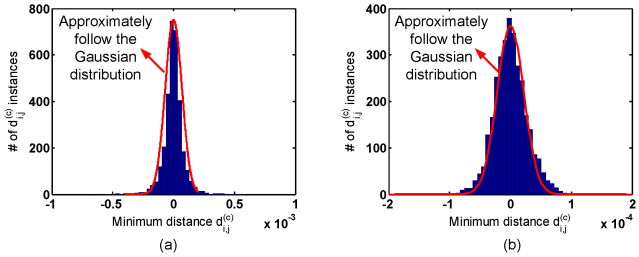

Figure 10: The histogram of $\{d_{i,j}^{(c)}\}$ for: (a) the adder, and (b) the comparator.

6.2 Sensitivity analysis

Sensitivity can be enhanced from two perspectives. First, in Fig. 7 and 8, only a subset of PMOS transistors in the upper 16-bit structure has more (or less) V_{th} shift than that in the lower 16-bit part. Hence, it is desirable to choose the test vector pairs that can activate those transistors to maximize the difference in I_{DDT}. Second, the PDF family $\{p_j(\cdot)\}$ is directly related to V_{th} intra-die variation. The points corresponding to authentic chips in Fig. 9 tend to be closer to the trend line with a smaller intra-die variation. Hence, I_{DDT} becomes more sensitive to unbalanced aging. With the increase in intra-die variation, the sensitivity decreases.

7. CONCLUSION AND FUTURE WORK

We have presented *CACI*, a methodology to detect recycled counterfeit chips in a supply chain by exploiting the discrepancy in I_{DDT} of two similar modules with different aging profiles. Using extensive simulations under realistic process variations, we have shown that it can identify recycled chips reliably with good sensitivity. With virtually no design modification, *CACI* can be applied to legacy chips in the market. Since modern SoCs include many regular self-similar structures that experience different level of stress during operation, *CACI* can be effectively employed to them. Since it eliminates effect of inter-die and intra-die systematic variations, it is easily scalable to large complex designs. Although we focus on ASICs in our study, the proposed approach can also be employed to FPGA chips since different configurable logic blocks are expected to suffer from different stress-induced aging. Furthermore, *CACI* can work for mixed-signal chips such as ADC and telemetry units, which increasingly use digital components of regular structure. Future work will consider extension of the approach to other chips (e.g., FPGA, mixed-signal) and integration with complementary approaches.

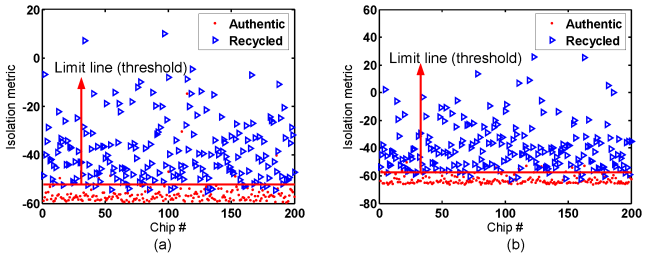

Figure 11: The isolation metric of 200 authentic chips and 200 one-year used chips: (a) the adder, and (b) the comparator.

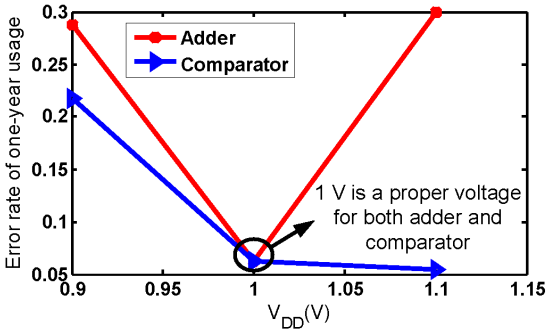

Figure 12: The change of error rate e at different voltage levels for the adder and the comparator.

8. REFERENCES

[1] U. Guin, *et al.*, "Counterfeit IC detection and challenges ahead," ACM SIGDA, March 2013.

[2] F. Koushanfar, *et al.*, "Can EDA Combat the Rise of Electronic Counterfeiting?" *DAC*, 2012, pp. 133-138.

[3] L. W. Kessler and T. Sharpe, "Faked Parts Detection," http://www.circuitsassembly.com/.

[4] Integra Technologies Inc., http://www.integra-tech.com.

[5] ABI Electronic Inc., http://www.abielectronics.co.uk.

[6] Y. Alkabani and F. Koushanfar, "Active Hardware Metering for Intellectual Property Protection and Security," *USENIX Security*, 2007.

[7] X. Zhang, N. Tuzzio and M. Tehranipoor "Identification of recovered ICs using fingerprints from a light-weight on-chip sensor," *DAC*, 2012, pp. 703-708.

[8] G. E. Suh and S. Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation," *DAC*, 2007, pp. 9-14.

[9] X. Zhang, K. Xiao, and M. Tehranipoor, "Path-delay fingerprinting for identification of recovered ICs," *DFT*, 2012, pp. 13-18.

[10] R. Moudgil, *et al.*, "A novel statistical and circuit-based technique for counterfeit detection in existing ICs," *GLSVLSI*, 2013, pp. 1-6.

[11] D. Brooks and M. Martonosi, "Dynamically exploiting narrow width operands to improve processor power and performance,", *HPCA*, 1999, pp. 13-22.

[12] Synopsys, HSPICE user guide: simulation and analysis, 2010.

[13] S. Narasimhan, *et al.*, "Multiple-parameter side-channel analysis: a non-invasive hardware Trojan dectection approach," *HOST*, 2010, pp. 13-18.

[14] P. Rossi, *et al.*, "A low power ultra-fast current transient measurement device," Sandia Report, Sand2004-5101, 2004.

[15] B. Goldstein, *et al.*, "CMOS low current measurement system for biomedical applications," *IEEE Bio-CAS*, vol. 6, No. 2, pp. 111-119, 2012.

[16] Predictive Technology Model, http://ptm.asu.edu/