This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2015.2449231, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

SeMIA: Self-Similarity based IC Integrity Analysis

Yu Zheng, *Student Member, IEEE*, Shuo Yang, *Student Member, IEEE* and Swarup Bhunia, *Senior Member, IEEE*

***Abstract*—Counterfeit chips in the supply chain as well as hardware Trojan attacks pose serious threats to the semiconductor industry. If undetected before deployment, they can lead to serious consequences including system performance/reliability issues during field operation and potential revenue/reputation loss for a trusted manufacturer. Currently, no unified detection method is available that can simultaneously address these integrity violations in integrated circuits (ICs). In addition, most existing detection approaches require a set of golden chips as a reference, which significantly increases the test cost and complexity. Furthermore, in some scenarios, it may be extremely difficult to obtain golden chips. In this paper, we present a novel unified IC integrity analysis approach that can effectively detect both recycled counterfeit ICs (the most dominant form of counterfeiting) as well as Trojan attacks in ICs without the need of golden chips. The proposed approach, referred to as SeMIA, exploits intrinsic structural self-similarity in a design (e.g., multiple cores, multiple functional units of the same type, different parts of an adder) to isolate recycled chips and hardware Trojan attacks under large inter- and intra-die process variations. It compares dynamic current (I_{DDT}) signatures between two adjacent similar circuit structures using an appropriate isolation metric to detect such attacks with high degree of confidence. SeMIA does not rely on any embedded structure for authentication, thus it comes at virtually zero hardware overhead and can be applied to chips already produced. Through extensive simulations, we show that for 15% inter- and 10% intra-die variations in threshold voltage for a 45nm CMOS process, over 98% of recycled chips can be reliably identified. Finally, experimental measurements on Field Programmable Gate Array (FPGA) chips demonstrate the effectiveness of SeMIA for protection against both attacks.**

***Index Terms*—Counterfeit chips, Hardware Trojan, Golden-free detection, Self-similarity, Dynamic current, Process variation, BTI.**

I. Introduction

Security has emerged as an important design and test parameter for integrated circuits (ICs) in recent years. The long and globally distributed supply chain of ICs has greatly increased the opportunity of IC counterfeiting attacks at different stages of the distribution cycle. On the other hand, increasing reliance on third-party Intellectual Properties (IPs) and design tools, and IC fabrication in external (and potentially untrusted) foundry have significantly reduced a designer's control on the manufactured chips, providing opportunities to adversaries for hardware Trojan (HT) attacks. Counterfeit IC and HT attacks constitute two major security threats arising form integrity violation during IC design, manufacturing and distribution process [1]–[3]. A counterfeit IC is an electronic component with discrepancy on the material, performance or characteristics, but sold as a genuine one. On the other hand, an HT can be defined as a malicious design modification that tampers a trusted design to incorporate undesired functional/parametric behavior. 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) through a supply chain that typically includes trading partner, distributor and retailer. The IC supply chain in Fig. 1, consists of multiple untrusted entities and is vulnerable to potential compromise by an attacker, who can insert counterfeit chips at any level in the chain. HTs can be introduced at different stages during the IC design and manufacturing process, e.g., tampering the design by an untrusted Computer-Aided Design (CAD) tool during System-on-Chip (SoC) integration, or a malicious implantation in an untrusted foundry [2], [4].

Counterfeit ICs typically come in various types, including an unauthorized copy, remarked/recycled die (e.g., selling a used chip as new), cloned design through piracy or reverse engineering, and failed or overproduced real part [5]. The cost of counterfeiting and piracy is estimated to rise to a staggering 1.2 to 1.7 trillion dollars by 2015 [5]. Among all counterfeit types, the recycled (i.e., aged/used) chip, often scavenged from used electronic goods, is the most dominant one with over 80% share in total counterfeit chips in the market [6]. 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 effects, recycled chips suffer from degraded device threshold voltage (V_{th}), thus leading to reduced reliability and/or performance. On the other hand, HT can potentially compromise an IC's functional or parametric behavior in a way that can evade conventional post-silicon test and validation process. The HTs are expected to be rarely activated during production test and to induce only minor variation in side-channel parameters, such as path delay or power. In addition to the revenue and reputation loss to the genuine IC designer, counterfeiting or HT attacks in ICs may lead to severe consequences with potentially degraded quality, reliability, integrity, and performance in field operation [3]. In particular, they pose serious threats in many mission-critical applications involving our military, communication, aviation, power-grid, and other national infrastructures.

Existing industry-standard methods and tools for counterfeit IC detection, such as [7], [8], primarily depend on functional or parametric tests, which are typically not effective in isolating counterfeit chips of all types. To address this growing need, new approaches are emerging from academia and industry. A

Yu Zheng, Shuo Yang and Swarup Bhunia are with the Department of Electrical Engineering and Computer Science, Case Western Reserve University, Cleveland, OH 44106, USA. E-mail: {yxz402,sxy390,skb21}@case.edu.

The work has been funded in part by National Science Foundation grants 1054744, 1245756, and 1441705.

We acknowledge extensive support on hardware experiments from George Daher in Sears Lab, EECS, Case Western Reserve University.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2015.2449231, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

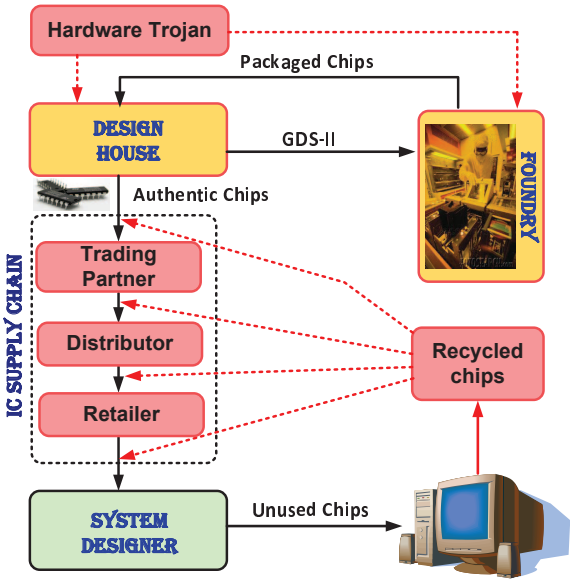

Fig. 1. Typical stages in an IC supply chain. Many of these stages are vulnerable to counterfeiting or HT attacks as shown.

design is locked and can be activated only by the original manufacturer through an authentication process [9]–[11]. To detect used chips, researchers have proposed inserting sensors into a design to track shift in device V_{th} due to aging [12]. Physical Unclonable Functions (PUFs) [13] have been considered as effective means for counterfeit chip isolation. They aim at producing unique identifier from each chip instance. However, they often incur considerable design and hardware overhead and cannot be applied to legacy chips in the market. Other detection methods rely on analysis of physical parameters (e.g., dynamic power, path delay) during post-manufacturing test on genuine chips. In [14], a scan based characterization of circuit delay is proposed to detect cloned chips. To address recycled chips, path delays are employed to form a fingerprint [15]–[17]. However, the target parameters are often difficult to measure for these approaches and the detection accuracy can suffer under large process/temporal variations. On the other hand, existing countermeasures against HT attacks primarily focus on non-destructive test solutions, primarily side-channel analysis approaches. The central idea behind side-channel analysis based HT detection is to distinguish a Trojan effect in a physical parameter (e.g., supply current or path delay) from process and temporal variations. While side-channel analysis provides a promising HT detection paradigm, a major challenge with these approaches lies in the need of a set of golden or reference ICs, which are used to calibrate intrinsic process noise. Obtaining a set of golden ICs can be extremely difficult since it may require exhaustive testing or destructive reverse-engineering based trust validation of these ICs [18].

In order to build a trustworthy system, a system designer needs to ensure the integrity of each IC before using it in a system. To the best of our knowledge, there is no unified detection method that can verify the integrity of an IC against both recycling and HT attacks. In this paper, we propose a golden-free IC integrity validation framework based on dynamic current (I_{DDT}) analysis, referred to as ***Self-similarity***

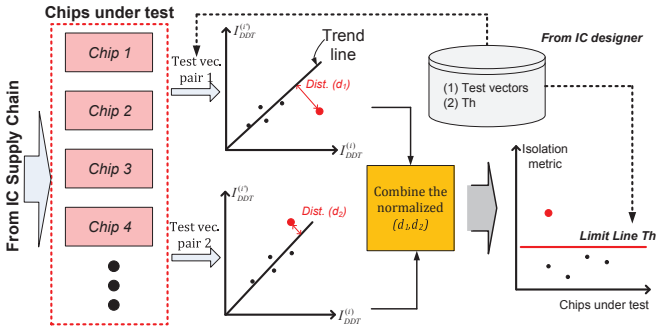

Fig. 2. Illustration of the proposed recycled/HT-affected chip isolation process.

*based **M**icrochip **I**ntegrity **A**nalysis (SeMIA)*, to simultaneously identify ICs that are recycled or tampered by HT attacks. SeMIA leverages on the structural self-similarity among circuit blocks in a chip. It compares the side-channel signature (e.g., I_{DDT}) of one block with another self-similar block on the same chip. The key idea is that different self-similar blocks (e.g., parts of an adder, comparator, memory, and logical datapath) experience different stress (hence, different aging profiles) due to widely varying level of activities, or exhibit asymmetric side-channel signatures due to HT attacks. For example, the datapath units in a processor may experience different activities in their upper (most significant bits i.e., MSBs) and lower (least significant bits, i.e., LSBs) parts, due to the abundance ($> 50\%$) of narrow-width operands i.e., <16 bits operands in a 32-bit adder, for reference workload [19], [20]. It leads to different levels of stress (hence, aging) in two parts of the adder. Similarly, part of a multiplier with an HT shows different level of activity and hence, dynamic power profile, compared to another similar part. We utilize the correlation of I_{DDT} in two self-similar modules to identify unbalanced shift in V_{th} due to aging or presence of HT in one of the modules. Fig. 2 illustrates the overall approach for detecting recycled chips. 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 used to derive an isolation metric. A chip is judged as recycled or tampered with HT when its isolation metric exceeds a pre-defined threshold.

In particular, the paper makes the following key contributions:

- It provides a formal representation of the problem of IC integrity validation by simultaneously incorporating the characteristics of recycled chips and HT circuits. The effects of aging profile as well as HT attack are captured into a unified variable.
- It presents a low-cost robust solution for IC integrity validation based on I_{DDT} analysis that identifies both recycled chips and HT attacks in regular self-similar structures in an IC. It requires no reference or golden chips and is scalable to highly complex chips of diverse types such as general-purpose processor, graphics engine, and digital signal processor (DSP). The employment of self-similar and adjacent logic blocks automatically

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2015.2449231, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

eliminates the effect of inter-die and intra-die systematic variations. The intra-die random variation effect (e.g., due to random dopant fluctuations) is minimized by considering switching of reasonable number of gates during vector selection and use of multiple test vectors. Moreover, we present an I_{DDT} measurement method that can maximize the discrepancy of circuit parameters between similar logic blocks.

- It validates the effectiveness of SeMIA through extensive circuit-level simulations with Hspice under a realistic process variation model for a 45nm CMOS technology as well as through hardware measurements. In our evaluation, among various aging effects, we consider the effect of negative bias temperature instability (NBTI) in V_{th} using MOSRA tool from Synopsys integrated into Hspice [21]. 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 also work under other aging effects. We evaluate the effectiveness of the approach for common circuit blocks such as carry-lookahead adder (CLA), array multiplier, equality comparator as well as a larger design, namely a five-stage pipelined DLX processor. The simulation results show that over 98% recycled or HT-affected chips can be identified correctly. We also validate SeMIA with hardware measurements using Field Programmable Gate Array (FPGA) chips that emulate unbalanced aging and HT attacks.

The rest of the paper is organized as follows. Section II describes the related work and the motivation behind the proposed solution. The problem with golden-free integrity analysis is formalized in Section III. The methodology of SeMIA is described in Section IV. Section V and Section VI present the simulation and experimental results, respectively. Section VII discusses possible attacks on SeMIA and its extension. We conclude in Section VIII.

II. Background and Motivation

Large volume of prior research has aimed at separately addressing the threat of counterfeit ICs and HT attacks.

A. Related Work

In case of recycled chips, usually transistor threshold voltage V_{th} is elevated due to aging effect e.g., Negative Bias Temperature Instability (NBTI). Methods to detect these chips can be classified into two broad categories: (1) analysis of circuit parameters, and (2) age estimation with integrated aging sensors. Among circuit parameters, several works employ path delay [15] [16]. However, in case of [15], a large number of test vectors is required to obtain reliable path delay fingerprints. As a result, it cannot be applied when the netlist of the original design 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 the approach in [16] is limited considering the difficulty to find two paths among vast set of available ones with sufficient aging-induced path delay discrepancy. On the other hand, aging sensor based approaches rely on embedding one or more sensors into a chip for tracking the V_{th} shift due to aging, thereby isolating aged chips from new ones [12]. However, aging sensors are well-known to suffer from poor accuracy under large process variations. Moreover, the low-overhead aging sensors typically provide low sensitivity, which limits its ability to detect aged chips used for relatively short duration (e.g., 6 months). Furthermore, they require design modification (also incur hardware overhead), and cannot be applied to chips already in market.

Protection against HT attacks can be classified into two broad categories: destructive and non-destructive methods. Destructive reverse engineering based HT detection methods are highly complex and expensive and do not scale well with the growing complexity of ICs. Furthermore, trust validation for a set of chips through destructive process does not rule out HT attack in the remaining chips. Non-destructive methods can be based on (1) Design-for-Security (DfS) and (2) post-fabrication test as well as characterization approaches. DfS approaches work towards making HT implantation difficult/ineffective or facilitating HT detection. For example, a design can be modified by inserting dummy/shadow flip-flops for improving observability and controllability of internal nodes which helps in detecting hard-to-trigger/observe HTs [23]. Similarly a design can be modified to accomplish on-line monitoring of path delay [24] or frequency shift of ring oscillators (ROs) built into circuit paths [25], [26]. In [27], a transparent mode is introduced in a design with a FSM to enhance the controllability and observability of internal nodes. Researchers have also shown that high-precision delay structure or current sensing circuit can be embedded into a design to improve HT detectability [28], [29]. Functional filler cells are inserted into unused space to prevent HT insertion [30]. However, the above approaches often incur considerable hardware overhead and suffer from poor HT coverage.

HT detection approaches, on the contrary, primarily rely on analysis of side-channel information of ICs such as, dynamic current (I_{DDT}), path delays, or quiescent current (I_{DDQ}) [31]–[33]. The activity of HT impacts dynamic power trace of a design, which can be isolated from process noise through statistical analysis e.g., Karhunen-Loeve expansion [31]. Researchers have also proposed using the combinational path delays to isolate HT-infected ICs by constructing the fingerprint for golden ICs, in which the effect of process variation is mitigated through principle component analysis [32]. The approach in [33] uses unexpected deviation in I_{DDQ} to detect HT. In [34], the authors show that HT breaks the leakage power correlation under different thermal conditioning. In [35], [36], a design is divided into several small regions to improve the sensitivity of HT detection by analyzing dynamic current signature of a region. The correlation between maximum frequency and dynamic current can be exploited to identify small HT circuits in the presence of large process variations [37]. These side-channel analysis approaches, however, require a set of golden chips for accurate characterization of process noise.

Researchers have also explored spatial as well as temporal self-referencing based side-channel analysis to improve the de-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2015.2449231, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

tection sensitivity or eliminate the need of golden ICs. In [38], a self-referencing approach that compares transient current signatures between two circuit blocks (similar or dissimilar) is proposed. The approach however requires a set of golden chips to effectively eliminate process variations. In [39], a golden-free temporal self-referencing approach is proposed to identify HT effect in current signature by comparing transient current waveforms from two different time windows. However, it only targets sequential designs and sequential HT circuits. A recently reported self-referencing approach [40] compares path delays between similar paths to observe HT-induced deviation. Although it eliminates the need of golden chips, it requires the original netlist for test generation and is likely to suffer from reduced detection sensitivity for HTs which have negligible impact on critical path delays. Another golden-free scheme is presented in [41] in which fingerprint of original ICs is extracted from Monte-Carlo simulation with realistic process variations. It depends on accurate model of process variations which may be difficult to obtain. Furthermore, none of these approaches target detection of recycled counterfeit chips.

B. Motivation

Modern digital ICs usually include many similar (or symmetric) structures over multiple levels of hierarchy. Fig. 3 shows an example architecture of a multi-core superscalar processor with structural self-similarity at multiple levels, e.g., across cores, functional units (FUs), and sub-circuits of FUs (e.g., full adder). Such structural self-similarity can be observed in other chips e.g., graphics engine, Digital Signal Processors (DSPs), many application-specific integrated circuits (ASICs), as well as memory subsystem (e.g., SRAM, DRAM and FLASH) with hierarchically regular blocks [42]. In addition, custom and reconfigurable hardware accelerators (e.g., image encoder/decoder, filtering units, security engine) are often designed based on a systolic array e.g., coarse-grained reconfigurable architectures (CGRAs), with identical sub-structures [43]. Finally, Modern SoC designs are often datapath dominant, where datapath elements with high degree of replication take most of the die area, as opposed to control logic. Hence, there is high probability that the signals in these regions can be used to design HTs (e.g., triggers or payload). Thus, an HT detection approach targeting these regions can provide high coverage. Moreover, existing approaches that aim at detecting HT in sequential logic including control logic [39] can be effectively combined to provide comprehensive HT coverage. The possible attacks and limitations of SeMIA are analyzed in detail in Section VII-A.

We note that such intrinsic structural self-similarity provides opportunity for efficient golden-free IC integrity analysis in presence of process noise. Based on this observation, we have developed the proposed approach, SeMIA, for IC integrity analysis. In SeMIA, we consider comparison of I_{DDT} instead of path delay or I_{DDQ}. This is because it allows: (1) selectively activating small region of logic circuits, which improves detection sensitivity compared to I_{DDQ} based approaches; (2) easier vector generation compared to path delay based approaches; and (3) better HT coverage than both I_{DDQ} and

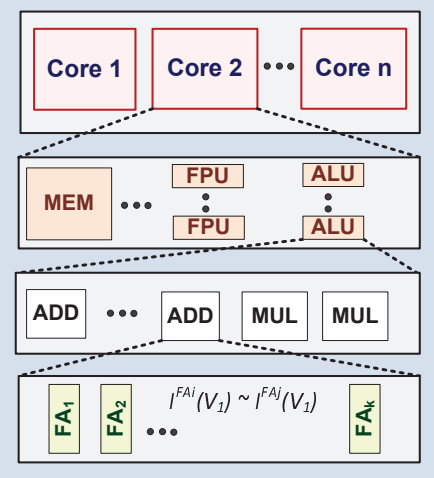

Fig. 3. Structural self-similarity in a multi-core processor can be observed at different levels of hierarchy.

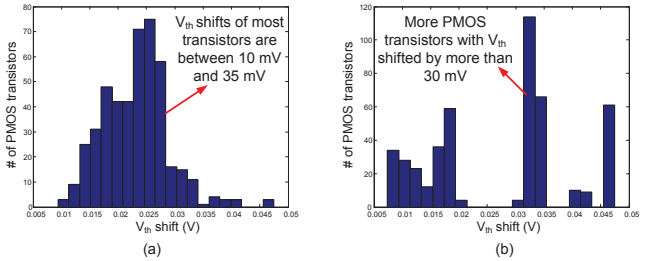

Fig. 4. The histogram of V_{th} shift in a 32-bit carry lookahead adder for one-year aging: (a) lower 16-bit part, and (b) upper 16-bit part.

delay-based approaches, since many HT circuits may not cause appreciable change in these parameters.

The key idea in SeMIA is to compare I_{DDT} between two identical structures and observe deviation due to HT attacks or aging effects. It is worth noting that, the I_{DDT} in similar modules should be virtually identical in the absence of process variations. If an HT is inserted into module i', the I_{DDT} would deviate from that in the original module i under certain test vector pair that induces higher HT activity. On the other hand, in a recycled chip, PMOS transistors in each structure would have different stress/recovery duration depending on application scenarios (that change input workload or vectors), thus experiencing variable NBTI-induced V_{th} shifts. We used MOSRA tool in Hspice to observe NBTI effect in a 32-bit CLA. Since typically more than 50% operands in a processor for benchmark applications are narrow-width [19], upper 16-bit of the inputs are most often all zero or all one. It is well-known that the distribution of V_{th} shift is dependent on the workload [20]. To simulate the scenario, we applied 16-bit random inputs with high activity (0.5) to the lower 16-bit, while all-zero and all-one with low activity (0.2) to the upper 16-bit. From Fig. 4, we can observe a significant difference in V_{th} increase between the upper and lower 16-bit logic of the CLA for one-year aging. On the other hand, major components of process variations (inter-die and intra-die systematic) induce uniform shift in V_{th}. Hence, I_{DDT} can be used to isolate aged chip under process variations by observing the nature of V_{th} shift in two similar and adjacent structures.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2015.2449231, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

III. Problem Formulation and Analysis

In this section, first we analyze ways to reduce the masking effect due to process variations. Then we describe the IC integrity validation problem that eliminates the need of golden chips.

A. Process Variation Mitigation

The correlation of I_{DDT} from similar and adjacent circuit structures can be employed to distinguish between the genuine and recycled/HT-affected chips. We consider both inter-die and intra-die V_{th} variations in a CMOS process. 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 random and systematic V_{th} shifts across 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 sensitized by test vector pair j are in set $G_{i,j}$. According to [44], 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 $\gamma_g = \alpha (V_{DD} - V_{th}^{(c)})^{\alpha - 1}$. Assume module i' is adjacent to module i and the activated gates are in set $G_{i',j}^{(c)}$. We can obtain the following relationship:

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

$S_{rand} = \sum_{g \in G_{i,j}} \beta_g \gamma_g \Delta V_{th}^{(c,g)} - \sum_{g \in G_{i',j}} \beta_g \gamma_g \Delta V_{th}^{(c,g)}$ 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 between adjacent similar modules. The summation and hence averaging on S_{rand} helps to mitigate the effects of intra-die random variation, assuming considerable (e.g., $10 - 25$) number of gates switch simultaneously. Under no intra-die variation, module i and i' should generate nearly the same I_{DDT} for a transition induced by test vector pair j. Hence, the trend line of (3) will be $y = x$. From (3), 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 effects lead to deviation from the trend line.

B. Golden-free Integrity Analysis

Based on availability of symmetric structures in a chip, we formulate the problem of golden-free detection of aged or HT-affected chips. The effect of non-uniform aging on I_{DDT} of a module pair $\{i, i'\}$ can be modeled as $S_{aged} = \sum_{g \in G_{i,j}} \beta_g \gamma_g \delta V_{th}^{(c,g)} - \sum_{g \in G_{i',j}} \beta_g \gamma_g \delta V_{th}^{(c,g)}$, 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 can be incorporated into (3) as:

$$I^{(c)}(G_{i',j}) = I^{(c)}(G_{i,j}) + S_{rand} + S_{aged} \quad (4)$$

The detection of recycled chip is formulated as isolating S_{aged} in (4). Assume $d_{i,j}^{(c)}$ is the distance from point $(I^{(c)}(G_{i,j}), I^{(c)}(G_{i',j}))$ to the trend line $y = x$. With the increase of S_{aged}, $d_{i,j}^{(c)}$ becomes larger.

Next, let us consider the modification of (3) in the presence of HT in module i'. The activity of HT can increase the average I_{DDT} by $I^{(c)}(HT_{i',j})$ as shown in (5), where $HT_{i',j}$ denotes the gates in HT circuit activated by test vector pair j in module i'.

$$I^{(c)}(G_{i',j}) = I^{(c)}(G_{i,j}) + I^{(c)}(HT_{i',j}) + S_{rand} \quad (5)$$

The detection of HT is formulated as isolating $I^{(c)}(HT_{i',j})$ in (5). Clearly, $I^{(c)}(HT_{i',j})$ contributes to the increase of $d_{i,j}^{(c)}$.

The common effect of HT and unbalanced aging profile in I_{DDT} is the deviation from the trend line, which can be considered as a unified objective in the proposed framework to detect these attacks. Intuitively, if $d_{i,j}^{(c)}$ is large enough, we can infer with high confidence that the circuit under test has an integrity violation, e.g., affected by either an unbalanced aging profile or an HT. Fig. 5 illustrates the calculation of $d_{i,j}^{(c)}$. The point (x_j, y_j) is obtained by solving:

$$\begin{cases} y = x \\ y = -x + I^{(c)}(G_{i,j}) + I^{(c)}(G_{i',j}) \end{cases}$$

as $x_j = y_j = (1/2)(I^{(c)}(G_{i,j}) + I^{(c)}(G_{i',j}))$. As a result, $|I^{(c)}(G_{i,j}) - x_j| = |I^{(c)}(G_{i',j}) - y_j| = |(1/2)(I^{(c)}(G_{i',j}) - I^{(c)}(G_{i,j}))|$. Considering the sign, it can be derived that

$$d_{i,j}^{(c)} = (\sqrt{2}/2)(I^{(c)}(G_{i',j}) - I^{(c)}(G_{i,j})) \quad (6)$$

Combining (3), (4) and (5) for only process variation, unbalanced aging profile and HT, we can obtain that

$$d_{i,j}^{(c)} = \begin{cases} S_{rand}(G_{i,j}, G_{i',j}) \\ S_{rand}(G_{i,j}, G_{i',j}) + S_{aged} \\ S_{rand}(G_{i,j}, G_{i',j}) + I^{(c)}(HT_{i',j}) \end{cases} \quad (7)$$

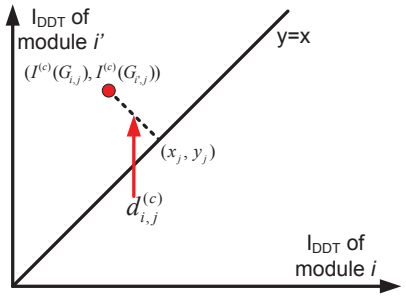

Fig. 5. The distance $d_{i,j}^{(c)}$ from the trend line is used to determine both an HT and aging effects.

The mathematical expectation of $d_{i,j}^{(c)}$ (denoted as $E(d_{i,j}^{(c)})$) is zero with only $S_{rand}(G_{i,j}, G_{i',j})$ for a genuine chip. However, it becomes nonzero in the presence of unbalanced aging

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2015.2449231, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

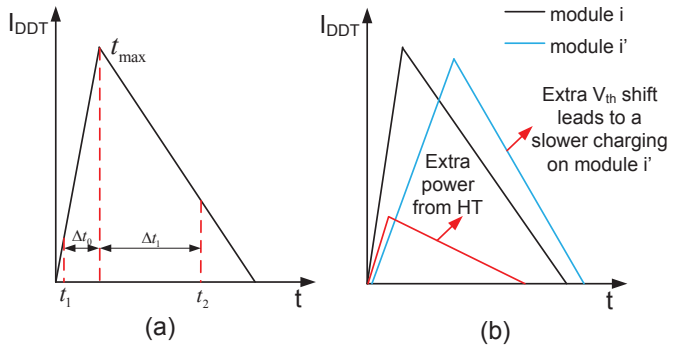

Fig. 6. (a) An appropriate TW to measure average I_{DDT}, and (b) shift in TW with V_{th} change due to aging.

profile or HT. $E(d_{i,j}^{(c)})$ should be estimated with only a suspect chip (i.e., no golden chips). Note that $E(d_{i,j}) = 0$ holds for all the test vector pairs. We consider T test vector pairs $j = 1, 2, ...T$ with little or no overlap in switching gates, and calculate $E(d_{i,j}^{(c)})$ in a chip by self-referencing as:

$$E(d_{i,j}^{(c)}) = \sum_{j=1}^{T} d_{i,j}^{(c)} / \sqrt{I^{(c)}(G_{i,j})^2 + I^{(c)}(G_{i',j})^2} \quad (8)$$

where $d_{i,j}^{(c)} / \sqrt{I^{(c)}(G_{i,j})^2 + I^{(c)}(G_{i',j})^2}$ mitigates the difference on nominal I_{DDT} for different test vector pairs. Hence, the detection problem is formalized as:

$$auth_c = \begin{cases} recycled\ or\ HT & if\ \ |E(d_{i,j}^{(c)})| > Th \\ authentic & otherwise \end{cases} \quad (9)$$

where Th is an acceptable limit. It basically reflects the residue of intra-die random variations that cannot be eliminated through averaging over multiple-gate switching. Th can be obtained through Monte-Carlo simulation under different intra-die process variations, which requires no actual measurement on golden chips or measurement of variations from a set of chips under test. To improve accuracy, we can enhance the sensitivity of S_{aged} and $I^{(c)}(HT_j)$ to I_{DDT} of similar and adjacent module i and i', as described in Section IV-A. SeMIA, however, cannot further differentiate a recycled chip from HT-affected one when $|E(d_{i,j}^{(c)})| > Th$.

IV. Methodology

In this section, we discuss the I_{DDT} measurement process to increase the sensitivity to unbalanced aging profile or HT activity. Next we describe the golden-free procedure to check the integrity of chips through I_{DDT} analysis.

A. I_{DDT} Measurement

We consider the time window (TW) for I_{DDT} measurement as well as the influence from V_{DD}, to maximize the sensitivity to HT and unbalanced aging profile. The location and size of a TW should be selected properly when measuring the average value of I_{DDT}. Fig. 6(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

$$\begin{aligned} &min\ \ t_1 - t_0 \\ &s.t. \int_{t_0}^{t_1} I_{DDT}(t)dt \geq \eta V_{DD} C_{L,t} \end{aligned} \quad (10)$$

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 (10), we minimize $t_1 - t_0$ to increase the sensitivity of I_{DDT} to V_{th}. Algorithm A is proposed to implement (10). In Step 1, t_{max} is the time when the maximum transient current $I_{DDT}^{(i)}(t_{max})$ occurs. Hence, $t_0 = t_{max} - \Delta t_0$ and $t_1 = t_{max} + \Delta t_1$ are employed to form an appropriate TW for computing average I_{DDT} in Steps 2-4.

Fig. 6(b) shows the I_{DDT} shape of module pair $\{i, i'\}$ with different aging profiles for the same test vector pair. The gates activated in module i' have larger V_{th} shift. Hence, I_{DDT} of $\{i, i'\}$ (blue and black triangle) in Fig. 6(b) do not completely overlap, creating a small shift in the time of the maximum I_{DDT} and the charge/discharge duration. If the TW of module i' is changed to track such shift, the average I_{DDT} may only show small discrepancy from that in module i. Hence, the difference of V_{th} shift is not fully reflected on I_{DDT} measurement.

Algorithm A: Measure Avg. 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 $I^{(c)}(G_{i',j})$

To address it, the computation of average I_{DDT} in Step 3-4 is based on the same TW obtained in Step 2 to enhance the difference. Next, we consider the effectiveness of Algorithm A on HT detection. As shown in Fig. 6(b), if an HT in module i' is sensitized, most power is concentrated in the TW of module i or i' (as observed in Hspice simulation). Hence, the power discrepancy due to HT can also be enhanced following the steps in Algorithm A.

V_{DD} affects I_{DDT}, and thus the effectiveness of Algorithm A. The charging duration $t_2 - t_1$ can be approximately

$$(t_2 - t_1) \propto \frac{C_{L,t} V_{DD}}{\beta (V_{DD} - V_{th})^{\alpha}} \quad (11)$$

In (11), the increase in V_{DD} leads to smaller $t_2 - t_1$. Hence, dynamic power is more concentrated around the time with the maximum I_{DDT}. The effectiveness of Step 3-4 in Algorithm A is therefore enhanced with the increase of V_{DD} until it achieves a certain value. Δt decreases with a larger V_{DD} ($\Delta t \to 0$ as $V_{DD} \to \infty$). For a given TW, the influence of V_{DD} on detecting recycled chip is shown through Hspice simulations and FPGA experiments in Section V.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2015.2449231, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

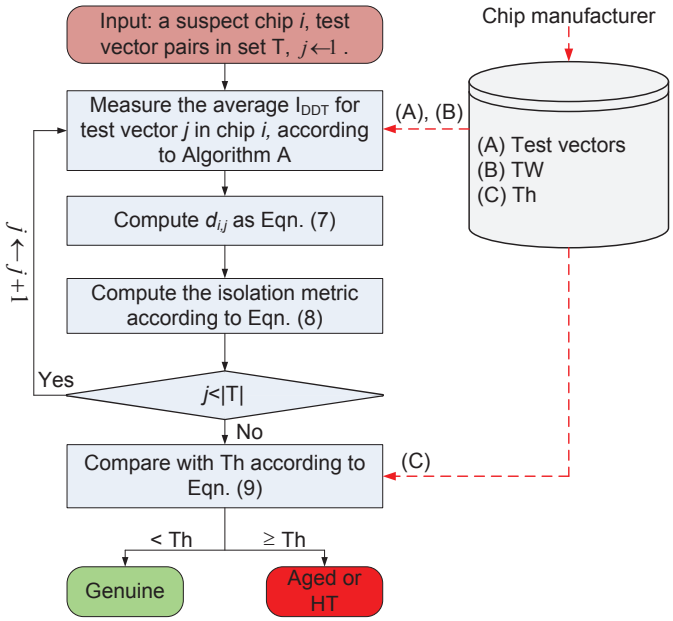

Fig. 7. The proposed IC integrity validation procedure without golden chips.

B. Overall Procedure

The procedure for the proposed unified integrity validation is shown in Fig. 7. We assume that a chip designer would derive the optimal test vectors, TW, and V_{DD} to activate similar modules and measure corresponding I_{DDT}s. We employ a region-based test vector generation approach as described in [35]. The test vector pairs in SeMIA should activate nearly independent set of gates with minimum overlap across vector pairs to ensure the high HT coverage. This vector set can be reused for recycled chip identification. Such test vectors can be derived from random patterns, based on the metric $F = max(inRegionActivity - outRegionActivity)$. For example, we decompose a datapath module into different regions and find vectors that can activate considerably more gates (leading to much larger I_{DDT}) in certain region than that outside it. An acceptable limit Th needs to be obtained through Monte-Carlo simulations using realistic process variation model. This information is made available to system designers for chip authentication. Since no golden chip is needed for the authentication process, the test workload for chip/system designers is significantly reduced.

During authentication of a suspect chip i, a system designer needs to measure the average I_{DDT} under the given TW and given test vector set T. Then I_{DDT} values are used to compute $d_{i,j}$ in (6). Based on the $d_{i,j}$ from all the test vector pairs in T, the isolation metric $E(d_{i,j}^{(c)})$ is computed according to (8). Finally, as described in (9), chip i is judged as not genuine, if $|E(d_{i,j}^{(c)})|$ is larger than the threshold Th. It is worth noting that the calculation of isolation metric does not require the process variation information from the chip manufacturer/designer unlike alternative approaches [45]. It makes SeMIA easier to employ during post-manufacturing test or system integration.

V. Simulation Results

In this section, we evaluate the effectiveness of SeMIA with respect to detecting both aged and HT-affected chips through circuit-level simulations.

A. Simulation Setup

The simulation is carried out in Hspice at 45nm CMOS process [46]. The process variation is modeled as 15% inter-die and 10% random intra-die variation on V_{th} following a Gaussian distribution. 16 test vector pairs are prepared to measure average I_{DDT} according to Algorithm A. Assuming equal probability for genuine and recycled/HT chips, we calculate $Pr(hit,\ recycled/HT)$ and $Pr(reject,\ new)$ to obtain the error rate e.

The transistor-level netlists of 32-bit CLA and 32-bit equality comparator are used as benchmark, since they are common in modern digital circuits. MOSRA tool integrated with Hspice is employed 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 activity (e.g., 0.2), while the lower 16-bit has the random vectors with high activity (e.g., 0.5). We simulate 200 genuine adders (and comparators) under the process variation, as well as two aged versions with one-year and five-year usage. An appropriate TW is selected for I_{DDT} measurement according to Algorithm A. The procedure of SeMIA in Fig. 7 is executed to obtain the $E(d_{i,j}^{(c)})$ of each chip and we make a judgment using (9).

We consider small combinational HTs for a 32-bit CLA and an 8-bit array multiplier. The HT is inserted into the lower 16-bit part of the adder, referenced with the upper 16-bit part. An HT-free 8-bit multiplier is used to reference the multiplier with HT. After the designs are synthesized by Design Compiler (DC), we note that the HTs take only 2.1% and 1.6% area of the adder and multiplier, respectively.

B. Analysis for Recycled Chip Detection

For one-year aging, the histograms of V_{th} shift in the adder and equality comparator are shown in Fig. 4 and Fig. 8, respectively. 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 for the lower and upper parts have different histograms and thus a recycled version can be isolated. For a given test vector pair, the correlation of average I_{DDT} for upper/lower 16-bit part in the adder and comparator is shown in Fig. 9. The points of recycled chips are slightly lower than that of genuine chips as in Algorithm A. Hence, $\{d_{i,j}^{(c)}\}$ of recycled chip has a different distribution. Fig. 10 shows the histograms of $\{d_{i,j}^{(c)}\}$ for the genuine adder and comparator. They follow the Gaussian distribution that matches the derivation in Section III-B and the mean value of $\{d_{i,j}^{(c)}\}$ is zero.

Fig. 11 shows that the isolation metrics of aged chips can be clearly separated from that of genuine chips. Th is set as 1.06×10^{-2} and 8.75×10^{-3} to minimize e as 2.5% and 2.25% for the adder and comparator under V_{DD} =1.0 V. For five-year

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2015.2449231, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

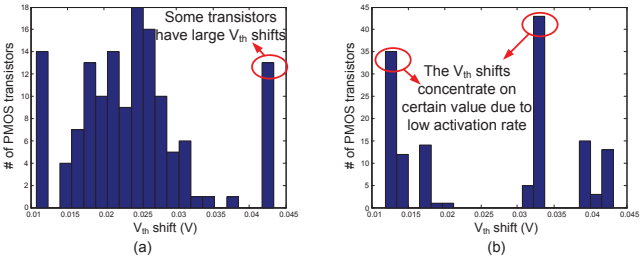

Fig. 8. The V_{th} shifts of comparator used for one year: (a) lower 16-bit part, (b) upper 16-bit part.

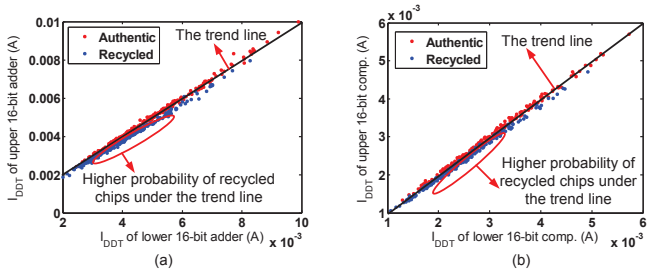

Fig. 9. I_{DDT} correlation for (a) the adder, and (b) the comparator.

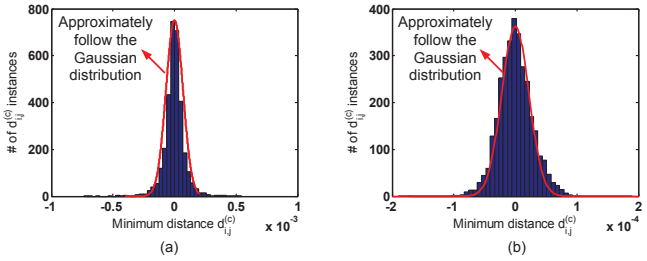

Fig. 10. The histogram of $\{d_{i,j}^{(c)}\}$ for (a) the adder, and (b) the comparator in authentic chips.

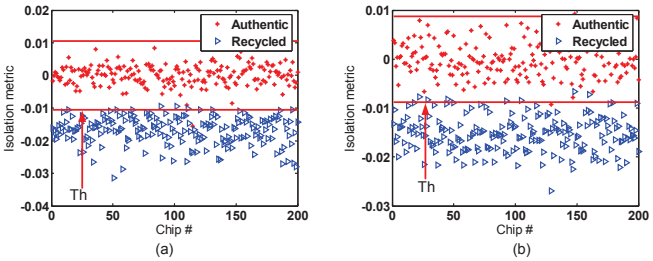

Fig. 11. The isolation metrics of 200 authentic chips and 200 used (for one year) chips: (a) the adder, and (b) the comparator.

usage, e is further reduced to 0.25% and 0.5%, respectively. Hence, SeMIA works effectively to identify recycled chips. Moreover, e is reduced with more usage duration. It is useful for recycled-chip detection, since it provides higher confidence in detecting more severely aged chips, which impose more serious reliability concerns when used.

V_{DD} affects the sensitivity of I_{DDT} to unbalanced aging profile. The average I_{DDT} is measured under different V_{DD} after one-year aging. Fig. 12 shows that when V_{DD} becomes 1.1 V and 0.9 V, e rises up to 14.3% and 4.3% for the adder, which are 6.8% and 6.0% for the comparator. Hence, it is helpful to select a proper value of V_{DD} for each circuit structure to achieve a smaller e. This can be done by a chip designer in dynamic power analysis during design time.

C. Analysis for HT Detection

The average I_{DDT} of adder in lower 16-bit part with activated HT is larger than that without HT. Hence, $E(d_{i,j}^{(c)})$ is non-zero that leads to the HT identification as (9). In Fig. 13, we can find that the isolation metrics are obviously different for the genuine and aged chips. The values of Th are 1.06×10^{-2} and 3.1×10^{-3} for the adder and multiplier, respectively. Fig. 13 shows that even though the size of HT is small (2.1% for adder and 1.6% for multiplier), the proposed isolation metric can successfully differentiate the HT-affected chips from genuine ones. Specifically, e is 2% and 2.5% for adder and multiplier, respectively under $V_{DD} = 1$ V.

Similar to aged chip detection, e also changes with V_{DD} as shown in Fig. 14. When V_{DD} is 0.9 V and 1.1 V, e becomes 2.5% and 14.5% for the adder. However, the trend is different for the multiplier. e decreases to 2.0% for $V_{DD} = 0.9$ V, which becomes 5.0% when V_{DD} rises to 1.1 V.

D. Aging and HT Detection in DLX Processor

The proposed validation approach can be scaled to larger designs including both datapath and control logic. To demonstrate this aspect, we verified the effectiveness of SeMIA in a 5-stage pipelined processor, namely DLX. We integrated the adders with unbalanced aging profile and HTs into the EX stage of the DLX processor. To mitigate the non-negligible currents produced from control logic and other datapaths, we chose a sequence of instructions that induces transition in only one pipelined stages in each cycle. Fig. 15(a) shows an example that accurately captures I_{DDT} from 'ADD' instruction and the test vector pair $(T1, T2)$ activating the gates in the upper 16-bit of the 32-bit adder. By using the same method, the I_{DDT} from the lower 16-bit part is obtained with different operands. The background I_{DDT} from the program counter and FSM transition can be mitigated by the correlation of I_{DDT} from the upper and lower 16-bit parts. Fig. 15(b) shows the comparison of error rates for a separate adder and the adder integrated into the DLX processor. We can observe that the difference is very small under different V_{DD}s. Specifically, for $V_{DD} = 1.0$ V, the error rate of recycled detection becomes 3.5% when the adder is placed inside the DLX processor, while it is 2.5% when testing the adder separately. It demonstrates the effectiveness of SeMIA for larger designs comprising of datapath modules and control logic.

VI. Experimental Results

In this section, we validate SeMIA through experiments with a set of commercial Altera DE0 boards as shown in Fig. 16. Since these boards do not come with a current sensing mechanism, we modified them to incorporate a sense resistor (one ohm) between the V_{DD} port of the regulator and the supply input of the FPGA chips. The voltage drop across the resistor is measured by an oscilloscope to obtain the I_{DDT}

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2015.2449231, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

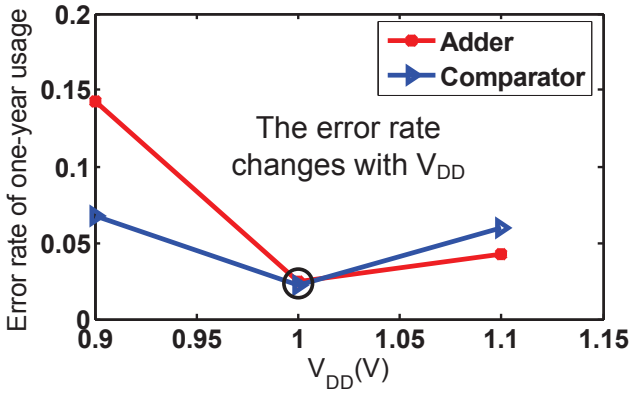

Fig. 12. In recycled chip detection, the error rate e changes for the adder and the comparator at different V_{DD}s.

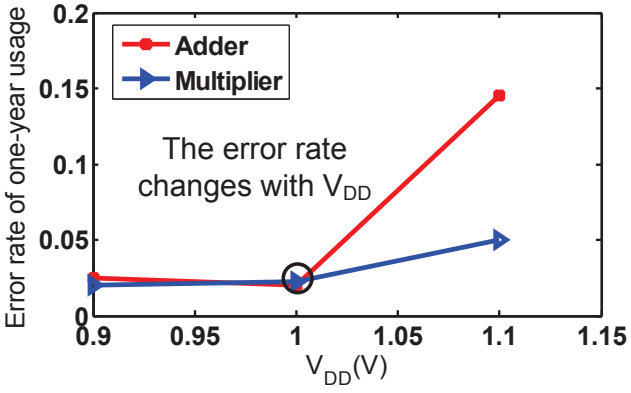

Fig. 14. In HT detection, the error rate e changes for the adder and the comparator at different V_{DD}s.

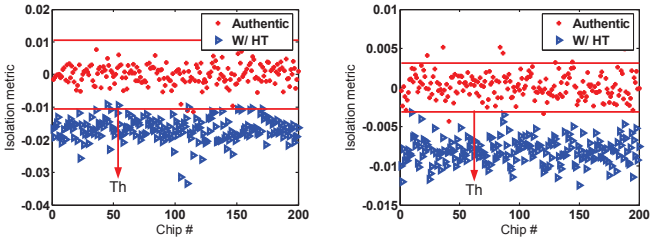

Fig. 13. Isolation metric for (a) 32-bit adder and (b) 8-bit multiplier.

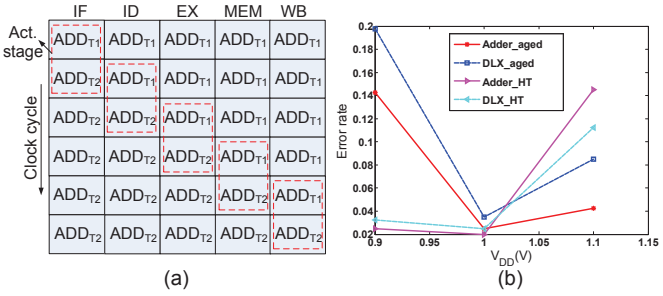

Fig. 15. (a) Activation of a pipelined stage under test vector pair $T1$ and $T2$, and (b) comparison of error rate between a separate adder and the adder integrated into DLX.

trace. The design under test (DUT) is a 32-bit array multiplier. We select a suitable TW for the test vectors to measure the average I_{DDT} according to algorithm A.

A. Analysis for Recycled Chip Detection

In our Hspice simulation, the unbalanced aging profile for one year and five years can be reliably detected by SeMIA. However, such long aging duration in an experiment is likely to cause malfunction of FPGA chips. Hence, we focus on identifying the existence of unbalanced aging in datapaths implemented in FPGAs. In our experiment, two 32-bit array multipliers (Mult1 and Mult2) were synthesized into certain regions of FPGA by the Altera Quartus-II toolset. Two chips were aged for 10, 20 and 30 hours under high temperature (55° C) and high V_{DD} (1.4 V) to observe I_{DDT} variation. The activities of test vectors applied to the two multipliers are 0.2 and 0.5, respectively, with the input frequency of 5 MHz.

After the aging on Mult1 and Mult2, we employed five test vector pairs to produce transient I_{DDT} profile under $V_{DD} = 1.2$ V and 1 MHz clock, which were captured in an oscilloscope. Algorithm A is employed to compute the average I_{DDT} denoted as $I_{DDT,1}$ and $I_{DDT,2}$. Fig. 17 shows the change of $|I_{DDT,1} - I_{DDT,2}|$ in three chips that are aged for up to 30 hours. We can find that $|I_{DDT,1} - I_{DDT,2}|$ increases rapidly with aging duration. Specifically, it achieves 0.25 mA on average after 30-hour aging, compared to only 0.1 mA before aging. For different V_{DD}s (i.e., 1.1 V and 1.3 V), we observed a similar trend. The experimental results support the existence of unbalanced aging profile under different test vectors for aging. Hence, a recycled chip with aging duration of few months or higher can be reliably identified by SeMIA.

B. Analysis for HT Detection

The platform for HT detection is shown in Fig. 18, including a phase-locked loop (PLL), a memory block, a design under test (DUT0) and its duplication with HT (DUT1). The PLL outputs a clock with frequency 10 MHz as the interval of test vector input. The memory block stores the test vectors. Signal HT_en is used to control the activation of gates in an HT. When it is 0, DUT0 and DUT1 have identical switching and no test vectors can flip the gates in the HT. As a result, the correlation of the I_{DDT} can mimic the case that no HT is inserted into DUT1. When HT_en is 1, the HT in DUT1 can be activated by certain test vectors. A test vector pair is read out from the memory and input into DUT0 and DUT1, controlled by the clock. The average I_{DDT} is measured repeatedly in an oscilloscope to eliminate the effect of temporal and measurement noises. The sequential HT [47] including a 32-bit counter takes 2.3% area of the DUT.

Fig. 19(a) and (b) show the I_{DDT} correlation of DUT0 and DUT1 for V_{DD} of 1.1 V and 1.2 V, respectively. If no HT is present, the corresponding points for ten FPGAs are scattered around the trend line $y = x$. However, when the test vectors induce switching activity in the HT, the points fall below $y = x$, which closely matches the simulation results. Fig. 19(c) and (d) show that the isolation metrics without HT are close to zero. Hence, a design with HT can be identified with negligible error rate.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2015.2449231, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

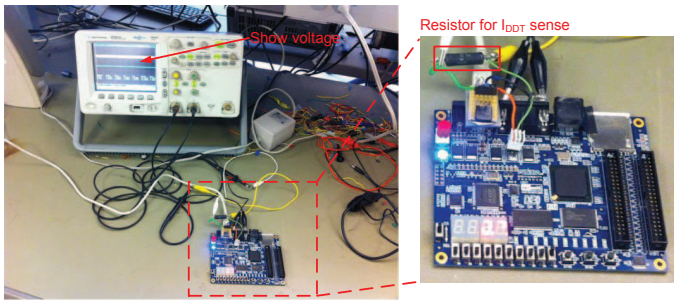

Fig. 16. The experimental platform on DE0 board.

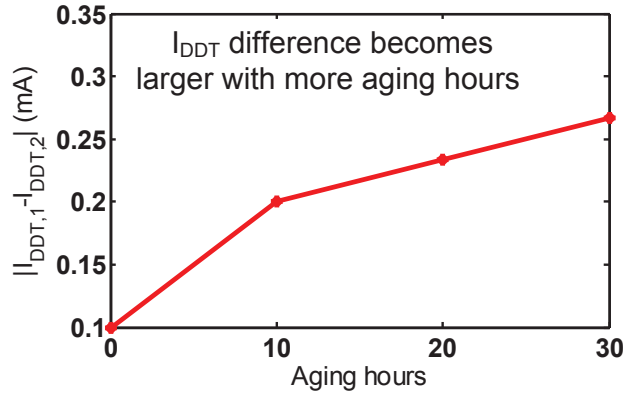

Fig. 17. I_{DDT} difference between Mult1 and Mult2 with aging duration from 10 hours to 30 hours.

VII. Discussion

A. Attacks and Countermeasures

The aging effects in recycled chips depend on the application scenario and therefore infeasible to be controlled by adversaries. It may be argued that an unbalanced aging profile can be eliminated by increasing V_{th} shift on the transistors with less aging. However, it is difficult to select proper test vectors to achieve the similar histogram of V_{th} deviation. It may not also be practically feasible to enforce balanced aging into large number of self-similar structures in a chip, e.g., a processor. Moreover, it is a complex (e.g., involving aging equipment) and expensive process, since the V_{th} should be monitored accurately in a long time.

We have focused on possible HT attacks in regular symmetric structures. If an HT is inserted into non-similar instances, it can evade detection by SeMIA. However, it is worth noting that, typically the die-area taken by modules with regularity or high degree of replication is substantial, as noted in diverse contexts [42]. Hence, SeMIA is expected to provide high HT coverage. In order to detect HT instances in random logic such as control unit of a processor, we can combine SeMIA with existing HT detection approach with complementary capabilities such as [39].

B. Extension of SeMIA

SRAM is widely incorporated into 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

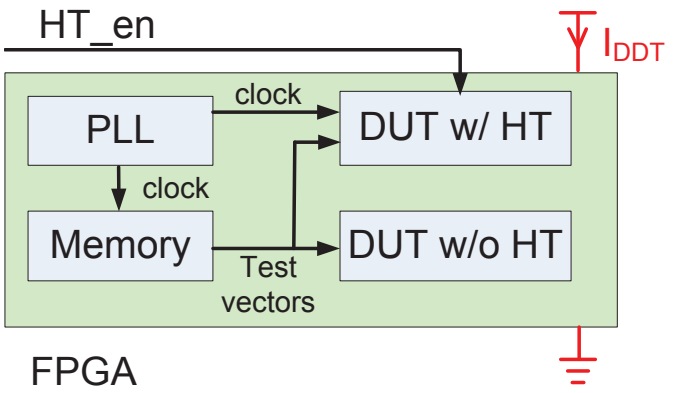

Fig. 18. The circuit structure for HT test in Cyclone-III FPGA.

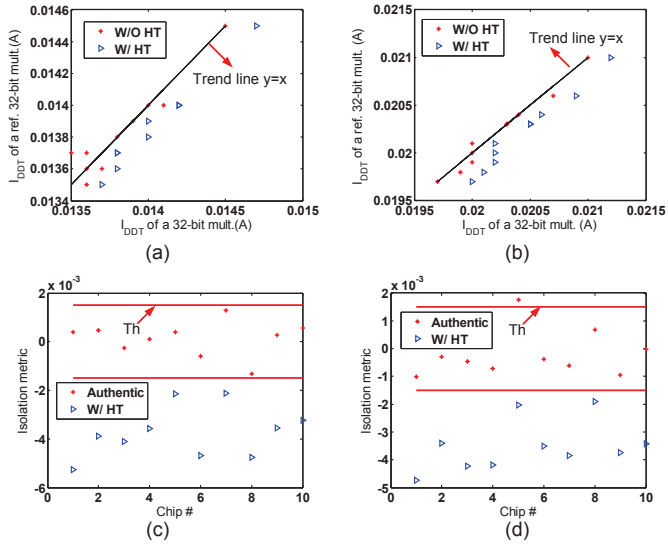

Fig. 19. (a) I_{DDT} correlation for multipliers under $V_{DD} = 1.1$ V, (b) I_{DDT} correlation for multipliers under $V_{DD} = 1.2$ V, (c) isolation metrics under $V_{DD} = 1.1$ V, and (d) isolation metrics under $V_{DD} = 1.2$ V.

in real applications [19], MSBs in a word store '0' (or '1') most of the time. The contents in LSBs are altered more frequently. Hence, the aging profile of MSBs is different from that in LSBs. Furthermore, an embedded memory usually has separate power grid that simplifies I_{DDT} measurement on memory core with reduced noise. Hence, it can be a good candidate to determine aging of a chip by employing SeMIA.

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

Finally, in addition to I_{DDT}, SeMIA can also use path delays (such as in [40]) to form the isolation metric as (8), if the test vectors for path activation are provided by the chip designer. As a result, the HTs (or aging effects) impacting path delays can be detected by SeMIA reliably.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2015.2449231, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

VIII. Conclusion

We have presented SeMIA, a golden-free methodology to detect both recycled counterfeit ICs as well as hardware Trojan attacks by exploiting the discrepancy in I_{DDT} between two self-similar structures. Using extensive simulations under realistic process variations, we have shown that it can identify these integrity issues reliably with high sensitivity. It requires no design modification and hence can be applied to legacy chips. We have also validated SeMIA through experiments in FPGA chips with example Trojan instances and practical aging profiles.

Modern complex SoCs include many regular self-similar structures at different levels of hierarchy that experience different level of stress during operation. Therefore, SeMIA can be effectively employed to isolate aged chips of varying complexity. Similarly, since a hardware Trojan attack is expected to be localized in a logic block, SeMIA can effectively work for detecting Trojan attacks in these SoCs. Since self-comparison automatically eliminates the effect of inter-die and intra-die systematic variations, it is easily scalable to large designs. When combined with complementary Trojan detection techniques such as self-referencing based Trojan detection in sequential logic, SeMIA can provide comprehensive Trojan coverage. Although we focus on I_{DDT} in our study of SeMIA, other parameters such as path delay can be applied for fingerprint construction. Furthermore, SeMIA also can work for digital signal processing units, crypto chips, as well as mixed-signal chips such as data converters and telemetry units, which increasingly use digital components of regular structure. Finally, although SeMIA does not require any design modification, design-for-security approaches that incorporate or enhance self-similarity across circuit blocks, can improve its effectiveness.

References

[1] M. Tehranipoor and F. Koushanfar, "A survey of hardware Trojan taxonomy and detection," *IEEE Design & Test of Computers*, vol. 27, no. 1, pp. 10-25, 2010.

[2] F. Wolff. C. Papachristou, S. Bhunia, and R.S. Chakraborty, "Towards Trojan-free trusted ICs: problem analysis and detection schemes," *DATE*, 2008, 1362-1365.

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

[4] R. S. Chakraborty, S. Narasimhan and S. Bhunia, "Hardware Trojan: threats and emerging solutions," *HLDVT*, 2009, pp. 166-171.

[5] U. Guin, M. Tehranipoor, D. DiMase and M. Megrdichian, "Counterfeit IC detection and challenges ahead," *ACM SIGDA*, March 2013.

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

[7] Counterfeit IC detection, Integra Technologies Inc., [Online] http://www.integra-tech.com/index.php/test-services/counterfeit

[8] SENTRY Counterfeit IC Detector, ABI Electronic Inc., [Online] http://www.abielectronics.co.uk/Products/SENTRYCounterfeitICDetector.php

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

[10] J. Rajendran, Y. Pino, O. Sinanoglu and R. Karri, "Logic encryption: a fault analysis perspective," *DATE*, 2012.

[11] A. Basak, Y. Zheng and S. Bhunia, 'Active defense against counterfeiting attacks through robust antifuse-based on-chip locks," *VTS*, 2014, pp. 1-6.

[12] U. Guin, X. Zhang, D. Forte, and M. Tehranipoor, "Low-cost On-Chip Structures for Combating Die and IC Recycling," *DAC*, 2014, pp. 1-6.

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

[14] Y. Zheng, X. Wang and S. Bhunia, "SACCI: scan-based characterization through clock phase sweep for counterfeit chip detection," *IEEE Trans. on VLSI systems (TVLSI)*, vol. 23, no. 5, pp. 831-841, 2015.

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

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

[17] K. Huang, J. M. Carulli and Y. Makris, "Parametric counterfeit IC detection via support vector machines," *DFT*, 2012, pp. 7-12.

[18] S. Bhunia, M. Hsiao, M. Banga and S. Narasimhan, "Hardware Trojan attacks: threat analysis and countermeasures," *Proceeding of the IEEE*, vol. 102, no. 8, pp. 1229-1247, 2014.

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

[20] H. Kukner *et al.*, "Degradation analysis of datapath logic subblocks under NBTI aging in FinFET Technolgy," Int. Sym. on Quality Electronic Design (ISQED), 2014, pp. 473-479.

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

[22] X. Wang, M. Tehranipoor and J. Plusquellic, "Detecting malicious inclusions in secure hardware: challenges and solutions," *HOST*, 2008, pp. 15-19.

[23] H. Salmani, M. Tehranipoor and J. Plusquellic, "New design strategy for improving hardware Trojan detection and reducing Trojan activation time," *HOST*, 2009, pp. 66-73.

[24] J. Li and J. Lach, "At-speed delay characterization for IC authentication and Trojan horse detection," *HOST*, 2008, pp. 8-14.

[25] X. Zhang and M. Tehranipoor, "RON: an on-chip ring oscillator network for hardware Trojan detection," *DATE*, 2011, pp. 1-6.

[26] J. Rajendran, V. Jyothi, O. Sinanoglu and R. Karri, "Design and analysis of ring oscillator based design-for-trust technique," *VTS*, 2011, pp. 105-110.

[27] R. S. Chakraborty, S. Paul and S. Bhunia, "On-demand transparency for improving hardware Trojan detectability," *HOST*, 2008, pp. 48-50.

[28] C. Lamech and J. Plusquellic, "Trojan detection based on delay variations measured using a high-precision, low-overhead embedded test structure," *HOST*, 2012, pp. 75-82.

[29] Y. Cao, C. H. Chang and S. Chen, "A cluster-based distributed active current sensing circuit for hardware Trojan detection," *IEEE Trans. on Info. Froensics and Security*, 2014.

[30] K. Xiao and M. Tehranipoor, "BISA: Built-in self-authentication for preventing hardware Trojan insertion," *HOST*, 2013, pp. 45-50.

[31] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi and B. Sunar, "Trojan detection using IC fingerprinting," *IEEE Symp. Security Privacy*, 2007, pp. 296-310.

[32] Y. Jin and Y. Makris, "Hardware Trojan detection using path delay fingerprint," *HOST*, 2008, pp. 51-57.

[33] Y. Alkabani and F. Koushanfar, "Consistency-based characterization for IC Trojan detection," *ICCAD*, 2009, pp. 123-127.

[34] S. Wei, S. Meguerdichian and M. Potkonjak, "Gate-level characterization: foundation and hardware security applications," *DAC*, 2010, pp. 222-227.

[35] M. Banga and M. S. Hsiao, "A region based approach for the identification of hardware Trojan," *HOST*, 2008, pp. 43-50.

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

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

[38] D. Du, S. Narasimhan, R. S. Chakraborty and S. Bhunia, "Self-referencing: a scalable side-channel approach for hardware Trojan detection," *CHES*, 2010, pp. 173-187.

[39] S. Narasimhan *et al.,* "TeSR: A Robust Temporal Self-Referencing Approach for Hardware Trojan Detection," *HOST*, 2011, pp. 71-74.

[40] N. Yoshimizu, "Hardware Trojan detection by symmetry breaking in path delays," *HOST*, 2014, pp. 107-111.

[41] Y. Liu, K. Huang and Y. Makris, "Hardware Trojan detection through golden chip-free statistical side-channel fingerprint," *DAC*, 2014, pp. 1-6.

[42] P. Subramanyan, N. Tsiskaridze, K. Pasricha, D. Reisman, A. Susnea and S. Malik, "Reverse engineering digital circuits using functional analysis," *DATE*, 2013, pp. 1277-1280.

[43] K. K. Parhi, "VLSI Digital Signal Processing Systems: Design and Implementation," Wiley, first ed., 1999.

[44] T. Sakurai and A. R. Newton, "Alpha-power law MOSFET model and its applications to CMOS inverter delay and other formulas," *JSSC*, vol. 25, no. 2, pp. 584-594, 1990.

[45] Y. Zheng, A. Basak and S. Bhunia, "CACI: Dynamic current analysis towards robust recycled chip identification," *DAC*, 2014, pp. 1-6.

[46] Predictive Technology Model, [Online] http://ptm.asu.edu/
[47] X. Wang, S. Narasimhan, T. Mal-Sarkar and S. Bhunia, "Sequential hardware Trojan: side-channel aware design and placement," *ICCD*, 2011, pp. 297-300.