SACCI: Scan-Based Characterization Through Clock Phase Sweep for Counterfeit Chip Detection

Yu Zheng, Student Member, IEEE, Xinmu Wang, and Swarup Bhunia, Senior Member, IEEE

Abstract—Counterfeit chips in a supply chain have emerged as a major security concern in the semiconductor industry with serious potential consequences (such as performance degradation, revenue, and reputation loss). With rising incidences of this attack, widespread effort has been made in both industry and academia to develop effective countermeasures. However, existing solutions to protect against these attacks suffer from both robustness issue (in terms of detecting chips with minor functional/structural deviations) as well as design/area overhead and test cost. In addition, they cannot reliably detect different forms of cloning attacks. In this paper, we propose a novel characterization method to identify counterfeit chips—in particular, the cloned ones—based on extraction of scan path delay signatures of a chip. It uses the scan chain, a prevalent design-for-testability structure, to create a robust authentication signature. The proposed approach has two major advantages: 1) it comes at virtually zero design and hardware overhead, since it does not require any additional embedded structure; and 2) it alleviates the design house from characterizing each manufactured chip instance, thus mitigating test cost. In addition, a novel and practical method based on clock phase sweep is proposed to measure delay of short scan paths with high resolution. Using Monte Carlo simulation on the layouts of two ISCAS-89 benchmarks at 45-nm CMOS process, we observe that over 99% of counterfeit chips can be reliably identified even under large process variations. Effectiveness of the approach is also validated with delay measurements in field programmable gate array chips.

Index Terms—Cloned chip, counterfeit chip detection, design-for-test, fake chip, process variations, scan chain.

I. INTRODUCTION

A COUNTERFEIT chip is an electronic component with discrepancy on the material, performance, or characteristics, but sold as a genuine chip. A counterfeit chip can be an unauthorized copy, remarked/recycled die, cloned design, or failed real part [1]. In 2012, the annual loss is estimated as $169 billion, which may rise to $1.2–1.7 trillion in 2015 [1], [2]. In addition to the revenue and reputation loss to the IC manufacturers, a counterfeit chip in electronic equipment may lead to severe consequences with potentially degraded quality, reliability, and performance [3]. As a result, counterfeit chips in a supply chain pose a major problem to manufacturers, system designers, and end users.

Existing industry-standard methods and tools to detect counterfeit chips, such as tools from Integra Technologies, Inc. and ABI Electronics Ltd. [4], [5], primarily depend on functional or parametric tests, which may not be effective in detecting minor deviations in functionality, parameters, or structure. To address the problem, new countermeasures are emerging from academia and industry. According to Koushanfar et al [3], intrinsic light emission can be captured by high sensitivity photon detectors to enhance undesired modification of a circuit. However, the optical instrument named Light Emission from OFF-State Leakage Current (LEOSLC) incurs high test complexity and cost. The active metering approach that provides remote control of a design for authentication has been explored to prevent counterfeiting attacks [6]. However, it requires design modifications and adds to the design overhead and cost. For detecting used (e.g., remarked/recycled) chip, an aging sensor can be implanted into the chip to track the change of threshold voltage [7]. It can work for only isolating aged chips and comes at a cost of additional design effort and hardware overhead. Aged chips can also be detected by monitoring side-channel parameters (e.g., quiescent supply current or path delay) under voltage or temperature-induced stress [8]. Physical unclonable function (PUF), such as ring-oscillator PUF [9], has been considered as an effective mechanism for identifying counterfeit chips by producing unique signature for chip authentication. However, in addition to the hardware/design cost of embedded PUF structure, it increases the test workload by forcing a design house to generate unique signatures for each chip post-fabrication. In addition, both PUF and aging sensors cannot authenticate a chip already in the market.

Counterfeit chips can be broadly classified into two major types. The first type has functional discrepancy (e.g., remarking, mis-specification). The second type has identical function but comes with discrepancy in circuit parameters (e.g., path delay). The second type of counterfeiting attacks can be mounted in two possible ways: 1) cloning of a design (generally obtained through stealing or reverse engineering) that incorporates structural integrity violations; and 2) reselling of aged chips as new. Among them, cloning attacks impose significant challenge in detecting them due to: 1) functional equivalence of the counterfeit chips, which makes functional validation ineffective; and 2) minor structural variations lead to modest change in circuit parameters often masked under process noise. Commercial tools for counterfeit detection, such as the ones in [4] and [5] cannot typically cover...
these attacks. Furthermore, the cloning attacks are not widely addressed in open literatures. There is a critical need to explore low-overhead robust methodology for detecting cloned chips in a supply chain.

In this paper, we propose a novel counterfeit chip detection approach to address different forms of counterfeiting attacks related to cloning of a design at various stages of IC life cycle. The proposed approach, referred as scan-based authentication for counterfeit chip identification (SACCI), utilizes the scan chain, a prevalent design-for-testability (DFT) structure, for chip authentication. As illustrated in Fig. 1, the scan path delays are measured on a small number of authentic chips (e.g., $d_{1,1}$ and $d_{2,1}$ for chip 1 and chip 2), which can be carried out by the IC manufacturer. Function $\text{sig}(\cdot)$ is derived to generate a reference set of scalar signatures of authentic chips and an acceptable deviation for counterfeit detection. By using existing on-chip structure, it alleviates the design overhead associated with alternative anticontrolfeiting approaches (e.g., PUF-based solutions) and reduces test cost due to the need to characterize only a small number of chips by a design house.

To model counterfeiting attacks that introduce minor structural deviations, we change the layouts for two benchmark circuits from the ISCAS-89 suite by imposing different area or timing constraints on layout. We consider realistic process models with different variation scenarios (up to 16.7% and 33.4% overall standard deviation on effective channel length $L_{\text{eff}}$ and threshold voltage $V_{th}$). A parallel scan path delay measurement (PSDM) method is proposed to measure small delay of scan paths with high resolution. We observe that over 99% counterfeit chips can be accurately characterized even under large process variations. We have also implemented PSDM based on clock phase sweep with low overhead to evaluate the effectiveness of SACCI using field programmable gate arrays (FPGAs). By incremental compilation on the original design in Quartus II, we emulate the counterfeit chips which experience minor deviations in layout. The experiment on 16 FPGAs shows that SACCI can work with high confidence under intrinsic process variations for 65-nm CMOS process. In particular, this paper makes the following major contributions.

1) It analyzes the counterfeiting attacks where chips experience structural integrity violations (leading to commensurate deviations in circuit parameters) and formalizes the counterfeit chip detection problem for such attacks.

2) It proposes a scan path delay characterization-based counterfeit chip detection approach that can reliably identify cloning attacks. The proposed approach helps in assuring trust of ICs acquired through a supply chain without requiring design modifications (hence avoiding design cost and hardware overhead). It proposes a strategy to select specific path delays for signature generation. For improving detection capability, it employs principle component analysis (PCA) to characterize the process noise and reduce the deviation of scan-path delay due to interdie and systematic intradie process variations. It also presents an effective isolation metric to generate stable signature and acceptable range of deviations.

3) PSDM is proposed to measure scan path delays and implemented based on clock phase sweep. It avoids the requirement for high-frequency clock at high resolution. Through FPGA experiments, it can successfully measure the delay of short paths (e.g., < 1 ns) with high resolution (e.g., 11 ps in 7-series FPGA of Xilinx [25]).

The rest of this paper is organized as follows. Section II describes different types of cloning attacks considered in this paper; and related work on IC authentication. Section III presents the method of path selection to achieve effective chip authentication and formulates the counterfeit chip detection problem. Section IV describes SACCI methodology. Simulation results are presented in Section V. Section VI presents the FPGA emulation results. Section VII discusses attacks on SACCI. We conclude in Section VIII.

II. COUNTERFEITING ATTACKS AND SCOPE OF THIS PAPER

In this paper, we address the cloning attacks. The left part of Fig. 2 shows a simplified life-cycle of chip that includes RTL synthesis, layout design (e.g., GDSII file) and manufacturing in foundry. We note that cloning attacks can occur at all steps. For example, an attacker may copy the RTL code in design house and use his/her own tool to complete synthesis, layout and then choose a foundry and process to manufacture counterfeit chips.
A. Scope of This Paper

The scope of counterfeit attacks based on cloning of a design is shown in the right part of Fig. 2.

1) **Type A**: Copy an RTL IP (soft IP) and fabricate a chip using the same or a different process.
2) **Type B**: Copy a gate-level IP (i.e., firm IP) and fabricate a chip using the same or a different process.
3) **Type C**: Reverse-engineer an authentic chip (ASIC or FPGA), reconstruct the design and fabricate a counterfeit chip using the same or different process.
4) **Type D**: Copy a GDSII file from a design house or foundry and fabricate with a different process or the same process at a later time (assuming the process evolves over time).

The counterfeit chips of Types A–D are functionally equivalent with the authentic chips. Types A–C would usually have different nominal path delays from the original one. It is because different synthesis/layout tools or scripts may be employed for Types A and B. In Type C, with increasing complexity of modern chips, it is extremely difficult for an attacker to obtain exact chip layout through reverse engineering process. For Type D, the counterfeit chips are manufactured by a process with different parameter ($V_{th}$ and $L_{eff}$) variations. It can also be a case of overproduced chips. The proposed approach, however, cannot detect overproduced chips using identical process. Such attacks, however, are less likely since a foundry is expected to prevent them to avoid possible reputation loss.

B. Related Work on IC Authentication

The scan chain has been considered as a source of watermarking to protect IPs. In [10], synthesis of specific set of registers are forced or restricted to appear by adding new design constraints. Besides extra hardware overhead, it, however, may impact testability of scan chain, such as fault coverage. Cui and Chang [11] explore the reordering of scan flip-flops (SFFs) in scan chain for watermarking with minimized test power and cost. Both [10] and [11] require modifications during design cycle and cannot protect the chips in the market, which are not equipped with watermarking. In [12], the path delay is measured and transformed to digital signature for chip authentication. However, extra shadow registers and an alternative clock tree need to be inserted into the original design, which may increase area/power overhead significantly. In [13], scan chain is employed to implement PUF with ultralow overhead. It needs an embedded structure named clock delay line to insert a short cycle into clock for signature generation. In addition, it cannot be applied in the chips in the market.

III. PATH SELECTION FOR COUNTERFEIT DETECTION

A. Which Paths Are Suitable?

To create difficult-to-clone identity of chips, we need to select path delays which are difficult to clone by an attacker. We note that, in general, number of noncritical short paths exponentially grows with the scale of chip. It can be prohibitively difficult for existing EDA tools to adjust the nominal delay of large number of noncritical paths to desired value. Manually adjusting all path delays on the layout is infeasible as the number of paths increases significantly. In addition, a minor modification on a short path can lead to a large percentage delay deviation. In this paper, we generate layout of s9234 and s35932 benchmark circuits from ISCAS-89 suite and perform minor deviations in the area or timing constraint to obtain layout variants. The discrepancy percent for path $j$ between the original and the modified layout is defined as $|D_{j}^{\text{mod}} - D_{j}^{\text{ori}}| / D_{j}^{\text{ori}}$ where $D_{j}^{\text{ori}}$ and $D_{j}^{\text{mod}}$ are the nominal delays of path $j$. We compute the discrepancy percents of 380 noncritical paths in s9234 (2719 for s35932) reported by Synopsys’s PrimeTime Tool. Fig. 3 shows that the discrepancy percent decreases with increasing nominal delay. Hence, it is reasonable to use delay of short paths to reliably detect counterfeit chips.

B. Why Scan Paths?

As an industrial DFT standard, scan chain is popularly inserted into most chips. Most of scan paths are noncritical ones with small delay, since either no gates or a few buffers are typically inserted. The number of scan paths is often large and scan paths are globally distributed in a chip. In addition, the delay measurement of scan path is much simpler than conventional at-speed scan testing on combinational paths [14]. This is due to the following two reasons: 1) it avoids the difficulty of test vector generation by an ATPG tool for combinational path sensitization; and 2) it eliminates the need of fast switching on the scan enable signal or enhanced-scan architecture in order to achieve high combinational path delay coverage. Hence, it is attractive to use scan path delays to authenticate a chip.

It may be argued that scan paths would have less diversity in nominal delay and hence less entropy. However,
we observe that the structure of the scan paths varies significantly depending on the layout. The scan cells are placed in a way that scan paths would have varying contributions of gate delay, interconnect delay as well as distributed R-C parasitics. Hence, an aggregation of scan path delays can provide high entropy.

Since scan paths are typically shorter than functional ones, there may be concern on precise delay characterization of these paths. Note that even though SFFs may have physical proximity, scan path delays cannot be very small to avoid hold timing violations, a common problem for scan chains [15]. Usually designers target keeping good hold margin (typically by inserting buffers) for scan paths to avoid zero-yield scenario due to inability to perform structural test on scan failure.

To prevent scan-based attacks on cryptographic cores, in some chips scan chains are physically disconnected by fuse or antifuse devices after manufacturing test [16]. This is, however, not a common practice since it prevents in-field test and debug. A viable alternative is to allow scan-out process after a validation process (e.g., using a special input sequence [17]), which would enable the scan-based characterization.

C. Problem Formulation

Assume the genuine and counterfeit chips are in sets $G$ and $C$, respectively. For chip $i$ in $G$ (or $C$), the delay of scan path $j$ is $d_{i,j}^{(G)}$ (or $d_{i,j}^{(C)}$)

$$
\begin{align*}
    d_{i,j}^{(G)} &= D_{i,j}^{(G)} + \Delta d_{i,j}^{(G)} \\
    d_{i,j}^{(C)} &= D_{i,j}^{(C)} + \Delta D_{i,j}^{(C)} + \Delta d_{i,j}^{(C)} 
\end{align*}
$$

where $D_{i,j}^{(G)}$ is the nominal delay of path $j$; $\Delta D_{i,j}^{(C)}$ is the discrepancy on the nominal delay of scan path $j$ between $G$ and $C$; $\Delta d_{i,j}^{(C)}$ and $\Delta d_{i,j}^{(G)}$ are the noise induced by process variation. In Types A–C, $\Delta D_{i,j}^{(C)} \neq 0$ is satisfied due to various causes, such as different synthesis/layout tools or restrictions (e.g., timing or area). In Type D, $\Delta d_{i,j}^{(C)}$ and $\Delta d_{i,j}^{(G)}$ are the random variables with different probability density functions (PDFs). Hence, the counterfeit detection is formalized as identifying $\Delta D_{i,j}^{(C)} \neq 0$ and/or different distribution between $\Delta d_{i,j}^{(G)}$ and $\Delta d_{i,j}^{(C)}$ in the presence of process variations.

IV. SACCI: METHODOLOGY

The major steps in SACCI are shown in Fig. 4. Both the chip manufacturer and system designer need to participate in this scheme. Post manufacturing, the chip manufacturer selects a specific set of scan paths. Path delays for the selected scan paths are measured on a small number of authentic chips (set $G$). After characterizing process noise, an isolation metric for each chip is calculated to identify an acceptable range specified by $\text{Th}_C$ for authentic chip. Characterization process by the chip manufacturer leads to storing three types of information in a database: 1) locations of selected scan paths; 2) process noise; and 3) $\text{Th}_C$. A system designer can access this database to authenticate suspect chips (in set $U$). During authentication, a system designer measures the delays of the select scan paths. The process noise is greatly reduced and the isolation metric for each chip is created. The chips in $U$ with isolation metric outside $\text{Th}_C$ are judged as counterfeit.

A. Scan Path Selection Method

Usually, a modern chip includes a large set of scan paths in the scan chain. For example, Alpha processor contains up to 2408 D flip-flops (DFFs) (i.e., up to 2407 scan paths) [18]. Measuring all scan path delays would incur long test time and large hardware resource (e.g., large memory to store the delay values). To address this issue, a chip manufacturer can only select a set of scan paths. The goal is to choose a set of paths that provides large discrepancy in nominal delay between the genuine and counterfeit chips, as shown in Fig. 3. It, in turn, improves the detection accuracy. The locations of selected scan paths are stored in a database to be used by a system designer for chip authentication.

B. Delay Measurement Method

The scan chain works as a shift register in scan mode that can be employed to develop the PSDM on the selected scan paths. A SFF is realized by adding a 2:1 multiplexor to the input of DFF. In Fig. 5(a), the output of SFF $j - 1$ is connected with the SD port of SFF $j$, $j = 1, 2, \ldots$, by setting signal TD as 1. Hence, the scan chain works in scan mode. The output of SFF $j$ is initialized as 0. It becomes 1 at the rising edge $t$ to generate $0 \rightarrow 1$ transition on scan path $j$. After the interval of $t_{\text{meas}}$, the rising edge $t+1$ shows in the clock of Fig. 5(b). Ignoring the uncertain window in Fig. 5(b) due to the setup and hold timing violation, the output of SFF $j + 1$ of chip $i$ in $G$ (same to $C$) can be simplified as

$$
O_{i,j+1}^{(G)} = \begin{cases} 
1 & t_{\text{meas}} \geq d_{i,j}^{(G)} \\
0 & \text{otherwise}
\end{cases}
$$

We can use two clocks with tunable phase difference to insert a delay-measurement cycle and change $t_{\text{meas}}$ as described in Section VI-B. Assume $t_{\text{meas}}$ starts from an initial
Fig. 5. (a) Structure of typical scan paths and (b) creating a clock pulse with period $t_{\text{meas}}$ for scan path delay measurement.

Algorithm 1 Procedure of PSDM

**Input:** The selected $N_{\text{path}}$ scan paths.

**Initialization:**

- $t_{\text{meas}} \leftarrow t_{\text{init}}$, $sw_{\text{num}} \leftarrow 0$ and $k \leftarrow 0$
- while ($sw_{\text{num}} < N_{\text{path}}$)
  
  - Generate $0 \rightarrow 1$ transition on all selected scan paths after the rising edge $t$.
  - Produce the rising edge $t+1$ after $t_{\text{meas}}$.
  - Identify $sw_k$ new switch points.
  - $sw_{\text{num}} \leftarrow sw_{\text{num}} + sw_k$
  - $t_{\text{meas}} \leftarrow t_{\text{meas}} + \Delta t$
  - $k \leftarrow k + 1$

**end of while**

**Output:** Path delays as (3)

value $t_{\text{init}}$ and the resolution of $t_{\text{meas}}$ is $\Delta t$. $k$ is called the switch point of scan path $j$, if $t_{\text{meas}} = t_{\text{init}} + (k - 1) \Delta t$ and $t_{\text{meas}} = t_{\text{init}} + k \Delta t$ lead to $O_{i,j+1} = 0$ and $O_{i,j+1} = 1$, respectively. The delay of path $j$ is estimated as

$$d_j^{(0)} = t_{\text{init}} + (k - 0.5) \Delta t.$$

(3)

Note $0 \rightarrow 1$ transition occurs on the selected scan paths to measure the delay in parallel, which reduces the test time significantly. The measurement can be repeated to average out the effect of the setup/hold timing violation and environmental noises, such as supply fluctuations.

The procedure of PSDM is shown in Algorithm 1 including multiple iterations. The $t_{\text{init}}$ is smaller than all the scan path delays. In iteration $k$, the delay-measurement cycle of $t_{\text{meas}}$ identifies $sw_k$ switch points among $N_{\text{path}}$ selected scan paths. The switch-point number $sw_{\text{num}}$ is increased by $sw_k$. If $sw_{\text{num}}$ is less than $N_{\text{path}}$, it goes into a next iteration with $k \leftarrow k + 1$ and $t_{\text{meas}} \leftarrow t_{\text{meas}} + \Delta t$; otherwise Algorithm 1 ends and computes the delays as (3).

C. Process Noise Characterization

The process-induced device parameter variations in chips can be classified into interdie, systematic intradie, and random intradie components. The effect of variation in $V_{\text{th}}$ and $L_{\text{eff}}$ on the path delay refers to [19]–[21]. The standard deviation of path delay is primarily due to the interdie process variation [22]. For Types A–C, interdie deviation can largely mask the discrepancy on the nominal delay between the genuine and counterfeit chip. Fig. 6 shows that the delay shift due to interdie variation has a larger standard deviation than that with intradie variation. Hence, the probability to detect $\Delta D_j^{(C)}$ becomes smaller. Similarly, in Type D, the difference on path delay variation due to different process variation parameters can be masked by interdie variations.

The interdie variation on device parameters is shared by all the transistors on the same die and varies from die to die. The systematic intradie variation is spatially correlated [20]. We can employ PCA to extract such characteristics from the scan path delays of chips in $G$ [23]. Assume $d_j^{(G)} = [d_{i,1}^{(G)}, d_{i,2}^{(G)}, \ldots, d_{i,N_{\text{path}}}^{(G)}]^T$. Employing PCA on matrix $[d_1^{(G)}, \ldots, d_{|G|}^{(G)}]$ of $|G|$ chips, the $l$th eigenvector $(1 \leq l \leq N_{\text{path}})$ is $\xi_l$ with the eigenvalues in the descending order. The vector projection of $d_j^{(G)}$ on $\xi_l$ is $(d_j^{(G)} \cdot \xi_l)\xi_l$, where $\cdot$ is inner product. We choose the first $p$ eigenvectors and update $d_j^{(G)}$ as

$$d_j^{(G)} \leftarrow d_j^{(G)} - \sum_{l=1}^{p} (d_j^{(G)} \cdot \xi_l)\xi_l.$$  

(4)

The updated elements of $d_j^{(G)}$ mitigate the effect of interdie and systematic intradie variations. The PDFs of scan path delays are estimated as $\{f_j(x)\}$, $j = 1, 2, \ldots, N_{\text{path}}$.

The vectors $\{\xi_l\}$ and PDFs $\{f_j(x)\}$ are the process noise information in Fig. 4. They are stored in the database for authenticating suspected chips. An advantage is that the nominal delay of each selected scan path is not shown in $\{\xi_l\}$ and $\{f_j(x)\}$. Hence, attacker cannot obtain them directly which helps in enhancing the security of SACCI.

D. Isolation Metric and Acceptable Range

An isolation metric is derived for a chip based on $f_j(x)$. We formulate the likelihood of $d_{i,j}^{(G)}$ under $f_j(x)$ as

$$\log(1/f_j(d_{i,j}^{(G)})),$$  

similar to the Shannon entropy in information theory [24]. If $d_{i,j}^{(G)}$ corresponds to a rare event,
\log_10(1/f(d_{ij}(G))) \text{ becomes a large value, which indicates small probability of its occurrence. We consider } N_{\text{path}} \text{ scan paths to have equal weight and hence, the isolation metric of chip } i \text{ in } G \text{ can be derived as }

\[ \text{sig}_i(G) = \frac{\sum_{j=1}^{N_{\text{path}}} \log_10(f_j(d_{ij}(G)))}{N_{\text{path}}} \] (5)

\text{sig}_i(G) \neq \text{sig}_i(G) \text{ due to process noise. Short scan paths are more susceptible to random variations. However, by using a large set of scan paths (e.g., 200 paths, as described in Section V) for creating the isolation metric through a summation process as in (5), the effect of random intradie variations is considerably mitigated. Define } \text{sig}(G) = \sum_{i=1}^{G} |\text{sig}_i(G)| \text{ and Var}(G) = \sum_{i=1}^{G} (\text{sig}_i(G) - \text{sig}(G))^2 / (G-1). \text{ Var}(G) \text{ increases with process variation. The acceptable range of authentic chip is defined as } \Delta t_C = [\text{sig}(G) - \gamma \cdot \sqrt{\text{Var}(G)}, \text{sig}(G) + \gamma \cdot \sqrt{\text{Var}(G)}], \text{ where } \gamma \text{ is a tunable parameter. As shown in Fig. 4, } \Delta t_C \text{ is stored in the database for authentication.}

E. Chip Authentication

System designer measures the scan path delays using PSDM described in Section IV-B. The delays of chip } i \text{ in set } U \text{ (suspect chips under test) are denoted by } d_{ij}(U). \text{ The process noise information of authentic chips in the database is employed as }

\[ d_{ij}(U) = d_{ij} - \sum_{l=1}^{p} (d_{lj}(U) \cdot \xi_i l). \] (6)

The signature of } \text{sig}_i(U) \text{ is computed as (5). If it falls within } \Delta t_C, \text{ it is judged as an authentic chip in } G \text{ (hit); otherwise a counterfeit chip in } C \text{ (reject). Hence, the authentication of chip } i \text{ is }

\[ \text{auth}_i = \begin{cases} \text{hit if } \text{sig}_i(U) \text{ in } \Delta t_C \\ \\ \text{reject otherwise.} \end{cases} \] (7)

V. Simulation Results and Analysis

In this section, we analyze the effectiveness of SACC in presence of different levels of process variations.

A. Simulation Setup

Synopsys Design Compiler and Cadence Encounter tools are used for synthesis and layout design, respectively. We use the same gate-level netlist after synthesis and modify the area and timing constraints (e.g., clock period) to generate the counterfeit layouts for Types A–C attacks. For Type D attacks, we use the original circuit with different process variation parameters. Two designs (s9234 and s35932) from the benchmark suite ISCAS-89 that represent small and large-scale circuits are considered to validate SACC. The baseline layouts are s9234base and s35932base. The counterfeit layouts s9234c1 and s35932c1 are obtained by changing area; s9234c2 and s35932c2 are generated by changing the timing constraints. We use PrimeTime to extract the scan path delays from the layouts. Fig. 7 shows the discrepancy on 200 selected scan paths. The average discrepancy percents

![Fig. 7. Nominal delay deviations for 200 scan paths in case of counterfeit layouts. (a) s9234c1. (b) s9234c2. (c) s35932c1. (d) s35932c2.](image)

![TABLE I](image)

![Fig. 8. Delay of scan path 1 in Case 1 for (a) s9234base and (b) s35932base.](image)
rate \( h \) as the conditional probability \( \Pr(\text{hit} \mid \text{fake}) \), and the false reject rate \( r \) as the conditional probability \( \Pr(\text{reject} \mid \text{genuine}) \).
In particular, when counterfeit chips (e.g., s9234c1, s9234c2, s35932c1, s35932c2) are in \( U \), \( h \) is evaluated as \( \frac{n_h}{|U|} \), where \( n_h \) is the number of hits. Similarly, \( r \) is \( \frac{n_r}{|U|} \), where \( n_r \) is the number of rejects, when genuine chips (e.g., s9234base and s35932base) are in \( U \). A small \( h \) and \( r \) would represent good performance.

### B. Study of Types A–C Attacks

Using Monte Carlo simulation, we generate 250 chips in \( G \) and 1000 chips in \( U \), for the process corners in Table I. The 200 paths in Fig. 7 are considered while generating signature.

Fig. 9(a) and (b) shows the signatures after the process noise mitigation based on PCA for s9234base in \( G \) and s9234c1 in \( U \) under Case 1 (and Case 3). It is observed that the signatures in \( G \) and \( U \) can be isolated successfully, while separation is more clearly visible for the smaller process variation in Case 3. Fig. 9(c) and (d) shows that the signatures of \( G \) and \( U \) overlap without employing PCA. Hence, PCA-based process noise mitigation is essential in SACCI for robust detection of counterfeit chips.

### C. Study of Type D Attack

In Type D attack, an attacker copies the authentic layout, but manufactures the chips in a process with different \( \sigma \) and \( \sigma' \), which leads to discrepancy on scan path delay distribution. The process corner of authentic chips is fixed as Case 1 and counterfeit chips at other corners. Fig. 12 shows the trend in change of \( h \) with increasing deviations in

Finally, we consider the influence of process variations on characterizing nominal delay discrepancy. s9234base and s9234c2 are manufactured under Case 2 and Case 1–3, respectively. In Fig. 11, \( h \) is the smallest under Case 1. Due to larger process noises, the counterfeit chips in Case 1 result in higher discrepancy statistically in scan path delays from authentic ones in Case 2, which in turn reduces \( h \). However, such difference is reduced for counterfeit chips in Case 3 and hence, \( h \) increases.

### Tables

#### Table II

<table>
<thead>
<tr>
<th>Case 1</th>
<th>Case 2</th>
<th>Case 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>h</td>
<td>0.034</td>
<td>0.003</td>
</tr>
<tr>
<td>r</td>
<td>0.002</td>
<td>0.002</td>
</tr>
<tr>
<td>h</td>
<td>0.076</td>
<td>0.015</td>
</tr>
</tbody>
</table>

#### Table III

<table>
<thead>
<tr>
<th>Case 1</th>
<th>Case 2</th>
<th>Case 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>h</td>
<td>0.018</td>
<td>0.000</td>
</tr>
<tr>
<td>r</td>
<td>0.000</td>
<td>0.000</td>
</tr>
<tr>
<td>h</td>
<td>0.000</td>
<td>0.000</td>
</tr>
</tbody>
</table>

Fig. 10. \( h \) and \( r \) with different \( N_{\text{path}} \) for (a) s9234c2 and (b) s35932c1.
process corner with \( \sigma \) effective in detecting counterfeit chips with identical layouts. Hence, SACCI can be for s9234base. It reaches zero for Case 4, because the chips for placement of extra buffers between DFF1 and DFF2 in s9234.

![Image](image.png)

Fig. 12. \( h \) for the same layout in different cases of process variations.

\( \sigma_{L,t} \) for s9234base and s35932base. Case 4 represents a new process corner with \( \sigma_{L,t} = 7\% \). In general, \( h \) decreases as the discrepancy in process variation increases. For the counterfeit chips under Case 2, \( h \) is nearly 100%, since Case 1 and Case 2 are very close in terms of process variations. As we can observe, \( h \) reduces sharply with increasing change of \( \sigma_{L,t} \). For the counterfeit chips under Case 3, \( h \) is reduced to <20% for s9234base. It reaches zero for Case 4, because the chips have very different isolation metrics. Hence, SACCI can be effective in detecting counterfeit chips with identical layouts but fabricated in two different processes/foundries.

VI. FPGA EMULATION RESULTS

In this section, we employ FPGA to emulate the authentic and counterfeit chip (Types A–C). PSDM is realized to measure the scan path delays. SACCI is observed to correctly detect the counterfeit chips under realistic process variations.

A. Counterfeit Chip Model in FPGA

Fig. 13(a) shows the procedure of generating configuration file to emulate authentic and counterfeit chip in FPGA. In Step 1, we compile the design (e.g., s9234) under a certain timing constraint and map it into FPGA as an authentic chip. To emulate the counterfeit chip, we incrementally compile the authentic netlist in Step 2, after inserting a buffer (two inverters) into certain scan paths. Fig. 13(b) shows an example of such buffer between SFF1 and SFF2. In Step 3, the inserted buffer in Step 2 is deleted and the netlist is incrementally recompiled and mapped into an FPGA as a counterfeit chip.

B. Architecture of PSDM

The clock sweeping technology (frequency sweep) has been earlier employed to measure path delay for delay testing [26]. The method may be ineffective to measure delay of a short path. For example, the clock frequency of Cyclone III can be maximum 500 MHz [27], which means the scan paths with delay <2 ns cannot be measured. Hence, it is not suitable for SACCI, which needs delay measurement of short path. The proposed architecture of PSDM generates the delay-measurement cycle of small period \( t_{\text{meas}} \) by the phase difference of two clocks running at low frequency. \( t_{\text{meas}} \) is tuned with the resolution \( \Delta t \) (e.g., 11 ps in 7-series FPGAs of Xilinx [25]) by sweeping the phase shift of one clock. Similar clock phase difference has been employed earlier in glitchy-clock for fault injection attack in [28].

Fig. 14(a) shows an architecture of PSDM, which can be realized off-chip or in the chip under test. The PLL outputs clock c0, c1, and c2 of period \( t_{\text{ori}} \). The phase of c1 is tunable, while the phases of c0 and c2 are fixed. The components in the shadowed area work under c2. The c0 and c1 are the inputs of clock-switch module to produce c3 as the clock of the design under test (DUT). The phase shift controller outputs the signals with the timing required by the PLL to change the phase of c1. The main controller manipulates sweeping of the phase of c1 in Algorithm 1. Test sequence generator produces the sequence of alternate 0 and 1 into the scan chain of the DUT to generate 0 → 1 transition on the scan paths. The switch point of each scan path can be identified by the switch detector, which is stored into a memory to estimate the delay as in (3).

Fig. 14(b) shows the generation of a delay-measurement cycle of period \( t_{\text{meas}} \) into c3 in an iteration of Algorithm 1. c2 is a delayed version of c0 by \( 0.5t_{\text{ori}} \). The signal sel_c2 is synchronized with the rising edge of c2. Initially, it is set to logic level 0. Hence, sel is also 0 that allows c0 to pass through the multiplexer. After the rising edge A2 of c2, the main controller sets sel_c2 to logic level 1. The rising edge A0 of c0 generates the rising edge A3 of c3 and then c3 holds 1. In addition, A0 triggers the DFF in the clock-switch module to sample sel_c2. As a result, sel becomes 1 after a small delay due to the select signal of the multiplexor [red line in Fig. 14(a)]. Then, c1 passes through the multiplexor to reset c3 to 0. With the arrival of the rising edge A1 of c1, c3 becomes 1 again that generates the rising edge A4. Hence, two rising edges (A3 and A4) in c3 create a cycle of period \( t_{\text{meas}} \). After A4, sel_c2 becomes 0 and c0 passes the multiplexor for a new iteration with \( t_{\text{meas}} \rightarrow t_{\text{meas}} + \Delta t \), if not all switch points are found.

Next, we discuss the achievable range of \( t_{\text{meas}} \). Assume the delay between A0 and the time that sel becomes 1 is \( t_{\text{min}} \). \( t_d > t_{\text{min}} \) should be satisfied to pass A1 to c3 in the delay-measurement cycle, which requires \( t_{\text{meas}} > t_{\text{min}} \) in PSDM. In addition, to correctly store the results after A4 into the memory under c2, \( t_{\text{meas}} \) should be less than \( t_{\text{ori}}/2 \).
The hardware resources of PSDM in Cyclone III (3C16F484C6) include 126 logic elements (<1% of total 15408 logic elements), and 2048 memory bits (<1% of total 516096 bits). The memory bits are used to store the switch points as shown in Fig. 14(a). Hence, PSDM is a low-complexity component which is suitable to be integrated on chip to facilitate authentication.

C. Measurement Results

We have synthesized s9234 with PSDM under the timing constraint as an instance of authentic design. Following the steps in Fig. 13(a), a counterfeit design can be obtained. We emulate 16 authentic/counterfeit chips in 16 Cyclone-III FPGAs (under 65-nm CMOS process) on Altera DE0 boards. The nominal scan path delays of authentic design as obtained from Altera Quartus II tool range between 1.5 and 5 ns. $t_{ori}$ is configured as $\frac{1}{17.64MHz} = 56.7$ns. Hence, all the scan paths can be measured successfully. The resolution of dynamic phase shift in PLL is 0.097 ns (1/8th of the VCO period 0.777 ns). In our experiment, the initial $t_{meas}$ of the authentic design is 0.482 ns and thus the scan paths of the delay larger than that can be measured during the phase sweep of clock c1. We observe that the measured shortest scan path in the genuine design is 1.1 ns.

To validate SACCI, we choose 22 scan paths in the authentic and counterfeit design with up to 2% difference on nominal delay. The initial $t_{meas}$ in (3) of PSDM between authentic and counterfeit chips is different due to Steps 2 and 3. The delays $d_{i,j}^{(G)} - d_{i,1}^{(G)}$ and $d_{i,j}^{(C)} - d_{i,1}^{(C)}$, $i = 1, 2, \ldots, 16$ and $j = 2, \ldots, 22$, are input into SACCI to eliminate such effect. Fig. 15(a) shows that the signature can correctly isolate the counterfeit chips. From Fig. 15(b), we observe that without PCA, the signatures of authentic chips largely overlap with those of counterfeit ones, thus preventing detection.

VII. ATTACKS ON SACCI

The signature of a chip produced through SACCI captures the effect of both nominal delay and delay distribution, which is related to the structure of the scan paths as well as process variation. In order to evade the proposed validation, an attacker needs to accomplish the following.

Step 1) Derive the nominal delays for all the selected scan paths by measuring delay variations across a reasonable number of authentic chips.

Step 2) Create a layout which closely meets the nominal delays and structures for all the selected scan paths.

Step 3) Fabricate counterfeit chips from the modified layout using a foundry and process to produce nearly identical path delay distributions for all the scan paths.

In the public database, a chip manufacturer publishes only the process noise information. Hence, an attacker needs to characterize nominal delays of all scan paths. Small deviations in nominal delays (~9% average discrepancy) for few scan paths would reflect well in the isolation metric and lead to accurate detection, as shown in Tables II and III. Step 2 requires an attacker to know the structure of the scan paths through reverse engineering and then to modify the layout to match them. Furthermore, since scan paths are usually short, meeting the nominal delay target with such a small discrepancy simultaneously for ~200 paths in the layout can be very challenging. Even if the nominal delays are reproduced, considerable discrepancy on the structure of scan paths will reflect strongly on the delay distribution. Finally, in Step 3 it is important to fabricate the faithfully reproduced layouts using identical process and foundry. In practice, most cloned chips in Fig. 2 would either deviate in layout or in
technology/process or in both and hence can be identified through SACCI with high confidence.

Assume Steps 2 and 3 are completed successfully on part of scan paths. We simulate s9234c1 and s35932c1 under Case 1 with \( h \) (\( N_{\text{path}} = 200 \)) shown in Fig. 16. It can be observed that even when large percent of scan paths are cloned, SACCI remains reasonably effective. Specifically, modifying 100 scan paths (50\%) in s35932c1 to mimic the nominal delay, structure and variations as in s35932b does not have any degradation in \( h \). For s9234c1, however, \( h \) degrades to some extent (from 0.3\% to 16\%).

VIII. Conclusion

We have presented an approach for counterfeit chip detection, referred to as SACCI, that utilizes scan path delay signature to identify cloned chips of different types. We have also presented an efficient low-overhead method to measure small delay variations in scan paths, which is validated with FPGA experiments. We have shown that SACCI can reliably identify counterfeit chips that incorporate minor structural or process parametric deviations through simulation and FPGA emulation for two benchmarks. It can isolate intrinsic process-induced parameter variations from counterfeiting attacks. In addition to avoiding design overhead and cost, SACCI imposes minimal additional test workload in the design house. Future work will include extension of the approach to nonscan designs and use of multiple correlated parameters (e.g., supply current) to further improve the authentication accuracy.

REFERENCES


Yu Zheng (S’12) received the B.S. degree in communication engineering and the M.S. degree in communication and information system from the University of Electronic Science and Technology of China, Chengdu, China, in 2007 and 2010, respectively. He is currently working toward the Ph.D. degree at the Department of Electrical Engineering and Computer Science, Case Western Reserve University, Cleveland, OH, USA.

His current research interests include hardware security, VLSI architecture design for communications, and signal processing.
Xinmu Wang received the Ph.D. degree in computer engineering from Qualcomm, San Diego, CA, USA, in 2014. She is a Product Security Engineer at Qualcomm Inc., San Diego, CA, USA. Her current research interests include hardware security, including hardware Trojan design and detection, design for cryptographic system side-channel attack resistance, and secure SoC.

Swarup Bhunia (M’05–SM’09) received the Ph.D. degree from Purdue University, West Lafayette, IN, USA, in 2005. He is currently a T. and A. Schroeder Associate Professor of Electrical Engineering and Computer Science with Case Western Reserve University, Cleveland, OH, USA. He has authored over 150 articles in peer-reviewed journals and premier conferences. His current research interests include low power and robust design, hardware security, and implantable electronics. Dr. Bhunia was a recipient of the National Science Foundation Career Development Award in 2011, the Semiconductor Research Corporation Technical Excellence Award in 2005, the SRC Inventor Recognition Award in 2009, and several best paper awards and best paper nominations.