An On-Chip Dynamically Obfuscated Wrapper for Protecting Supply Chain Against IP and IC Piracies

Dongrong Zhang, Xiaoxiao Wang, *Member, IEEE*, Md. Tauhidur Rahman, *Member, IEEE*, and Mark Tehranipoor, *Fellow, IEEE*

***Abstract*— With the modern semiconductor supply chain, the ownership of both intellectual property (IP) and integrated circuit (IC) cannot be guaranteed. The IP piracy may take place at the untrusted IC designer or untrusted foundry without the knowledge of the original IP owner. The untrusted foundry can also perform IC piracy with reverse engineering of GDSII, overproducing the number of ICs, and shipping out-of-spec/defective devices. A holistic solution is proposed to protect the ownership of both IP owners and IC designers. In this solution, a dynamically obfuscated wrapper for split test (DOST) and a secure split test methodology together aim at preventing IP overusing at multiple abstraction levels and enabling IC designers to fully control the production, test, and authentication processes. DOST has been implemented and validated on video graphics array-liquid crystal display, floating-point and graphics unit, Leon3, and Leon3mp benchmarks. DOST enables the structural tests in the locked mode and the functional tests in the functionally unlocked mode. The results show that the proposed method is highly robust against IP and IC piracies with an insignificant area (1.381%) and power (1.276%) overhead.**

***Index Terms*— Authentication, counterfeit, integrated circuit (IC) piracy, intellectual property (IP) piracy, overproduction, ownership certification, supply chain security.**

I. Introduction

IN MODERN semiconductor industry, time-to-market has a direct impact on the price of final products. Hence, to save time and reduce the cost, integrated circuit (IC) designers usually reuse the same intellectual property (IP) whenever possible. Like time-to-market, the manufacturing cost is also another critical cost-controlling parameter that controls the price of final products. The cost of having a sub-22-nm foundry is more than $5 billion and has been increasing over time. A change in a technology node in every two years makes it more expensive with the technology node approaching ∼10 nm [1], [2]. Therefore, it is almost impossible for most of the vertical semiconductor industries (i.e., design and fabrication are completed in the same company) to afford such high cost. To compete in the global market, the IC designers are outsourcing their designed ICs to off-shore foundries for fabricating their products.

In the horizontal business model, the IC supply chain starts at the IP owner where the IP is designed and outsourced at different abstraction levels. An IP designer outsources soft IP or hard IP core to an IC designer. The IC designer integrates different IPs from different vendors. The integrated design is outsourced for synthesis and testing to a third party to minimize the development cost. The third party sends back the GDSII file to the IC designer or sometimes directly to the foundry for the fabrication and testing of the final part. However, this horizontal semiconductor supply chain suffers from major trust issues, including both IP and IC piracies [3]–[9]. Explicitly, the IC designer can overuse the IP without the consent of the IP owner [9]. The untrusted foundry can reuse the mask, sell the original design to a third party, and send out the defective parts to make profit [1]. Furthermore, the layout of an IP or an IC can be extracted at any abstraction level by reverse engineering the GDSII [10]. Testing is performed to decide whether a fabricated chip is functioning correctly and to confirm whether the fabricated chips are within the specification. Unfortunately, the existing testing practices conducted by the foundry cannot prevent defective or pirated devices from entering market [6], [7]. Entering such chips into the market has catastrophic consequences on the economy, safety, and security of electronic systems. Those chips can underperform, fail, or bypass the security mechanisms. Therefore, one must have proper defense mechanisms so that only authentic chips enter the market. Such an assurance is challenging and expensive. There have been several approaches in the literature, which aim at bringing trust and integrity in modern semiconductor supply chain. The most effective and popular techniques are summarized in the following.

A. Split Manufacturing

Split manufacturing is proposed to ensure trust in the supply chain where a chip is partly fabricated in an untrusted foundry. Using this method, the fabrication of a chip is completed in two separate phases: the front end of line (FEOL) and the back end of line (BEOL). The FEOL and the BEOL involve the

Manuscript received February 9, 2018; revised May 11, 2018; accepted June 12, 2018. Date of publication July 26, 2018; date of current version October 23, 2018. This work was supported by the National Science Foundation of China under Grant 61631002 and Grant 61504007. *(Corresponding author: Xiaoxiao Wang.)*

D. Zhang and X. Wang are with the School of Electronics and Information Engineering, Beihang University, Beijing 100191, China (e-mail: wangxiaoxiao@buaa.edu.cn).

M. T. Rahman is with the Department of Electrical and Computer Engineering, University of Alabama in Huntsville, Huntsville, AL 35899 USA (e-mail: tauhidur.rahman@uah.edu).

M. Tehranipoor is with the Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL 32611 USA (e-mail: tehranipoor@ece.ufl.edu).

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

Digital Object Identifier 10.1109/TVLSI.2018.2850807

lower and the upper layers, respectively [11]. The FEOL layers are fabricated in an untrusted foundry where the IC designer does not reveal the full design to keep the original functionality of the circuit unknown. On the other hand, the BEOL layers are fabricated in a trusted foundry [11]–[15]. The FEOL and BEOL layers are aligned, connected, and tested by the trusted foundry as well. This method cannot prevent the IP (soft/hard) piracy performed by the IC designer although split manufacturing can prevent an untrusted foundry from overproduction. Besides, the BEOL layers can be fully or partly reverse-engineered with the knowledge of electronics design automation routing strategy [16], [17]. Therefore, the FEOL (i.e., untrusted) foundry can overproduce ICs by discovering the BEOL connections. Another limitation of this technique is that it cannot prevent defective/out-of-spec ICs entering the market if the untrusted assembly performs testing.

B. Metering/Locking

In this technique, the IC designer locks the original functionality of a chip by locking it with an on-chip private key [18]–[20]. Usually, the unique fingerprint generated by an on-chip physical unclonable function (PUF) or true random number generator (TRNG) is used to generate private and public keys [21]–[23]. There are several netlist locking/unlocking mechanisms to meter the fabricated chips in an untrusted foundry, such as hardware metering, HARPOON, logic barrier, and more [3]–[5], [24]. The major limitation of these approaches is that the IP/IC needs to be unlocked before any production test. Therefore, the defective/out-of-spec chips can be labeled as good ones and sold into the market. The untrusted party can also request extra keys (to unlock more than the licensed number of copies) by claiming that they have a lower yield than actual.

C. Secure Split Test

Secure split test (SST) is proposed to ensure the trust and integrity in a modern semiconductor supply chain by locking the original functionality of the IC [6], [7]. In SST, instead of the foundry, the IC designer decides whether an IC passes the test or not. SST is very robust against a wide range of threat models, because the SST uses both functional locking and scan locking. Therefore, an attacker cannot obtain the correct information after performing testing on an unlocked chip. The locking key is unique from chip to chip and not revealed to the foundry. The key is generated inside the chip using a TRNG. The TRNG output is used to lock both functionality and scan chains. The TRNG's value is encrypted and sent to the IC designer so that the foundry or man-in-the-middle attacker cannot reveal any information from the encrypted sequence. The foundry/assembly applies the test patterns to all locked ICs and collects the corresponding test responses. The foundry/assembly then sends the perturbed test responses, encrypted TRNG's value, and electronic chip identification (ECID) to the IC designer for test-result checking. The IC designer checks responses for all chips and decides which chip is faulty and which chip is functionally correct. Because of unique keys, each chip will have a unique response for a given input pattern. If the chip is fault-free, an activation key is sent to the foundry/assembly to activate the chip. The SST only relies on structural testing. However, functional tests, such as speed binning, need to be performed after IC unlocking. Therefore, the SST cannot completely prevent the untrusted foundry from labeling the out-of-spec (i.e., binning failure) devices as in-spec ones. Besides, the expected responses of each device under test (DUT) are uniquely encrypted by TRNG, which results in high automatic test equipment (ATE) storage and programming effort. The final limitation of the SST is that the IC designer has to check all of the test responses of each chip, which can increase the test time.

To overcome the limitations of the above-mentioned techniques, we propose a novel dynamically obfuscated wrapper for split test (DOST) to ensure the verification of IP and IC ownerships. Our proposed technique offers the following advantages.

1) It enables and supports both structural and functional tests in a locked chip. Therefore, it prevents foundry from sending defective or out-of-spec devices into the market.
2) It prevents overproduction and reverse engineering of IP/IC.
3) It is applicable for both the IP and the IC protection with hierarchical flexibility.
4) DOST adds negligible overhead.

The rest of this paper is organized as follows. The threat models are highlighted in Section II. The architecture of the proposed DOST is introduced in Section III. Section IV presents the DOST-based SST methodology. Section V discusses the protection of our proposed technique at multiple hierarchy levels. The implementation flow is presented in Section VI. The experimental results and the attack analysis are discussed in Section VII. Finally, we conclude this paper in Section VIII.

II. Threat Models and Objectives

A. Threat Models

1) *Overuse of IP:* The modern electronic system is very large and complex. The IC designer relies on the third-party IPs to reduce the development cost. The untrusted IC designer may integrate IP in unauthorized ICs without the consent of the original IP owner. An untrusted foundry with access to a designer's IP (i.e., the mask/GDSII) can reuse it in an unauthorized design. These deceitful activities result in the IP owner's revenue loss [9], [26].
2) *IC Overproduction:* An untrusted foundry can fabricate more chips than the agreed volume and sell the overproduced ICs in the gray/black market for illegal profit. [6], [7], [19].
3) *Release of Defective ICs:* The design house does not have any proof whether the fabricated chips have been appropriately tested or not. Some defective chips might exhibit the correct functionality except under rare conditions or inputs and almost impossible to identify them in the supply chain. These defective chips should be

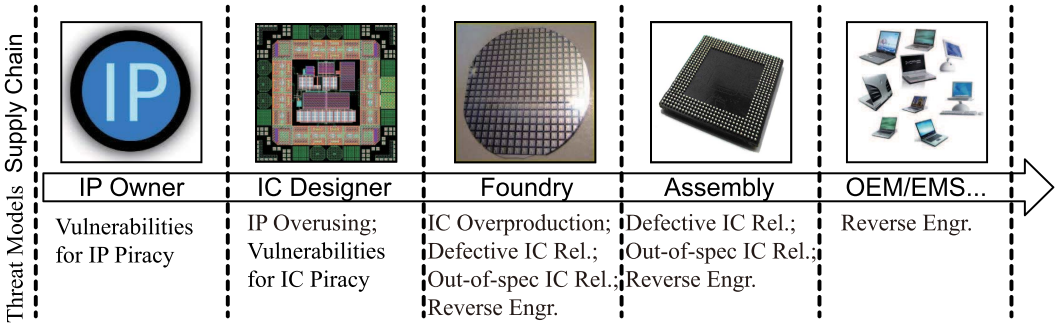

Fig. 1. Threat models distributed along the different stages of the supply chain.

TABLE I
EFFECTIVENESS OF EXISTING COUNTERMEASURES FOR ENSURING THE IP AND IC OWNERSHIPS

Countermeasure	Threats for IP		Threats for IC				IP and IC Co-protection	Cost
	Overusing	Reverse Engr.	IC Over-production	Defective IC	Out-of-spec IC	Reverse Engr.		
Split Manufacturing [11–15]	×	×	✓	×	×	×	×	Multiple Fabs Post Fabrication
Hardware Metering [3, 4]	✓	✓	×	×	×	✓	×	Locking Circuit, TRNG (PUF), and so on
HW Locking: HARPOON [5]	✓	✓	×	×	×	✓	×	
HW Locking: Logic Barrier [24]	✓	✓	×	×	×	✓	×	
Secure Split Test (SST) [6, 7]	×	✓	✓	✓	×	✓	×	RSA, TRNG, Locking Circuit LFSR, PUF, I/O Wrapper, etc.
DOST	✓	✓	✓	✓	✓	✓	✓	

(1) ✓ indicates that the countermeasure can prevent the trust issue;
(2) × indicates that the countermeasure is ineffective.

discarded by the foundry or assembly. The untrusted foundry can sell these rejected components to the open market under the name of the original IC designer, which can pose a severe threat to the quality and reliability of a system [6], [7], [19]. Consequently, the IC designer might endure both reputation and revenue losses.

4) *Release of Out-of-Spec ICs:* An untrusted foundry or assembly may incorrectly label the out-of-spec ICs (i.e., speed/voltage binning failure ICs) as in-spec ICs to gain a substantial profit. These chips have a lower quality and can hamper the reputation and profits of the original IC designer.
5) *Reverse Engineering:* The untrusted foundry can reverse engineer chips and extract the netlist of the original design (IP or IC). Reverse engineering is performed mostly to reuse or sell the IP without the consent of the original IP owner.

The threat models distributed along the different stages of the supply chain are shown in Fig. 1.

B. Objectives

The objective of this paper is to propose a robust solution to protect the IP and IC against threats listed in Section II-A. Table I summarizes the limitations and major challenges of the existing countermeasures for ensuring the IP and IC ownerships. It is important to note that most of existing countermeasures cannot prevent defective and out-of-spec ICs from being activated and sold into the market, let alone provide IP and IC coprotection. The proposed solution to ensure the trust and integrity in the modern supply chain must have the following criteria.

1) The proposed technique must ensure both the IP and the IC protection in the supply chain.
2) It must have minimal data volume exchanging between the foundry and the IP owner/IC designer. Doing so, the IP owner/IC designer can control the fabrication quality with a negligible workload.
3) It must allow the IP owner or IC designer to perform a final activation based on both structural and functional test results. This would make sure that defective and out-of-spec ICs are not activated.
4) The proposed method prevents illegal copies (including overused IPs and overproduced ICs) from being activated or functional.
5) The proposed solution must prevent the design from being reverse engineered.
6) Finally, it must ensure the IP and IC coprotection with hierarchical compatibility.

III. DOST STRUCTURE

The overview of DOST for the IP or IC ownership protection is shown in Fig. 2. The proposed DOST is composed of fingerprint generator, linear-feedback shift register (LFSR), I/O wrapper, and result checker circuit.

A. Fingerprint Generator

DOST's operation is based on two types of signatures: temporary fingerprint and permanent fingerprint. In general, a DUT is tested using the temporary fingerprint and activated using the permanent fingerprint. The fingerprint generator is used to generate and manage these two signatures (see Fig. 2). Before the production test, aging-sensitive PUF (AS-PUF)

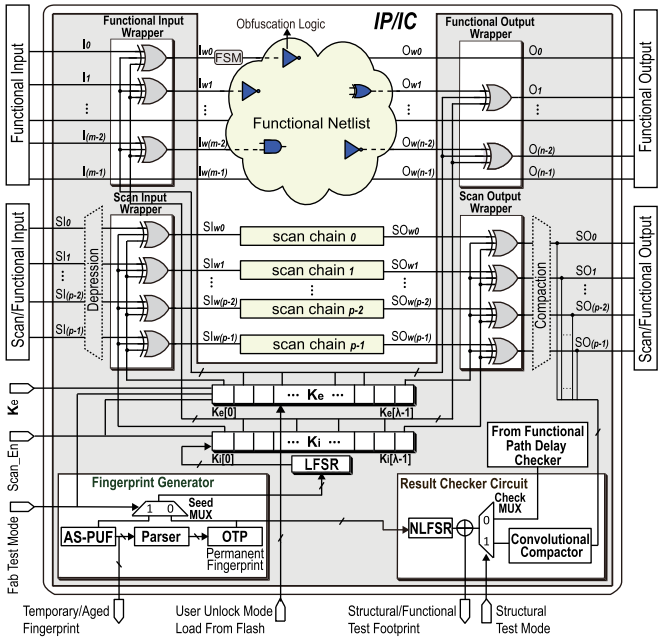

Fig. 2. Detailed architecture of the proposed DOST (encompassed within the gray region).

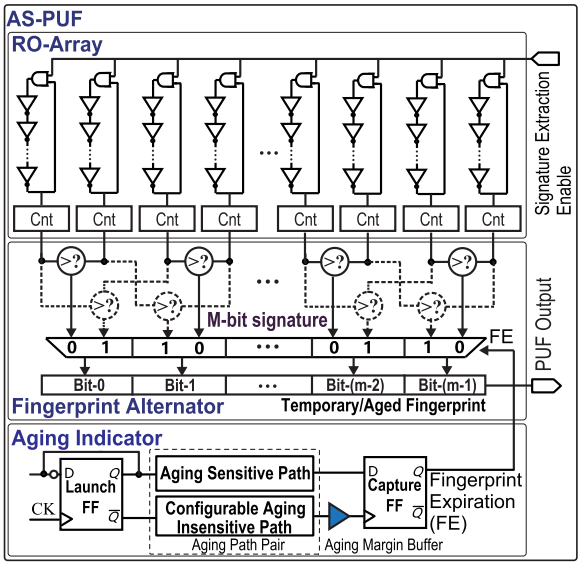

Fig. 3. AS-PUF.

(shown in Fig. 3) dumps an m-bit temporary fingerprint at the foundry. The m-bit temporary fingerprint is parsed and stored into an on-chip one-time programmable (OTP) device as the permanent fingerprint. Controlled by Fab Test Mode signal, the temporary fingerprint is fed to LFSR during the foundry testing, and the permanent fingerprint is fed to LFSR during the final activation. The temporary fingerprint is collected and transferred from the test facility (foundry or assembly) to the IP owner/IC designer. However, the permanent fingerprint is not transferred and accessible by the test facility. Only the IP owner/IC designer can calculate the private permanent fingerprint from the public temporary fingerprint. After the test time window, because of aging, the output of AS-PUF is changed from temporary fingerprint to a significantly different aged fingerprint. Hence, the activation based on the temporary fingerprint fails at the end of the test time window without the final activation key.

The schematic of AS-PUF is shown in Fig. 3. The delay difference of Aging Path Pair in AS-PUF can be affected by aging, which could change the output of AS-PUF. The aging sensitivity of a path is determined by several factors, such as the size of cells and time zero threshold voltage [22], [27], [28]. Silicon results show that large/small standard cells of high/low threshold voltage age at different rates [29], [30]. Small HVT cells, which are more sensitive to aging [29], are used to build the aging-sensitive path of AS-PUF. On the other hand, large LVT cells are used to build the aging-insensitive path. Note that HVT and LVT stand for high and low threshold voltages, respectively. After a given test time window which means that the delay difference between the initially balanced configurable aging-sensitive path and aging-insensitive path [31] approaches the delay of aging margin buffer, the aging indicator within the AS-PUF generates a fingerprint expiration (FE) signal to change the output of ring oscillator-physical unclonable function [32] from temporary fingerprint to a significantly different aged fingerprint. It should be noted that the IP owner/IC designer can adopt other types of AS-PUF, which provides the same function as AS-PUF.

B. LFSR

During testing, the temporary fingerprint, generated by AS-PUF, is used as the seed of LFSR. As shown in Fig. 2, the internal key (K_i) is generated by LFSR and shifted synchronously with the test pattern into the K_i register chain. However, during the final activation of the DUT, the permanent fingerprint is fed to LFSR to generate K_i.

C. Internal and External Key Registers

The internal and *external key*s (K_i and K_e) are designed for locking and unlocking the I/O wrapper. Both of them are λ-bit long [the maximum length of design for testability (DFT) scan chains]. During the structural test, K_i and K_e are shifted into the internal and external key registers from LFSR and external pin synchronously with the test patterns. As shown in Fig. 2, the first scan-in bit (bit-0) of K_i and K_e is distributed to all XOR gates of the scan input wrapper, while the last bit [bit-(λ-1)] of both keys is applied to the scan output wrapper. The other bits of K_i and K_e are randomly connected to the individual gates within the functional I/O wrapper. K_i and K_e work in three modes: structural test, functional test, and activation modes.

1) Structural Test Mode: K_i for the structural test, which is unique for each DUT and determined by temporary fingerprint, is used to lock the scan I/O wrapper. A correct K_e for the structural test generated by the IP owner/IC designer is used to unlock the scan inputs/outputs. According to the following equation:

$$PS_{\text{In/Out}} = ES_{\text{In/Out}} \oplus (K_i \oplus K_e) \tag{1}$$

where $PS_{\text{In/Out}}$ is the internal plain scan test pattern/response and $ES_{\text{In/Out}}$ is the external universally encrypted test patterns/response. According to (1), by adjusting K_e, the IP

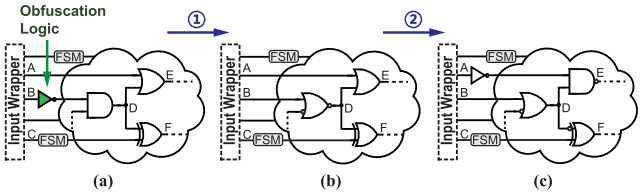

Fig. 4. OLs and FSMs are randomly inserted to obfuscate functional inputs/outputs. The OLs can be moved to larger logic depths according to De Morgan's laws, and the same movement can be applied to the OL inserted to primary outputs. (a) OL at primary input. (b) OL at logic depth i. (c) OL at logic depth $i+1$.

owner/IC designer can keep external encrypted test patterns/responses universal for all DUTs. This is performed intentionally to reduce the data exchanging and communication complexity between the IP owner/IC designer and the foundry/assembly.

2) Functional Test Mode: The same K_i is used for the functional test. However, a new K_e dedicated to the functional test is applied. K_i and K_e set for functional test together temporarily unlock the functional I/O wrapper. During the functional test, instead of being shifted in serial, K_e can be loaded from a flash address. As shown in Fig. 2, a specific functional input (output) is randomly controlled by $K_i[i]$ and $K_e[j]$. The value of i and j is only known by the IP owner/IC designer. Considering obfuscation logics (OLs) are introduced at functional inputs/outputs, which is detailed in Section III-D, to unlock this functional input (output), (2) should be satisfied

$$K_i[i] \oplus K_e[j] \oplus OL = 1 (0 \leq i, j \leq \lambda - 1). \tag{2}$$

According to (2), with the knowledge of OL, i, and j, the IP owner/IC designer can always calculate K_e for the functional test from the public temporary fingerprint.

3) Circuit Activation: A DUT is ready to be activated when it passes all structural and functional tests. LFSR loads the permanent fingerprint as seed and generates a new K_i. The foundry has to wait for K_e set for the final activation, which can only be generated by the IP owner/IC designer, to activate a device finally. It should be noted that loading of K_e set is also controlled by Fab Test Mode signal, as shown in Fig. 2. After testing, K_e set for the final activation can be loaded from a secure OTP.

D. I/O Wrapper With the Obfuscation Logic

The I/O wrapper consists of both scan and functional I/O wrappers (Fig. 2). The inputs of the wrappers are fed from K_i and K_e, as described in Section III-C.

To protect the design from reverse engineering, some randomly selected inputs and outputs are obfuscated by inserting OLs, as shown in Fig. 4(a). It should be noted that OLs can be moved to larger logic depth according to De Morgan's laws as shown in Fig. 4(b) and (c), which makes it difficult for attackers to differentiate OLs from the original netlist. Furthermore, to make DOST more robust against the Boolean Satisfiability (SAT) attack [39], several finite-state machines (FSMs) are randomly inserted to functional inputs, as shown in Fig. 4. Note that the FSM would be transparent after transferring α correct states. Hence, in order to completely unlock the functional I/O wrapper, a K_e set that includes α K_es for a functional test or final activation should be loaded in order. In this paper, α is set as 3.

E. Result Checker Circuit

The result checker circuit is used to prevent the foundry from misreporting test results to the IP owner/IC designer for keys, which prevents the release of defective and out-of-spec ICs. Fig. 2 shows the proposed result checker circuit that is composed of a convolutional compactor and a nonlinear feedback register (NLFSR). In the structural test mode, the scan chain outputs are compressed by the convolutional compactor [34] into one sequence. There is a possibility of error masking due to convolutional compacting. However, it has been reported that the error masking rate is below 3.3% for industrial designs [34], which is acceptable for the proposed method. The NLFSR [35] then obfuscates the compressed sequence to generate the structural test footprint. Note that the NLFSR is also uniquely seeded with the permanent fingerprint generated by AS-PUF. A structural test footprint that contains the structural test pass/fail information is dumped and logged by the ATE. Only the IP owner/IC designer, who has the knowledge of NLFSR function, can recover the compressed scan outs using the AS-PUF's value. Thus, the foundry cannot predict the fault-free structural test footprint of any DUT and has to report their logged footprint. Similarly, during the functional test, the outputs of functional path delay checkers (see [36]) are shifted into result checker circuit and a functional test footprint is dumped. Again, the functional test footprint is not manageable.

To avoid reverse engineering and malicious modifications, it is suggested to replace 3-input XOR gates in I/O wrapper of DOST by circuits with the same function which are composed of normal logic gates, such as 2-input AND gate, 2-input OR gate, inverter, and so on, as shown in Fig. 5(b). These 3-input XOR circuits could be all or partly moved to different logic depths according to De Morgan's laws. More importantly, netlists of DOST and IP/IC under protection should be flattened together, as shown in Fig. 5(c). Then, the camouflaging technology [33] should be adopted to implement the circuit. These countermeasures make it difficult to separate DOST from the whole flattened netlist and make malicious modifications to obtain K_i.

IV. DOST-Based Test Methodology

A. Test Methodology

The stages of the DOST-based SST methodology are shown in Fig. 6 and discussed as follows.

1) Test Initiation: During test initiation, test patterns and responses detecting stuck-at, transition, delay faults, and so on are generated first based on the original IP/IC design. Then, the original test patterns/responses for the structural test are universally encrypted and delivered together with functional test patterns/responses to the foundry. After fabrication, the I/O wrapper of the protected IP/IC is locked by a unique K_i [Fig. 7(a)]. The foundry collects the AS-PUF's values of

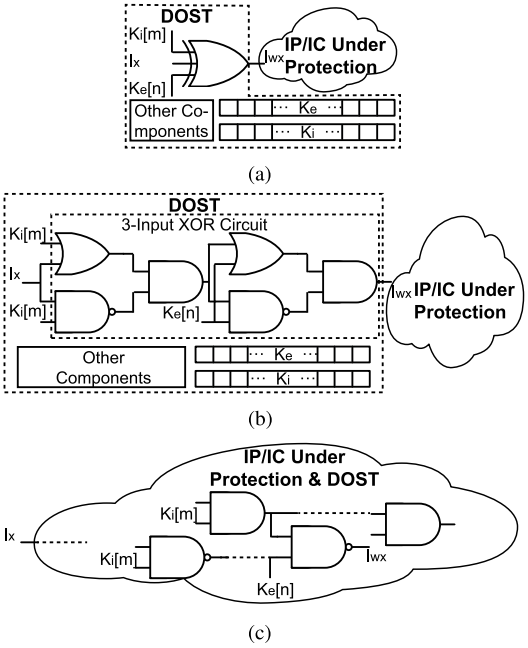

Fig. 5. Countermeasures to avoid reverse engineering and malicious modifications on DOST, which makes the attacker difficult to separate DOST from the whole netlist and make malicious modifications to obtain K_i. (a) Initial connection between one of 3-input XOR gate in I/O wrapper of DOST and IP/IC under protection. (b) 3-input XOR gates in I/O wrapper of DOST are replaced by circuits with the same function which are composed of normal logic gates. (c) Netlists of DOST and IP/IC under protection are flattened together. In addition, 3-input XOR circuits in I/O wrapper are moved to different logic depths according to De Morgan's laws.

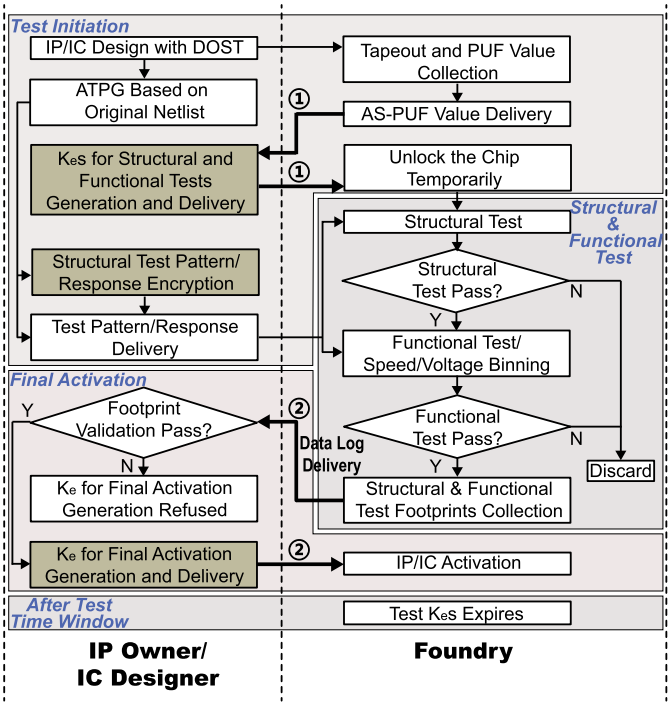

Fig. 6. Stages of DOST-based test methodology.

DUTs and sends them to the IP owner or IC designer. The IP owner/IC designer calculates K_e sets for structural and functional tests.

2) Structural Test: As shown in Fig. 7(b), during the structural test, the universally encrypted patterns are applied to all DUTs, as shown in Fig. 8. At the same time, a unique K_e set for structural test delivered by the IP owner/IC designer is supplied externally to unlock the scan I/O and decrypt the patterns. The structural test footprint is generated at the same time. If the DUT passes the structural test, the functional test is conducted. Otherwise, the defective DUT is discarded, as shown in Fig. 6.

3) Functional Test: As shown in Fig. 7(c), during the functional test, a unique K_e set for the functional test is applied in sequence to unlock the functional I/O wrapper. In this stage, all functional tests can be performed, such as standard functional, speed binning, and voltage binning. A uniquely encrypted functional test footprint is dumped (Fig. 8).

4) Final Activation: When IC passes all tests, the foundry logs the ECID, AS-PUF's value, K_e values, and structural and functional test footprints of each in-spec IC, as shown in Fig. 9. The collected data are then sent to the IP owner/IC designer for footprint validation. If the footprints show that test results are not misreported, the IP owner/IC designer will deliver K_e sets for final activation to the foundry to permanently unlock the corresponding ICs, as shown in Fig. 7(d). If the footprint does not match the reported test result, the activation request will be refused as shown by the IC marked with ECID_2 shown in Fig. 9.

5) After Test Time Window: After the test time window, test K_e sets expire due to the changes of K_i caused by AS-PUF aging. In other words, the delivered test K_es cannot unlock the I/O wrapper anymore. If the activation request is refused by the IP owner/IC designer, the protected IP/IC has locked again, as shown in Fig. 7(e).

Fig. 10 shows the flow of all DUTs. After fabrication, if the DUT fails the structural test, the defective DUT not permanently unlocked has to be discarded. Similarly, the out-of-spec DUT has to be discarded. If the foundry/assembly does not discard them, the IP owner/IC designer can refuse to deliver the final activation K_e set based on the structural and functional test footprints. Thus, the temporarily unlock status will expire after test time window and the corresponding device is disabled and has to be discarded anyway. Finally, a licensed number of DUTs that pass all tests can be used with the locked scan I/Os and permanently unlocked functional netlist.

B. Test Overhead Evaluation

1) Data Exchanging Overhead: As shown in Fig. 6, ① and ② represent twice extra data exchanges required between the IP owner/IC designer and foundry in the proposed secure test methodology: 1) the IP owner/IC designer delivers test K_e sets based on the foundry extracted AS-PUF's value and 2) the foundry reports structural/functional test footprints, and the IP owner/IC designer returns the final activation K_e set if footprints match the reported pass status. The exchanging data volume increment mainly comes from structural and functional test footprints, which equals to $1 \sim 2$ additional

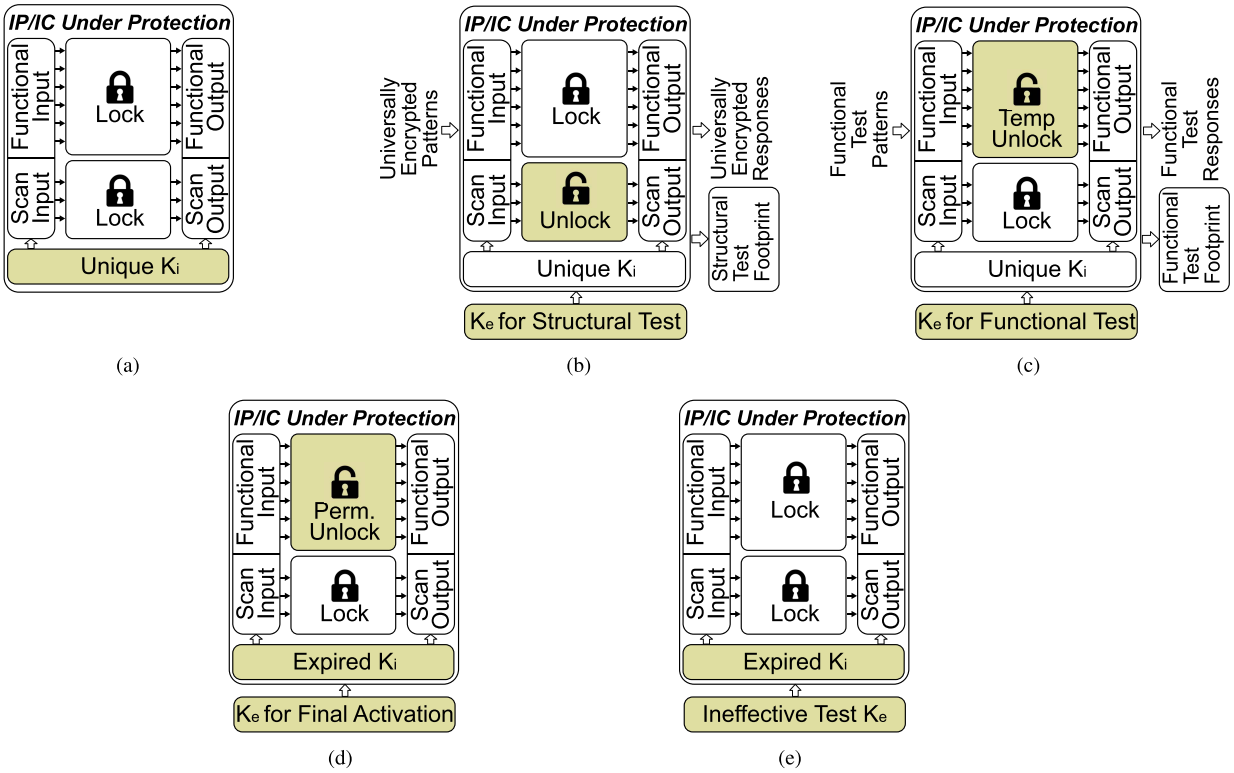

Fig. 7. DOST-based IC test and activation flow. (a) After fabrication, the I/O wrapper of the protected IP/IC is locked by a unique K_i. Note that the value of K_i is determined by the output of AS-PUF and LFSR. (b) During the structural test, universally encrypted patterns are applied to the protected IP/IC. At the same time, a unique K_e set for the structural test is supplied externally to unlock the scan I/O and decrypt the encrypted patterns. A structural test footprint is dumped in this process. (c) During the functional test, a unique K_e set for the functional test is applied to unlock the functional I/O and all functional tests can be performed. A uniquely encrypted functional test footprint is dumped in this process. (d) After the footprints are validated by the IP owner/IC designer, K_e set for final activation is applied to activate the protected IP/IC. (e) K_i expires after test time window due to AS-PUF's value expiring. The K_e sets for a test cannot unlock the I/O wrapper anymore. If the activation request is refused, the protected IP/IC is locked again.

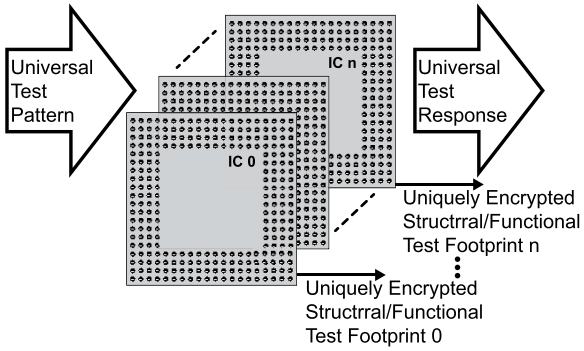

Fig. 8. Universal test patterns are applied to all DUTs, and every DUT generates uniquely encrypted structural/functional test footprints.

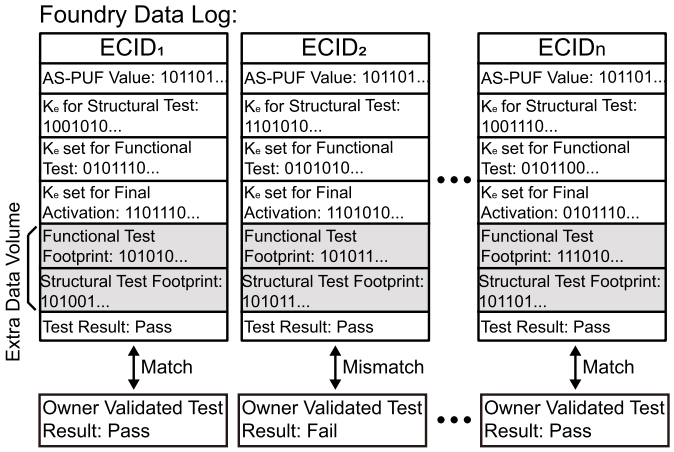

Fig. 9. Data log is delivered to the IP owner/IC designer by the foundry. And the data log validation result is given by the IP owner/IC designer. The gray parts represent the extra data volume equaling to $1 \sim 2$ additional scan I/Os' data comparing with transitional tests.

scan I/Os' data volume. In contrast, the SST [6], [7] needs to exchange all test responses of each DUT. Therefore, DOST offers a significant reduction in data exchange between the IP owner/IC designer and the foundry. The extra data volume for each benchmark is shown in Table III.

2) Pattern Encryption Effort: Test patterns/responses for the structural test are encrypted to ensure the high-level scan security and safety. The algorithm used to encrypt the test patterns/responses is shown in 1. With DOST, every original pattern/response only needs to be XORed with test K_i and K_e once by the IP owner/IC designer before delivering them. Table II shows the computation effort for several benchmarks.

V. Multilevel DOST Protection

DOST provides a unified solution to protect both IP and IC in modern semiconductor supply chain. The hierarchical protection levels that include both IP level (DOST_{IP}) and IC level (DOST_{IC}) are shown in Fig. 11.

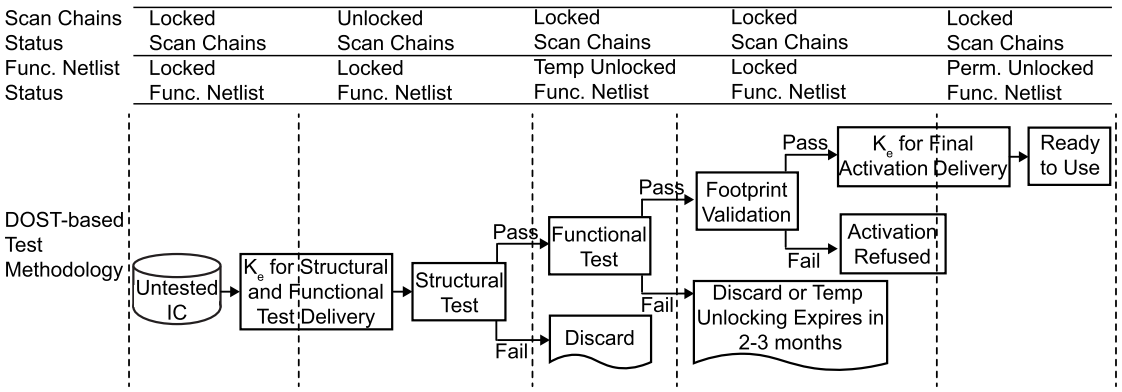

Fig. 10. Direction and the netlist state of all DUTs within DOST flow.

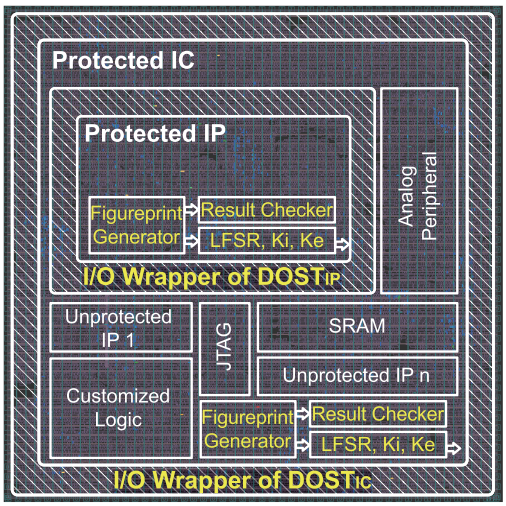

Fig. 11. Hierarchical DOST protection. IP level ($DOST_{IP}$) and IC level ($DOST_{IC}$) DOST protect the specific IP and the whole IC ownership, respectively.

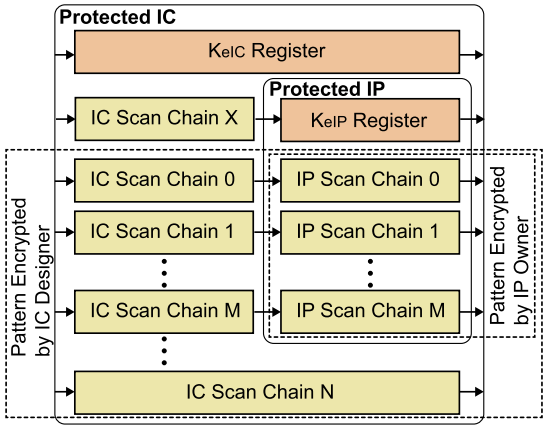

Fig. 12. IP–IC merging for multihierarchical-level DOST protection.

A. IP Protection

$DOST_{IP}$ (see Fig. 11) ensures the integrated IP ownership. The IP owner can deliver a universal test pattern set with the synthesized soft or firm/hard IP at the same time to the IC designer. The IP owner, then, transfers the structural and the functional test K_e sets. The K_e sets are calculated based on the AS-PUF_{IP}'s value provided by the foundry or IC designer. As the activated IP count is the only concern for the IP owner, he/she can let the IC designer validate the IP test result and make the final activation decision. The IC designer then sends the licensed number of AS-PUF_{IP} signatures from passed ICs to the IP owner. The IP owner receives them and computes the same number of final activation K_e sets. The above approach makes sure that the activated count can be fully controlled by the IP owner. Section VII-C shows the robustness of DOST against IP piracy.

B. IC Protection

As discussed in Section IV, $DOST_{IC}$, shown in Fig. 11, ensures that the IC designer controls the test and activation of the whole IC. As the foundry cannot perform structural and functional tests without test K_e sets delivered by IC designer. Besides, the IC can be activated if and only if the structural and functional test footprints pass the IC designer's validation. As discussed in Section VII-C, DOST makes sure that overproduced, defective and out-of-spec ICs are not activated and sold into the market. Also, it protects IC from reverse engineering.

C. Multihierarchical Level Protection

With low area overhead, DOST can concurrently exist in multiple hierarchical levels to provide protection to IP and IC belonging to different parties. Scan I/Os and external key register of $DOST_{IP}$ can be stitched into any IC scan chains. The chain merging and pattern encryption for multihierarchical-level DOST protection are shown in Fig. 12. As shown in Fig. 13, the foundry collects the AS-PUF_{IP}'s and AS-PUF_{IC}'s value of a device. The IP owner and IC designer calculate test $K_{e_{IP}}$ sets and $K_{e_{IC}}$ sets for $DOST_{IP}$ and $DOST_{IC}$, respectively. The external keys are concatenated as K_e sets and delivered to the foundry. After all tests, the IC designer requests the contracted number of the final activation $K_{e_{IP}}$ sets from the IP owner. $K_{e_{IP}}$ are, then, merged into the device final activation K_e sets.

VI. DOST-Based Implementation Flow

The implementation flow of DOST for the IP owner or IC designer, shown in Fig. 14, is divided into the following steps.

Step 1 (IP/IC Design and Synthesis): In this phase, the IP or IC is designed and synthesized for test and verification. The DFT structure is inserted during synthesis.

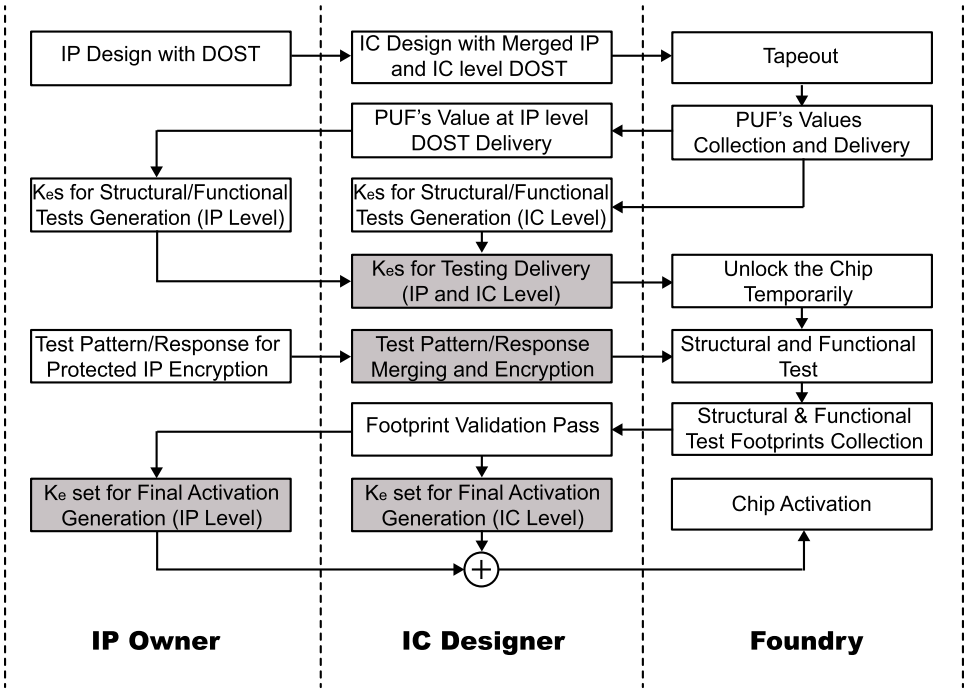

Fig. 13. Data exchange with multihierarchical-level DOST protection.

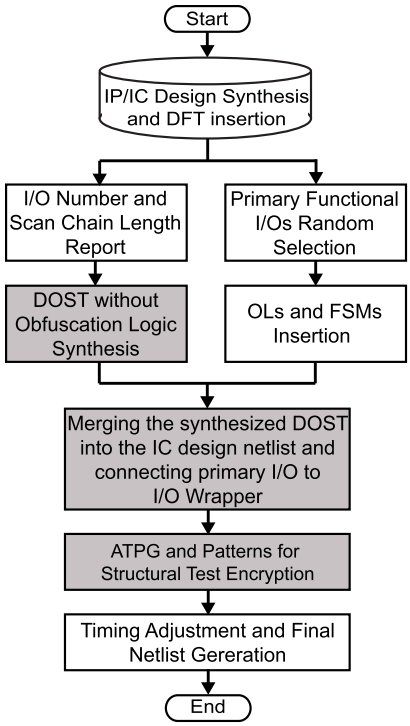

Fig. 14. DOST-based design implementation flow.

Step 2 (Functional I/O Random Selection): The designer randomly selects primary functional I/Os for OLs and FSMs insertion.

Step 3 (OLs and FSMs Insertion): OLs and FSMs are inserted into the selected I/O group during engineering change orders. To make OLs more difficult to be identified, a larger logic depth is implemented using De Morgan's laws (Fig. 4).

Step 4 (DOST Synthesis): In this step, the fingerprint generator, LFSR, key registers, and result checker belonging to DOST are synthesized. Note that the length of internal and external key registers is equal to the maximum length of DFT scan chains.

Step 5 (DOST Insertion): The synthesized DOST is merged into the design.

Step 6 (Automatic Test Pattern Generation and Pattern Encryption): In this step, the structural test patterns based on the DOST inserted netlist with the scan I/O wrapper forced as transparent are generated. Then, the IP owner or the IC designer performs one-time encryption and generates the encrypted universally deliverable patterns/responses for all DUTs. DOST does not affect the IP/IC function. Hence, the functional test patterns should be generated based on the DOST free netlist.

Step 7 (Layout Generation and Delivery): After timing closure, the final netlist is generated. The final IP is delivered to the IC designer. The IC designer generates the final layout and provides the GDSII file to the foundry for fabrication.

VII. Experimental Results and Analysis

DOST is implemented in a 32-nm technology node on OpenSPARCT2, Gaisler, and OPENCORE benchmarks. The circuits are synthesized with 10-MHz full scan. The functional clock frequency is 100 MHz with a test compressed scan chain length equaling to 64 ($\lambda = 64$).

A. Overhead

Table II shows the overheads of DOST implemented with 16-bit AS-PUF, 16-bit LFSR, and achterbahn-80 NLFSR [35]. The area overhead is as low as 0.959%–2.267%. The scan

TABLE II

AREA, SHIFTING POWER, AND PATTERN PROCESSING TIME OVERHEADS OF DOST

IP Benchmark	VGA-LCD	FGU	Leon3	Leon3mp
# SFF	17058	27931	49443	82514
# Scan Chains	267	437	723	1290
Area Overhead	2.267%	1.118%	1.181%	0.959%
Shifting Power Overhead	1.892%	1.079%	1.132%	1.012%
Pattern Proc. Time Per Pattern (μs)	59.3	84.2	141.4	234.0

TABLE III

DATA EXCHANGING OVERHEAD OF DOST

IP Benchmark	VGA-LCD	FGU	Leon3	Leon3mp
# Path Delay Monitors [37]	72	55	204	46
Bits of Functional Test Footprint	360	275	1020	230
Bits of PUF Signature and K_es	272	272	272	272
# Structural Test Patterns to Detect Stuck-at Fault	1,615	1,807	2,185	3,807
Bits of Structural Test Footprint	103,360	115,648	139,840	243,648
Data overhead of Structural Test Footprint	0.38%	0.29%	0.14%	0.08%

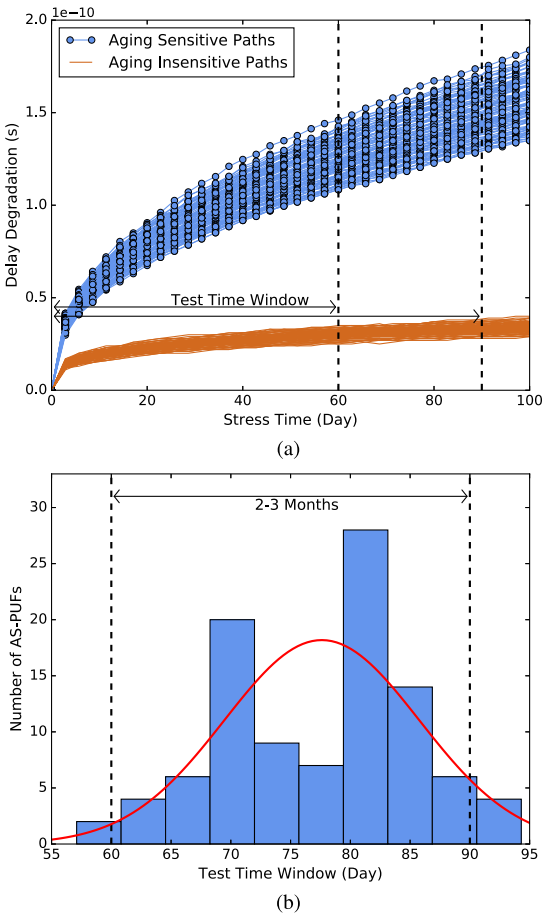

Fig. 15. (a) Delay degradations of aging path pairs within 100 AS-PUFs and (b) test time window distribution of AS-PUFs, considering 30% V_{th}, 10% L, 10% W, and 20% t_{ox} variations, at 25 °C without aging acceleration stress.

shifting power overhead is in the range of 1.012%–1.892%. Note that the overheads can be even smaller for a large-scale industrial application. The processing time overhead per pattern for encryption is shown in Table II as well. With a Linux workstation of 2.4 GHz, 20-core CPU, a single-thread Python parser, the maximum time for patterns encryption per pattern is 234.0 μs, which is negligible. The exchanging data overhead required by the proposed SST methodology is shown in Table III. Considering the path delay monitors [37], used to monitor the most critical path group, the data size of functional test footprints for different benchmarks are limited to 230–1020 bits. The structural test footprint is equal to the data volume of an additional scan I/O, which is equal to 0.08%–0.38% of the whole scan data. The results show that the data size of PUF signature, K_e sets, and functional test footprints is negligible compared with the structural test footprint. Therefore, only around 0.08%–0.38% of scan data volume is exchanged between the IP owner/IC designer and foundry which is significantly smaller than [6], [7], which requires all scan data to be exchanged.

B. Temporary Authentication Window Analysis

In the proposed test methodology, the foundry/assembly has a time window to conduct functional tests in the temporarily unlocked mode. The temporarily unlocked mode is authenticated based on the temporary fingerprint of AS-PUF (Fig. 2). The delay degradation of aging path pairs within 100 AS-PUF samples (Fig. 3), considering 30% V_{th}, 10% L, 10% W, and 20% t_{ox} variations, at 25 °C without accelerated stress is shown in Fig. 15(a). As the test time window ends when the degradation difference between an aging path pair approaches the delay of aging margin buffer (Fig. 3). Furthermore, according to Fig. 15(a), the test time window length is affected by process variation. Fig. 15(b) shows the distribution of test time windows of 100 AS-PUF samples. It can be seen that 95.0% AS-PUFs' temporary fingerprints expire in 2–3 months, and all of them end within four months. This test window distribution guarantees enough fabrication and test time for most foundry and assembly. Note that the test time window can be alternated by changing the delay of aging margin buffer.

C. Attack Analysis

The threat models shown in Section II violate the IP and IC ownerships. Also, the attacker may try to break through the protection of DOST and perform IP/IC piracies. The performance of DOST against these attacks is discussed in this section.

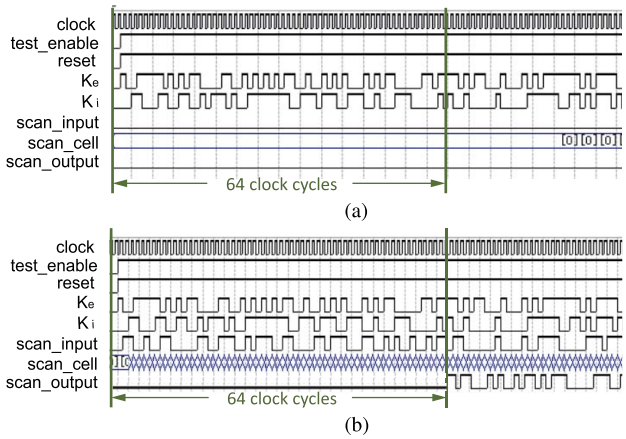

Fig. 16. Security performance of the proposed architecture under attacks. (a) Under flushing attack, scan outputs always equal to scan inputs λ clock cycles before, with no crypto information leaked. (b) Under resetting attack, K_i and K_e are all reset and $\lambda = 64$ (λ is the length of scan chains with test compressed) and zeros are scanned out first without leaking K_i.

1) Overusing IP/IC: Untrusted IC designer or foundry can reuse IP in unauthorized ICs without the consent of the IP owner. And an untrusted foundry can tape out more than the licensed number of ICs by reusing the mask. However, with DOST, only a contracted number of final activation K_e sets are given to the foundry for in-spec IP/ICs. The illegal (i.e., overbuilt) chips cannot be functionally activated. Hence, the DOST-based test flow introduced in Section IV can prevent overusing IP or IC.

2) Delivering Defective ICs to the Market: The foundry may intend to deliver defective ICs to the market as fault-free ones. In DOST, the scan response is shifted to a convolutional compactor and stream ciphered by NLFSR to generate the structural test footprint. As NLFSR is seeded by AS-PUF, the structural test footprints are unpredictable and unique from device to device and not manageable by the foundry. K_e set for final activation is released to unlock a particular IC only when it passes the structural test. To decipher the footprint, the NLFSR function might be another target of an untrusted party. However, Achterbahn-80 NLFSR [35] is adopted in DOST and the time complexity for function attack is as high as $O(2^{276})$.

3) Delivering Out-of-Spec ICs to the Market: To make profits, out-of-spec (e.g., lower speed than the specified speed) devices can be labeled as in-spec ones. However, with DOST, the IC designer can verify the speed binning results from the functional test footprint and check if the device is in-spec as the foundry claimed. If the foundry makes any wrong claim, K_e set for final activation will not be provided by the IC designer to unlock the IC. Even if an out-of-spec device is released to market without the final activation K_e set, it will be malfunction after the test time window. And the IC designer can defense for innocence with DOST generated footprints.

4) Key Registers Attack: The attacker can perform key attacks targeting the final activation K_e sets, which includes: 1) stealing K_i through flushing and resetting attacks, then he/she can calculate final activation K_e sets for any device with a known K_i and K_e set pair and 2) applying brute-force attack for final activation K_e sets. The security analysis of the DOST against the above-mentioned key attacks is shown in the following.

1) *Flushing Attack:* The attacker may seek to obtain K_i by simply flushing the scan chains. The scan I/O wrapper are controlled by bit-0 and bit-$(\lambda - 1)$ of K_i and K_e. During flushing attack, as shown in Fig. 2, with λ scan clocks, bit-0 of K_i and K_e ($K_i[0]$ and $K_e[0]$) are shifted to bit-$(\lambda - 1)$ and the wrapped SI (SI_w) is shifted to the position of wrapped SO (SO_w) in Fig. 2. Therefore

$$\text{SI}_w = \text{SI} \oplus (K_i[0] \oplus K_e[0]) \tag{3}$$

$$\text{SO} = \text{SI}_w \oplus (K_i[0] \oplus K_e[0]) = \text{SI}. \tag{4}$$

Equation (3) shows that the scan output always equals to scan input at λ clock cycles before. The simulation waveforms during flushing attack are shown in Fig. 16(a). It can be seen that the scan output sequence and the scan input sequence are the same, regardless of correct or incorrect K_e. It signifies that the scan out value does not contain any key information.

2) *Resetting Attack:* The attacker might also seek to obtain K_i by resetting the device and observing scanning outs. However, LFSR, K_i, and K_e are synchronously reset with the scan cells. After resetting, for the first λ clock cycles, $K_i[\lambda - 1]$ equals 0, and the scan out can be expressed as

$$\begin{aligned}\text{SO} &= SC[\lambda - 1] \oplus K_i[\lambda - 1] \oplus K_e[\lambda - 1] \\ &= K_e[\lambda - 1]\end{aligned} \tag{5}$$

where $SC[\lambda - 1]$ is the last bit of a scan chain and is equal to 0 for the first λ clock cycles. Therefore, the scan out is always equal to the corresponding bit of public K_e without revealing K_i [see Fig. 16(b)].

3) *Brute-Force Attack:* The final activation key K_e set is written into a secure OTP, as discussed in Section III-C. Therefore, there is no chance for an attacker to perform brute-force attack to obtain the correct K_e set for the final activation.

4) *SAT Attack:* In SAT attack [39], [41], the attacker compares the responses of activated and unactivated ICs and finds distinguishing input patterns to identify the correct activation key. Since the attacker has only one chance to write the correct final activation K_e set into OTP, it is almost impossible for him/her to guess the right key once. Even if the attacked IC is still in the test time window, the attacker needs to apply distinguishing input patterns together with scanning in various K_e sets to exclude the wrong keys. However, limited by the clock frequency and serial scan operation, it takes a long time to attack. Moreover, getting the temporary unlocked key is useless after the test time window.

5) Reverse Engineering Attack: The attacker (i.e., untrusted foundry or other parties in the supply chain) can perform malicious modifications based on the reverse engineering extracted netlist [38] to break through the protection of DOST, which includes: 1) removing DOST and 2) inserting hardware Trojan to reveal K_i during testing. If the attacker seeks to get

TABLE IV
COMPARISON AMONG DOST, CSST [6], [7], HARDWARE METERING [3], AND LOGIC BARRIER [24]

Metrics	DOST	CSST [6, 7]	Hardware Metering [3]	Logic Barrier [24]
Area Overhead	Extra RO-based PUF, convolutional compactor, K_i and K_e registers, and FSRs (low)	Extra RSA module, Scrambling block, and TRNG (high)	Extra FSM logic and PUF (low∼medium)	Extra reconfigurable-logic barriers for IOs, lookup table, and PUF (high)
Security during Production Tests	Both structural and functional tests are conducted with protection. Volume authentication takes places after all tests	Only structural test is conducted with protection	Neither structural or functional tests is conducted with protection. A Large volume of authentication takes place before all tests.	Neither structural or functional tests can be conducted with protection. Volume authentication takes place before all tests.
Overproduced IC Deactivation	Yes	Yes	No. Foundry can overproduce ICs by claiming lower (than the original) yield.	No. Foundry can overproduce ICs by claiming lower (than the actural) yield.
Defective IC Deactivation	Yes	Yes	No	No
Out-of-spec (speed) IC Deactivation	Yes	No; Speed binning takes place without protection	No	No
IP and IC Co-protection	Yes	No	No	No
Extra work load for DFT engineers *	One-time encrypted pattern /response generation; 3 K_es and structural and functional test footprints computation and validating for each IC	N-time test pattern/response generation for each IC (N equals to the production volume); Whole test response checking for each device	—-	—-
Data exchange volume between IC designer and test facilities *	3 K_es, structural and functional test footprints.	All test responses, test and activation keys for each IC.	—-	—-

* Applicable for the methodologies with secure tests enabled.

rid of DOST from the reverse engineering extracted netlist, after DOST removed, the original IP/IC netlist with OLs and FSMs is left. Then, the attacker may break the OLs with the following.

1) *Brute-Force Attack Assisted by Reverse Engineering:* The function of the original netlist with OLs and FSMs is expressed as

$$I_{\text{obf}} = \text{Function}_{\text{OB}}(I)$$
$$O_{\text{obf}} = \text{Function}_{\text{OB}}(O) \quad (6)$$

where I/O and $I_{\text{obf}}/O_{\text{obf}}$ are the input/output without/with obfuscation, respectively, and $\text{Function}_{\text{OB}}$ is the obfuscation function including OLs and FSMs. According to (6), the probability of recovering original netlist with brute force is $P_{\text{in}} * P_{\text{out}}=[1/(C_m^0+C_m^1+C_m^2+\cdots+C_m^m)]^{\alpha} * [1/(C_n^0+C_n^1+C_n^2\cdots+C_n^n)] = 1/2^{m*\alpha+n}$, where m and n are input and output port count, respectively. It can be seen that the brute-force attack is impractical (i.e., with a probability of $1/2^{2103}$ for floating-point and graphics unit (FGU) benchmark when $\alpha = 3$).

2) *SAT Attack Assisted by Reverse Engineering:* There are overall two attack scenarios as follows.
   a) *Attacking the Netlist Including DOST:* The whole netlist of the IC can be extracted by reverse engineering. However, due to the existence of AS-PUF, K_i is unique for each chip. Thus, SAT attack cannot be applied.
   b) *Attacking the Netlist Without DOST:* As the attacker may identify the internal and external key registers of DOST, SAT attack can be performed by setting K_i as constant and applying various K_es as shown in Fig. 17(a) and or removing the external key registers and directly applying different keys on functional I/O wrapper, while K_i is set as constant, as shown in Fig. 17(b).

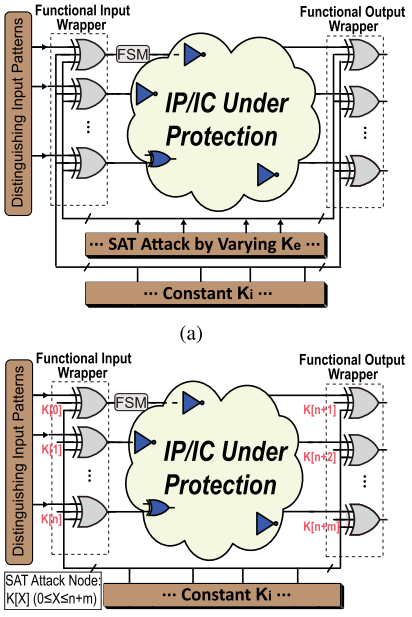

Fig. 17. Two possible methods to apply SAT attack when removing DOST from the reverse engineering extracted netlist. (a) Attacker sets K_i as constant and applies various K_e sets to perform SAT attack. The attack complexity is related to the length of K_e, which is equal to the maximum length of scan chains. (b) Attacker removes the external key registers and directly applies different keys on functional I/O wrapper. At the same time, K_i is set as constant. The attack complexity is related to the functional I/O count.

The complexity of the above SAT attacks is related to the length of K_e or the functional I/O count. With α-state FSM, the minimum key input number

is $\min\{2^{\lambda*\alpha}, 2^{(m+n)*\alpha}\}$, where $m + n$ represents the functional I/O count. In this implementation, λ is set as 64, and α is set as 3. For FGU, the minimum attack count is 2^{192}. The number proves that even with small FSMs, the probability to crack the DOST-protected IP/IC by SAT attack is low.

However, according to Section III, it is suggested that netlists of DOST and IP/IC under protection should be flattened together. In addition, 3-input XOR gates in I/O wrapper could be replaced by circuits with the same function, and then, these circuits need to be moved to different logic depths according to De Morgan's laws. The above-mentioned countermeasures make the attacker difficult to separate DOST from the whole flattened netlist by reverse engineering and perform malicious modifications to reveal K_i.

D. Comparing With Existing Techniques

The comparisons of DOST with major antipiracy techniques, including CSST [6], [7], hardware metering [3], and logic barrier [24], are listed in Table IV. The results and analyses show that DOST can prevent defective, overproduced, and out-of-spec ICs from entering the market with better assurance and efficiency, and provide IP and IC coprotection.

VIII. Conclusion

In this paper, we presented a novel DOST and an SST methodology to prevent IP and IC piracies by overusing IP in unauthorized IC or shipping overproduced, defective, and out-of-spec ICs to the market. By temporary fingerprint generation and authentication, the foundry can conduct structural tests in the locked mode and functional test in the temporarily unlocked mode. The result checker circuit ensures that only the IP owner/IC designer can control the whole test process. The results and attack analyses demonstrated that DOST could provide high security against IP and IC piracies with low overhead. We verified our claims by implementing DOST on four benchmarks from OpenSPARCT2, Gaisler, and OPENCORE.

References

[1] *2014 International Technology Roadmap for Semiconductors*. Accessed: Nov. 2016. [Online]. Available: http://www.itrs.net/links/2014ITRS/Home2014.htm

[2] Digitimes Research. *Trends in the Global IC Design Service Market*. Accessed: Nov. 2017. [Online]. Available: http://www.digitimes.com/Reports/Report.asp?datepublicsh=2012/3/13&pages=P.S&Seq=400&read=toc

[3] F. Koushanfar and G. Qu, "Hardware metering," in *Proc. 38th Annu. Design Autom. Conf.*, 2001, pp. 490–493.

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

[5] R. S. Chakraborty and S. Bhunia, "HARPOON: An obfuscation-based SoC design methodology for hardware protection," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 28, no. 10, pp. 1493–1502, Oct. 2009.

[6] G. K. Contreras, M. T. Rahman, and M. Tehranipoor, "Secure split-test for preventing ic piracy by untrusted foundry and assembly," in *Proc. IEEE Int. Symp. Defect Fault Tolerance VLSI Nanotechnol. Syst. (DFTS)*, Oct. 2013, pp. 196–203.

[7] M. T. Rahman, D. Forte, Q. Shi, G. K. Contreras, and M. Tehranipoor, "CSST: Preventing distribution of unlicensed and rejected ICs by untrusted foundry and assembly," in *Proc. IEEE Int. Symp. Defect Fault Tolerance VLSI Nanotechnol. Syst. (DFT)*, Oct. 2014, pp. 46–51.

[8] J. A. Roy, F. Koushanfar, and I. L. Markov, "EPIC: Ending piracy of integrated circuits," in *Proc. Conf. Design Autom. Test Eur.*, 2008, pp. 1069–1074.

[9] M. Potkonjak, G. Qu, F. Koushanfar, and C.-H. Chang, "20 Years of research on intellectual property protection," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2017, pp. 1–4.

[10] *Chipworks Reverse Engineering Software*. Accessed: Mar. 2017. [Online]. Available: http://www.chipworks.com/en/technical-competitive-analysis

[11] R. W. Jarvis and M. G. McIntyre, "Split manufacturing method for advanced semiconductor circuits," U.S. Patent 7 195 931, Mar. 27, 2007.

[12] *Intelligence Advanced Research Projects Activity Trusted Integrated Circuits Program*. Accessed: Mar. 2017. [Online]. Available: https://www.fbo.gov/utils/view?id=b8be3d2c5d5babbdffc6975c370247a6

[13] Y. Xie, C. Bao, and A. Srivastava, "Security-aware 2.5 D integrated circuit design flow against hardware IP piracy," *Computer*, vol. 50, no. 5, pp. 62–71, 2017.

[14] Y. Wang, P. Chen, J. Hu, and J. J. V. Rajendran, "Routing perturbation for enhanced security in split manufacturing," in *Proc. 22nd Asia South Pacific Design Autom. Conf. (ASP-DAC)*, Jan. 2017, pp. 510–605.

[15] P.-L. Yang and M. Marek-Sadowska, "Making split-fabrication more secure," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Design (ICCAD)*, Nov. 2016, pp. 1–8.

[16] J. J. V. Rajendran, O. Sinanoglu, and R. Karri, "Is split manufacturing secure?" in *Proc. Conf. Design, Autom. Test Eur.*, 2013, pp. 1259–1264.

[17] Y. Wang, P. Chen, J. Hu, and J. J. V. Rajendran, "The cat and mouse in split manufacturing," in *Proc. 53nd ACM/EDAC/IEEE Design Autom. Conf. (DAC)*, Jun. 2016, pp. 1–6.

[18] S. Amir, B. Shakya, D. Forte, M. Tehranipoor, and S. Bhunia, "Comparative analysis of hardware obfuscation for IP protection," in *Proc. Great Lakes Symp. VLSI (GLSVLSI)*, New York, NY, USA: ACM, 2017, pp. 363–368.

[19] M. T. Rahman, D. Forte, and M. M. Tehranipoor, "Protection of assets from scan chain vulnerabilities through obfuscation," in *Hardware Protection Through Obfuscation*. Cham, Switzerland: Springer-Verlag, 2017, pp. 135–158.

[20] Y. Xie and A. Srivastava, "Delay locking: Security enhancement of logic locking against ic counterfeiting and overproduction," in *Proc. 54th Annu. Design Autom. Conf.*, 2017, p. 9.

[21] M. T. Rahman, K. Xiao, D. Forte, X. Zhang, J. Shi, and M. Tehranipoor, "TI-TRNG: Technology independent true random number generator," in *Proc. 51st Annu. Design Autom. Conf. (DAC)*, New York, NY, USA: ACM, 2014, pp. 179:1–179:6.

[22] T. Rahman, D. Forte, J. Fahrny, and M. Tehranipoor, "ARO-PUF: An aging-resistant ring oscillator PUF design," in *Proc. Conf. Design Autom. Test Eur. (DATE)*, Leuven, Belgium, 2014, pp. 69:1–69:6.

[23] X. Zhang, N. Tuzzio, and M. Tehranipoor, "Identification of recovered ICs using fingerprints from a light-weight on-chip sensor," in *Proc. 49th Annu. Design Autom. Conf.*, 2012, pp. 703–708.

[24] A. C. Baumgarten, "Preventing integrated circuit piracy using reconfigurable logic barriers," M.S. thesis, Dept. Comput. Eng., Iowa State Univ., Ames, IA, USA, 2009.

[25] X. Wang, Y. Guo, T. Ramhan, D. Zhang, and M. Tehranipoor, "DOST: Dynamically obfuscated wrapper for split test against IC piracy," in *Proc. Asian Hardw. Oriented Secur. Trust Symp. (AsianHOST)*, 2017, pp. 1–6.

[26] D. Forte, S. Bhunia, and M. M. Tehranipoor, *Hardware Protection Through Obfuscation*. New York, NY, USA: Springer-Verlag, 2017.

[27] N. Karimi, A. K. Kanuparthi, X. Wang, O. Sinanoglu, and R. Karri, "MAGIC: Malicious aging in circuits/cores," *ACM Trans. Archit. Code Optim.*, vol. 12, no. 1, pp. 5:1–5:25, 2015.

[28] U. Guin, X. Zhang, D. Forte, and M. Tehranipoor, "Low-cost on-chip structures for combating die and IC recycling," in *Proc. 51st Annu. Design Autom. Conf. (DAC)*, 2014, pp. 87:1–87:6.

[29] X. Wang *et al.*, "Radic: A standard-cell-based sensor for on-chip aging and flip-flop metastability measurements," in *Proc. Test Conf.*, Nov. 2012, pp. 1–9.

[30] X. Wang *et al.*, "Aging adaption in integrated circuits using a novel built-in sensor," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 34, no. 1, pp. 109–121, Jan. 2015.

[31] X. Wang, M. Tehranipoor, and R. Datta, "Path-RO: A novel on-chip critical path delay measurement under process variations," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Design (ICCAD)*, Nov. 2008, pp. 640–646.

[32] X. Wang and M. Tehranipoor, "Novel physical unclonable function with process and environmental variations," in *Proc. Conf. Design Autom. Test Eur. Conf. Exhib.*, 2010, pp. 1065–1070.

[33] J. Rajendran, M. Sam, O. Sinanoglu, and R. Karri, "Security analysis of integrated circuit camouflaging," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2013, pp. 709–720.
[34] G. Mrugalski, A. Pogiel, J. Rajski, and J. Tyszer, "Fault diagnosis with convolutional compactors," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 26, no. 8, pp. 1478–1494, Aug. 2007.
[35] *Specification of ACHTERBAHN-128/80*. Accessed: Apr. 2017. [Online]. Available: http://matpack.de/achterbahn/specification.html
[36] J. Chen, S. Wang, and M. Tehranipoor, "Critical-reliability path identification and delay analysis," *ACM J. Emerg. Technol. Comput. Syst.*, vol. 10, no. 2, p. 12, 2014.
[37] M. Sadi, M. Tehranipoor, X. Wang, and L. Winemberg, "Speed binning using machine learning and on-chip slack sensors," in *Proc. 25th Ed. Great Lakes Symp. VLSI*, 2015, pp. 155–160.
[38] S. E. Quadir *et al.*, "A survey on chip to system reverse engineering," *ACM J. Emerg. Technol. Comput. Syst.*, vol. 13, no. 1, p. 6, 2016.
[39] M. Yasin, B. Mazumdar, O. Sinanoglu, and J. Rajendran, "Security analysis of anti-sat," in *Proc. 22nd Asia South Pacific Design Autom. Conf. (ASP-DAC)*, 2017, pp. 342–347.
[40] G. T. Becker, M. Fyrbiak, and C. Kison, "Hardware obfuscation: Techniques and open challenges," in *Foundations of Hardware IP Protection*. Cham, Switzerland: Springer, 2017.
[41] H. Zhou, R. Jiang, and S. Kong, "CycSAT: SAT-based attack on cyclic logic encryptions," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Design (ICCAD)*, Nov. 2017, pp. 49–56.

Dongrong Zhang is currently with Beihang University, Beijing, China, together with Dr. X. Wang. His current research interests include on-chip monitoring, physical design, and on-chip dynamic adaptation methodologies.

Dr. Zhang was honorably mentioned by the 2015 International Mathematical Contest in Modeling. He received the second and third places at the 25th Feng Ru Cup Competition of Academic and Technological for his inventions—ID Certification System Basing on Personal Movement Identification and Color Laser Projection System.

Xiaoxiao Wang (M'04) received the B.S. and M.S. degrees in electrical engineering from Beihang University, Beijing, China, in 2005 and 2007, respectively, and the Ph.D. degree in electrical and computer engineering from the University of Connecticut, Mansfield, CT, USA.

In 2010, she joined the Microcontroller Solutions Group, Design for Testability (DFT) Team, Freescale Semiconductor, Austin, TX, USA. In 2014, she joined Beihang University as a Faculty Member, where she is currently a Professor. Her current research interests include on-chip measurement architecture design, reliability, and DFT.

Md. Tauhidur Rahman (S'12–M'18) received the B.S. degree from the Bangladesh University of Engineering and Technology, Dhaka, Bangladesh, the M.S. degree from the University of Connecticut, Mansfield, CT, USA, and the Ph.D. degree in electrical and computer engineering from the University of Florida, Gainesville, FL, USA.

He is currently an Assistant Professor at the Electrical and Computer Engineering Department, University of Alabama in Huntsville, Huntsville, AL, USA, where he also directs the SeRLoP Research Lab. His current research interests include hardware security and trust, cybersecurity, Internet-of-Things security, embedded security, and reliability.

Dr. Rahman was a recipient of the two best paper awards and the Richard Newton Young Student Fellow Award in 2014.

Mark Tehranipoor (S'02–M'04–SM'07–F'18) received the Ph.D. degree from the University of Texas at Dallas, Richardson, TX, USA, in 2004.

He was the Founding Director of the Center for Hardware Assurance, Security and Engineering and the Comcast Center of Excellence for Security Innovation, University of Connecticut, Mansfield, CT, USA. He is currently the Intel Charles E. Young Preeminence Endowed Chair Professor of Cybersecurity at the University of Florida, Gainesville, FL, USA. He is also the Founding Director of the Florida Institute for Cybersecurity Research, Gainesville, FL, USA. He has published 10 books, over 20 book chapters, and over 400 journal articles and refereed conference papers. His current research interests include hardware security and trust, supply chain security, Internet-of-Things security, and VLSI design, test, and reliability.

Dr. Tehranipoor is a Golden Core Member of the IEEE Computer Society (CS) and a member of the Association for Computing Machinery (ACM) and the ACM Special Interest Group on Design Automation. He was a recipient of a dozen best paper award and nomination, including the 2008 IEEE CS Meritorious Service Award, the 2009 NSF CAREER Award, the 2012 IEEE CS Outstanding Contribution, and the 2014 AFOSR MURI Award. He co-founded the IEEE International Symposium on Hardware-Oriented Security and Trust (HOST) and served as the HOST-2008 and the HOST-2009 General Chair. He has served as the Program Chair for a number of IEEE and ACM sponsored conferences and workshops, including HOST, International Symposium on Defect and Fault Tolerance in VLSI Systems, IEEE Defect and Data Driven Testing, IEEE Defect-Based Testing, and IEEE North Atlantic Test Workshop. He serves on the program committee of over dozen leading conferences and workshops. He is currently serving as the Founding Editor-in-Chief for the *Journal of Hardware and Systems Security* and an Associate Editor for the *Journal of Electronic Testing: Theory and Applications*, the *Journal of Low Power Electronics*, the IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION SYSTEMS, and the *Transactions on Design Automation of Electronic Systems* (ACM). He has given over 175 invited talks and keynote addresses.