Probing Assessment Framework and Evaluation of Antiprobing Solutions

Huanyu Wang[®], Student Member, IEEE, Qihang Shi[®], Member, IEEE, Domenic Forte[®], Senior Member, IEEE, and Mark M. Tehranipoor, Fellow, IEEE

Abstract—Probing attacks against integrated circuits has become a serious concern, especially for security-critical applications. With the help of modern circuit editing tools, an attacker could remove layers of materials and expose wires carrying sensitive on-chip assets, such as cryptographic keys and proprietary firmware, for probing. Most of the existing protection methods use an active shield that provides tamper-evident covers at the top-most metal layers to the circuitry below. However, they lack formal proofs of their effectiveness as some active shields have already been circumvented by hackers. In this paper, we investigate the problem of protection against front-side probing attacks and propose a framework to assess a design's vulnerabilities against probing attacks. Metrics are developed to evaluate the resilience of designs to bypass an attack and reroute the attack, the two common techniques used to compromise an antiprobing mechanism. Exemplary assets from a systemon-chip layout are used to evaluate the proposed flow. The results show that long net and high layer wires are vulnerable to a probing attack equipped with high aspect ratio focused ion beam. Meanwhile, nets that occupy small area on the chip are probably compromised through rerouting shield wires. On the other hand, the multilayer internal orthogonal shield performs the best among common shield structures.

Index Terms—Assessment, focused ion beam (FIB), hardware security, physical attack, probing attack.

I. INTRODUCTION

With the rapid development of information technology and increasing reliance on electronic systems, the risk of leaking security-critical information, such as personal confidential information, commercial data, encryption keys, obfuscation keys, device configuration, and firmware stored in integrated circuits (ICs), through software- and hardware-based attacks is higher than ever. Although countermeasures against software and noninvasive hardware attacks, e.g., side channel and fault injection attacks, have been widely investigated, there is no efficient protection method against physical attacks.

Manuscript received September 27, 2018; revised December 21, 2018; accepted February 5, 2019. Date of publication April 12, 2019; date of current version May 22, 2019. This work was supported in part by NSF under Project 1717392, in part by SRC under Task ID 2769.001, and in part by AFOSR MURI under Project FA9550-14-1-0351. (*Corresponding author: Huanyu Wang.*)

The authors are with the Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL 32611 USA (e-mail: huanyuwang@ufl.edu; qihang.shi@ufl.edu; dforte@ece.ufl.edu; 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.2019.2901449

Physical attacks could circumvent encryption processes by attacking their silicon implementations to extract sensitive information from devices. Probing is one kind of physical attacks whereby an attacker makes contact with the probes at signal wires in order to extract sensitive information [1]. With the help of focused ion beam (FIB), a powerful circuit editing tool that can mill and deposit material with nanoscale precision, an attacker can also circumvent protection mechanisms and reach wires carrying sensitive information [2]. While FIB-based attacks are often considered to be restricted to very well-equipped attackers, it is now possible to rent by time or buy a secondhand FIB at very low cost. Furthermore, since failure analysis community continuously improves FIB resolution, even modern nanoscale chips cannot avoid FIB-based probing attacks. Successful probing attacks have been reported on smartcards and microcontrollers in mobile devices [3], [4], in which plaintexts, such as personal data, code format intellectual property (IP), or even encryption keys, were compromised [5].

In recent literature, various countermeasures, e.g., active shield, analog shield, and t-private circuit, have been proposed to protect security-critical circuits against front-side probing attacks that occur from the passivation layer and through upper metal layers. Active shield is the most common method, which detects milling by placing a dynamic signal carrying wire mesh as a protective shield on the top most metal layer [6], [7]. To detect the attack, a digital pattern is transmitted through the shield wires, and the received signals are compared with the same pattern from the lower metal layer. If a mismatch at a comparator is detected, an alarm is triggered, which results in a security action such as the destruction of sensitive information. Unfortunately, large area overhead and routing congestion are imposed on the design by the active shield. Furthermore, as will be demonstrated in our evaluation, a high aspect ratio FIB and its circuit edit capability can circumvent active shields [3], [4]. Analog shield, which measures analog parameters of the shield mesh, such as capacitance and delay to detect the attack, can be an alternative approach to active shield [8]. However, its main challenge is detection of the error due to process variation and environmental noise in advanced technology nodes. Reference [9] proposed the t-private circuit approach where a security-critical circuit is transformed so that at least t + 1 probes are required within one clock cycle to extract one bit of information. Although the t-private circuit increases the probing attack's difficulty and time cost, its

1063-8210 © 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

 $O(t^2)$ times area overhead for design transformation is prohibitively expensive [10]. Furthermore, the randomized encoding/decoding bits used in t-private circuits are themselves vulnerable to FIB-based tampering.

Even though back-side probing attacks, which occur through the silicon substrate rather than top-level passivation, have been proposed, security-critical designs may choose to fabricate a back-to-back 3-D IC to avoid leaving back-side exposed [6]. Therefore, protection against front-side attacks is of prime importance. Among existing countermeasures against front-side probing attacks, shield-based approaches are the most investigated. However, there has never been a formal evaluation of their overall effectiveness, especially when the high aspect ratio FIB can easily bypass the shield protection. In addition, no existing literature has investigated as to which routing layer is the best place to build the shield and detect a breach. In fact, top routing layers are known to have much wider minimum wire width and space than the lower layers, thus creating more chances for bypassing the shield with advanced FIB. This is especially true for devices, such as smartcards, which are often fabricated with the technology of larger dimensions such as 90 nm [3], [11].

In this paper, we make the following contributions:

- a framework to quantitatively assess the vulnerability of a design's layout against front-side probing attacks;
- an exposed area (EA) metric to assess the probing attack, which utilizes the space between shield wires with high aspect ratio FIB, considering three probing scenarios with different attack assumptions;
- an added trace length metric to assess the probing attack, which reroutes shield wires to open a shield-free region;
- 4) a shield structure taxonomy that summarizes existing common shield patterns from the literature;
- 5) evaluations of the proposed methodology on multiple assets from a system-on-chip (SoC) benchmark under the protection of different shield structures.

The rest of this paper is organized as follows. Section II presents a background related to probing attack and protection. Section III presents the proposed framework, and the metrics to assess bypass attack and reroute attack. In Section IV, we provide evaluation results on the proposed methodology using a SoC benchmark, before concluding the paper in Section V.

II. BACKGROUND

A number of techniques can be used to extract data from devices. One example is photon emission analysis where the photons emitted from the switching transistors are measured and analyzed, but the resolution is limited by the wavelength of infrared light ($\sim 1 \mu m$) [12]. A modern optical and electron microscopy can be used to extract the information stored in read-only memory (ROM) by observing the binary state of each cell. However, they are not applied to electrically erasable programmable ROM or flash memory because the electron distribution might be changed and thus the contents inside the memory will be disturbed [13]. Probing is another kind of physical attack, which is particularly effective for data extraction and hence warrant attention and investigation.

A. Probing Techniques

Circuit probing refers to techniques that allow an attacker to directly observe partial or full sensitive information, e.g., plaintexts or encryption keys in a chip. Signals that are more likely to be targeted in a probing attack are termed as assets. An asset is a resource of value which is worth protecting from an adversary. Probing attacks are categorized as invasive attacks because they require decapsulation, exposure of signal routing, and permanent modification of the IC. Typical probing attacks [4], [10] consist of the following steps.

The first step of the most invasive physical attacks is to either partially or fully remove the chip package in order to expose the silicon die. If the attacker does not possess the layout and/or original netlist, then full or partial reverse engineering may be needed to understand how the chip works. By studying the netlist, the attacker can identify the assets such as encryption keys, device configuration, manufacturer firmware, and obfuscation keys. One-to-one correspondence between the netlist and the layout can then determine the wires and buses to be probed as well as their exact locations, and in the event where cutting of a wire is unavoidable, determining whether the cut would impact asset extraction. The next step is locating these wires and buses in the IC sample under attack using the coordinates achieved from sacrificial devices. Some computer-aided design (CAD) tools, such as the Synopsys Camelot CAD Navigation System, could help to accurately locate and reach the target wires in the chip at nanoscale precision. An overlay of CAD layout database/graphic data system layout data can be shown in a scanning electron microscope or a FIB live image. Overlay of images from other inspection techniques, e.g., photon-emission electron microscopy, can also be used for navigation.

Wires of targeted nets that the attacker wishes to reach are likely buried under multiple passivation, metal, and dielectric layers. On ICs fabricated with feature dimensions larger than 0.35 μ m, laser cutters can be used to remove these layers to expose targeted wires for probing [1]. For technologies of lower dimensions, the most common and powerful tool is FIB [13]. With the help of a modern FIB system, such as ZEISS ORION NanoFab [14], an attacker can edit out obstructing circuitry with 5 nm level resolution [2]. The better the resolution of the FIB system, the higher the FIB aspect ratio it can achieve, and the smaller the milling hole it will create. Typical FIB systems use a gallium ion (Ga⁺) beam having spot size less than 10 nm. However, it is difficult to control the Ga ions in 10 nm level precision due to the relatively large mass of Ga⁺. Thus, the effective operational resolution for Ga-FIB is sub-100 nm. Recently, a helium ion (He⁺) beam FIB system is available [14], which is capable for nanostructuring in 5 nm level resolution [15]. However, because of the smaller mass of He⁺, the sputter rate of He-FIB is much slower than Ga-FIB.

Using FIB, a small hole can be milled in the chip to expose target wires from the lower layer as shown in Fig. 1(a). This feature indicates that many countermeasures can be disabled by simply disconnecting a few wires, and that a FIB-equipped attacker could field as many concurrent probes



Fig. 1. (a) FIB deposits Pt in the milling hole to build conducting path from target wire. (b) Deposited conducting path serves as electrical probe contact.



Fig. 2. Basic working principle of active shield and bypass attack on active shield.

as a logic analyzer allows. State-of-the-art FIBs can also deposit material in the milling hole with nanometer resolution. Platinum (Pt) or tungsten (W) gas is released from the gas injection system (GIS) nozzle at the chip surface. A highenergy ion beam can help these gas atoms to be deposited in the milling hole to build a conducting path that can serve as electrical probe contacts as shown in Fig. 1(b). When the target wire is exposed and an electrical connection is established without triggering any probing alarm from active or analog shields, the asset signals can be extracted, for example, with a nano or microprobing system.

B. Countermeasures and Limitations

In this section, we briefly review FIB/probing countermeasures and highlight their limitations. Unfortunately, to the best of our knowledge, no method has been proposed to adequately address back-side probing attacks, which is a part of our future work.

Active shield is so far the most widely used probing countermeasure. In this approach, a shield, which carries signals, is placed on the top-most metal layer to detect holes milled by FIB. As shown in Fig. 2, a digital pattern is generated from a pattern generator, transmitted through the shield wires on the top-most metal layer, and it is then compared with a copy of itself transmitted from the lower layer. If an attacker mills



Fig. 3. Probe attempt detector.

through the shield wires on the top layer to reach the lower target wire, a hole is expected to cut one or more shield wires, thereby leading to a mismatch at the comparator and triggering an alarm signal to erase or stop the generation of sensitive information. Despite its popularity, the biggest problem for active shield is that they impose large design overheads and are very vulnerable to attacks with advanced FIBs. Aspect ratio is a measure of the FIB performance defined as the ratio between depth and diameter of the milled hole [16]. A FIB with high aspect ratio can penetrate the shield with a hole of smaller diameter by leveraging the space between shield wires without damaging the shield wires, which is called bypass attack. In addition to milling, FIB is also capable of depositing conducting traces [17], which adds circuit editing to the attacker's capability. This capability allows the attacker to implement reroute attack which makes the shield wire free of cutting by rerouting a copy path between identified equipotential points. Reroute attack is a good alternative technique when it proves too difficult to bypass [3], [4]. The attacker can also completely disable the active shield by editing its control circuitry or payload. When milling and depositing in nanometer scale and applied on silicon ICs, the state-of-art FIB systems can reach an aspect ratio up to ~ 10 [18]. Another problem with the active shield method is that at least an entire metal routing layer must be dedicated to the shield, which does not go well with the designs with tight cost margin, or designs with few routing layers.

An alternative approach to active shield is to construct an analog shield. Instead of generating, transmitting, and comparing digital patterns, analog shields monitor parametric disturbances, such as capacitance, RC delay, with its mesh wires. In addition to shield designs, the probe attempt detector (PAD) [8] (as shown in Fig. 3) also uses capacitance measurement on selected security-critical wires to detect additional capacitance introduced by a metal probe. Compared to active shields, analog shields detect probing without test patterns and require a smaller area overhead. The PAD technique is also unique in remaining effective against electrical probing from the back-side. The problem with analog sensors or shields is that analog measurements are less reliable due to process



Fig. 4. Input encoder (left) and output decoder (right) for masking in t-private circuits.

and environmental variations, a problem further exacerbated by feature scaling.

Besides detecting the FIB milling directly, the FIB navigation process could also be utilized to sense the attack [19]. The charge changes on the surface of the IC during FIB navigation could be detected by an extremely sensitive local charge sensor, which could collect the charge and store the information for afterward read-out. The charge sensors can be distributed loosely on the chip and cover a wide chip region without additional cost besides area. The sensitivity of the charge sensor is the key for this detection method because the beam used for FIB navigation is very weak. However, the resilience of the charge sensor against environmental noise or power, voltage, and temperature variation is not well examined. In addition, the detection of charge sensor is not completed in real time, which needs further actions after power-up. The attacker may recover the charge density on the chip surface before power-up to avoid being detected.

The *t*-private circuit technique is proposed in [9] based on the assumption that the number of concurrent probe channels that an attacker could use is limited, and exhausting this resource thereby deters an attack. In this technique, the circuit of a security-critical block is transformed so that at least t + 1probes are required within one clock cycle to extract one bit of information. First, masking is applied to split computation into multiple separate variables, where an important binary signal, x, is encoded into t+1 binary signals by XORing it with t independently generated random signals $(r_{(t+1)} = x \oplus r_1 \oplus \cdots \oplus r_t)$ as shown in Fig. 4. Then, computations on x are performed in its encoded form in the transformed circuit. x can be recovered (decoded) by computing $x = r_1 \oplus \cdots \oplus r_t \oplus r_{(t+1)}$. The major issue with *t*-private circuit is that the area overhead involved for the transformation is prohibitively expensive. In addition, generating and protecting the random signals from being disabled by FIB is nontrivial.

C. Threat Model

In this paper, we restrict our focus to the perpendicular electrical probing on ICs from the front-side. Back-side probing, optical probing, angled (tilted) probing, and shield disabling are outside the scope of this paper, and are part of future work. The objective of the adversaries is to extract assets stored in an IC through probing attack. We further assume a strong attacker that has full layout information of the design: 1) through reverse engineering; 2) by cooperating with a rogue employee in the foundry; or 3) assuming that the foundry itself is the adversary. We presume the attack is performed by milling a hole using the FIB technology, building conducting path from the lower asset net to upper probing pad via the milling hole, and probing at the pad to extract asset information.

III. PROPOSED METHODOLOGY

A. Layout-Driven Framework to Assess Antiprobing Designs

To avoid being sidetracked by unnecessary or insufficient objectives, we first establish principles for antiprobing designs. One misconception for chip designer is that they might underestimate the capability of the attackers who are able to implement nanolevel probing using FIB. In fact, they can also perform circuit editing which allows them to disable the shield by editing its control circuit or payload [4]. Sensitive information or assets are the goal of a probing attack. However, asset sensitivity decays with time, i.e., information expires, passwords are reset, backdoors are fixed, and functional designs are phased out of market by new generations. Therefore, if delayed long enough, objectives of an attacker with even infinite resources can be rejected.

In addition to hindering attackers with advanced equipment, it is not meaningless to deter less well-equipped attackers, especially for low-cost devices, such as smartcards. Countermeasures vulnerable to the most advanced equipment might still work against attackers who do not have access to such capabilities. Customized designs instead of IPs could be used to reduce the risk when the IPs being used have been successfully attacked. Furthermore, it is necessary to keep assessing the design with the knowledge of attacks it is designed to protect against.

Considering the principles mentioned earlier, we propose the following framework to assess the vulnerability of a design to probing attacks:

- for each necessary step in a probing attack, enumerate all known alternative techniques and the capabilities required by the technique;
- estimate the expected time-cost for each technique, where time-cost is the total time needed to perform the specific technique;
- the protection against attackers with infinite resources is represented with the summation of techniques with the lowest time-cost from each necessary step;
- the protection against less well-equipped attackers can be assessed by repeating the same process without techniques requiring unavailable capabilities.

The larger the total attack time-cost is, the less vulnerable the design is against the probing attack. It is possible that a particular technique has infinite time-cost against a particular design. For example, it is almost impossible to bypass a dense active shield with low aspect ratio FIB. However, the shield can be disabled through circuit editing attack [4], so the overall time-cost is unlikely to be infinite. Fig. 5 shows a typical flow of a probing attack, where each step is shown in a row and each block shows an alternative technique to complete that step [1], [3], [4], [20]. The specific capability to enable that technique is shaded with different colors. *Disable shield* technique is represented in two blocks because it can be completed



Fig. 5. Diagram of known microprobing techniques for assessment of design vulnerability.



Fig. 6. Inputs and outputs for the assessment of bypass attack and reroute attack.

either by circuit editing or fault injection, but in both options reverse engineering is required. Techniques in white boxes that do not have a colored alternative show possible exploits from design flaws rather than lack of protection. For example, "use shield to help fine navigation" is possible if shield wires were placed in the same direction with regard to functional routing [4], and if no internal clock source is used, the attacker could simply "stop external clock" to extract all information without having to use multiple simultaneous probes.

From the proposed framework, we can see that the layout is of central importance in both restricting the attacker's options and increasing his/her time-cost. As we can see from Fig. 5, Step 3, Reach the Target Wires, is the most difficult and time-consuming step in a successful probing attack, which requires more advanced attack facilities and skills. The difficulty in this step basically determines the overall time-cost for an attack. Therefore, the method to evaluate the difficulty of different techniques in Step 3 is the key in our framework to assess the IC's vulnerability to probing attacks. In Step 3, there are typically four techniques to compromise an antiprobing design without triggering any protection mechanism. Due to the complexity and variety of disable shield and backside attacks, the method to evaluate the difficulty and measure timecost, implementing these two techniques are outside the scope of this paper and will be addressed in the future work. Hence, in this paper, we propose metrics to assess the difficulty of bypass attack and reroute attack. Fig. 6 shows the inputs and



Fig. 7. Finding MEA and EA.

outputs for the assessment of these two attacks. Possible target nets for probing attack, technology node used for fabrication, and the layout of the design are needed for both assessments. We calculated EA and added the trace length to quantify the bypass attack and reroute the attack difficulty, respectively.

B. Bypass Attack Assessment

In this section, we consider a milling scenario using the FIB technology as shown in Fig. 2, where colored bars are used to represent metal wires on different layers, assuming that the lower blue wires in Fig. 2 are on metal layer n, green wires are on metal layer n + p, top purple wires are on metal layer n + q (q > p), and the attacker wishes to probe one of the dark blue wires on layer n to extract sensitive information. The smaller hollowed-out cone shown in Fig. 2 represents a hole milled with high aspect ratio FIB equipment.

1) Classical Mode: From a layout point of view, a probing attacker is interested in the scenario where he/she could bypass the shield wires using high aspect ratio FIB and avoid complete cutting of any metal wires at the purple layer, in order to avoid its detection by the active shield. It is least likely to result in complete cutting of a wire if the milling center is located in the middle of any two shield wires. Therefore, there might exist a region around the middle line between two adjacent shield wires. If the milling center drops in this region, there are no shield wires being completely cut. We define this region as EA for probing attack. To find the EA, we calculate a distance from the far edge of the shield wire ($d_{faredge}$) [21]. In the classical mode (d_c : Classical)

$$d_c = \frac{D_{s2t} - T_s}{2R_{\rm FIB}} \tag{1}$$

where D_{s2t} is the depth from the shield layer to the target layer, T_s is the thickness of the shield wire, and R_{FIB} is the aspect ratio of FIB used by the attacker. If the milling center exists within d_c from the far edge of the shield wire, a complete cut will happen. Equation (1) shows how to find the area into which the milling center should not fall. We term this area the *milling-exclusion area* (MEA). The desired EA will be its complement. Fig. 7 shows how this area can be found for any given target wire (white) and shows covering of the wires (green and purple) on the higher layers that are capable of projecting MEA on the target wire.

2) Realistic Modes: A shortcoming of d_c is that it is too conservative as a minimum cross section of cut wire is still necessary to ensure correct signal transmission on the shield wires. Hence, we also consider two additional realistic probing attack scenarios: *exclusive mode* and *obstructive mode*.



Fig. 8. (a) Accessing target wires without cutting any shield wires (exclusive mode). (b) Accessing target wires with a part of the shield wire being cut off (obstructive mode).

Both modes can access probing target wires successfully, but at a different time-cost, and have different scope of applications. The exclusive mode probing is applicable for both active shield and analog shield designs, while the obstructive mode probing is only applicable for analog shield design.

In the exclusive mode as shown in Fig. 8(a), to avoid affecting the normal performance of shield wires, the attacker will avoid partial cutting of any shield wires. Furthermore, a minimum space (S_{s2h}) is left between the shield wire and the conducting path to minimize the effect of changed parasitic capacitance during the attack on the original timing of shield wires. In order to account for limitations of lithography and metalization, S_{s2h} is set to the same value with the minimum distance between metal wires as provided by the technology library. In addition, because of the process variation, the shield wires may be wider or thinner than ideal wire width. Hence, to guarantee the minimum space between the shield wire and the milling hole, an additional process variation margin (M_{pv} : typically 10% of wire width) is added to the width of the shield wire. Using similar calculation in (1), a violation of the exclusive mode attack will happen if the center of milling exists within d_e (exclusive mode), where

$$d_e = \frac{D_{s2t}}{2R_{\rm FIB}} + W_s + S_{s2h} + M_{\rm pv}$$
(2)

where D_{s2t} is the depth from the shield layer to the target layer, W_s is the ideal width of the shield wire, S_{s2h} is the minimum space between the shield wire and the milling hole, M_{pv} is the additional margin obtained from process variation, and R_{FIB} is the aspect ratio given by the FIB technology used by the attacker. The FIB aspect ratio would depend on the attacker's capability. Therefore, the designer has to choose a target R_{FIB} to assess the strongest level of attack. Note that the aspect ratio for milling and depositing is totally different. In general, the R_{FIB} for depositing is far less than that for milling because the gas from GIS, which is located on the top of the chip as shown in Fig. 1(a), is very difficult to reach the bottom of the hole if the hole is too narrow. Without the gas, a good conducting path cannot be built from the lower target wires. Based on recent literature on FIB capability [18], $R_{\text{FIB}} \leq 10$ would likely be sufficiently high for both milling and depositing in the near future.

In the obstructive mode, attackers have to cut off a part of the shield wire to get access to the target wire that is horizontally close to the shield wire as shown in Fig. 8(b). Nevertheless, a minimum area of shield wire cross sections should still be maintained to ensure sufficient current density to drive the load cells of the wire. Again, to keep our assessment technology independent, we choose to use the wires with similar minimum cross-sectional area as provided by any technology library; in most cases, this is found by a product of minimum width and thickness of Metal 1 interconnects. The additional process variation margin is also added to the shield wires in this mode to ensure that the sufficient cross section area is exactly achieved. Furthermore, an insulator layer as shown in Fig. 8(b), which occupies one corner of the milling hole, should be deposited around the shield wire to avoid shorting the conducting path with the shield wire. The thickness of this insulator layer should be consistent with the aforementioned minimum shield to hole space in the exclusive mode probing scenario, which could refer to the minimum metal spacing in the layout design rule. In the obstructive mode, d_{faredge} is defined as follows:

$$d_o = \frac{D_{s2t}}{2R_{\rm FIB}} + W_{s_\min} + S_{s2h} + M_{\rm pv}$$
(3)

where $W_{s_{\min}}$ is the minimum shield wire width to guarantee the sufficient current density, and other items are consistent with (2).

Comparatively, probing in the exclusive mode has a minimal effect on the chip's operation with smallest EA. As long as sufficient space between shield wires exists, detection of the wires by either the active shield or the analog shield is difficult; however, target wires, which are far away from the shield wires in horizontal direction, can only probed. In contrast, probing in the obstructive mode could probe those target wires close to the shield wires with larger EA. However, it needs to deposit one more insulator layer which takes more time and it may be detected by analog shield since the RC delay of the shield wire will be prolonged due to the partial cut-off. Hence, the exclusive mode can be typically used to attack the design with the analog shield, while the obstructive mode probing is suitable for attacking the active shield as long as the signals are transmitted correctly on the shield wires. Both probing modes cannot probe the target wires directly under the shield wires. In this case, an angled probing might be needed. Note that probing at an angle is considered out of the scope of this paper.

To successfully extract target wire's information through conducting path [see Fig. 8 (green)], a minimum contact area between the target wire and the cone-shaped conducting path

Algorithm 1 Proposed Locator Algorithm for EA.									
I	Input : targeted_nets, precision, all_layers								
0	Output: draw.script								
1 b	1 begin								
2	t	$argeted_wire_shapes \leftarrow get_net_shapes(targeted_nets)$							
3	1	$V \leftarrow \text{sizeof_collection}(targeted_wire_shapes)$							
4	f	for $(i = 1: N)$ do							
5		$targeted_wire_shape \leftarrow targeted_wire_shapes(i)$							
6		$canvas_size \leftarrow get_sizes(get_bounding_box$							
7		(targeted_wire_shape))*precision							
8		Print command in draw.script to create canvas in							
		draw.script whose size equals to canvas_size							
9		$layers_above \Leftarrow get_layers_above(all_layers,$							
		get_layerof(targeted_wire_shape))							
10		$M \Leftarrow \text{sizeof_collection}(layers_above)$							
11		for $(j = 1: M)$ do							
12		this_layer \leftarrow layers_above(j)							
13		$d_{faredge_on_thislayer} \leftarrow d_{faredge}$ (Classical,							
		Exclusive, or Obstructive)							
14		$intersecting_wire_shapes \Leftarrow$							
		get_net_shapes(targeted_nets) in							
		get_bounding_box(<i>targeted_wire_shape</i>) on							
		this_layer							
15		$L \leftarrow \text{sizeof_collection}(intersecting_wire_shapes)$							
16		for $(k = 1: L)$ do							
17		$intersecting_wire_shape \Leftarrow$							
		intersecting_wire_shapes(k)							
18		Print command in <i>draw.script</i> to create							
		projection in <i>draw.script</i> whose radius/widths							
		equals to d_faredge_on_thislayer							
19		end							
20		end							
21	e	end							
22 e	nd								

should be satisfied to guarantee the sufficient current density through the conducting path. The cross section area of Metal 1 in a technology can be used to determine this minimum contact area. If the area of a continuous EA is smaller than the minimum contact area, this EA should also not be taken as a vulnerable area to probing attack since it cannot support a good signal transmission from target wire to external probe station.

3) Finding Exposed Area of All Target Wires in a Design: Now, wires in layout designs are seldom single rectangles, but instead consist of a number of rectangular wires, usually called *shapes* by layout design tools. By iterating through each of these constituent rectangular wires, mill-exclusion areas from each intersecting wire can be projected onto each wire that may carry sensitive information and become the target of probing attack. This process is elaborated in the pseudocode as shown in Algorithm 1 [21].

In Algorithm 1, it starts with the set of target nets which are the input to the algorithm. At first, the wire shapes constituting these target nets are extracted in *targeted_wire_shapes*. Then, MEAs are to be projected onto a bitmap canvas created



Fig. 9. Exemplary results produced by proposed algorithm. (a) Exemplary targeted wire (highlighted) in layout. (b) Mill-exclusion area (black) projected on canvas of same wire.



Fig. 10. Max FIB aspect ratio that the shield can protect against.

for a specific wire shape of a target net. The *intersect-ing_wire_shapes* on each layer could be calculated using the locations of *targeted_wire_shapes* extracted from the layout design tool. A different d_{faredge} is calculated for each intersecting wire shape to find the MEA, which is then projected to the aforementioned bitmap canvas by locating ends and sides of each intersecting wire shape as shown in Fig. 9. Finally, the EA can be achieved by running the output script *draw.script* after all MEAs are projected. Considering the efficiency and adaptability of the processing steps, both canvas generation and MEA projection are stored in MATLAB scripts format.

4) Shield Security in Bypass Attack: As shown in Fig. 10, the center of the milling hole least likely to result in a d_{faredge} violation is in the center of the space between any two shield wires. This creates a restriction of milling hole diameter on the active shield layer to avoid d_{faredge} violations. The maximum diameter of the milling hole and the depth from shield layer to target layer could determine the maximum FIB aspect ratio that the shield can protect. This is an excellent indicator of the security provided by the shield. In the exclusive probing mode, the maximum FIB aspect ratio that the shield can protect against can be achieved as follows:

$$R_{FIB_e} = \frac{D_{s2t}}{P_s - W_s - 2M_{pv} - 2S_{s2h}}$$
(4)

TABLE I Exclusive Mode Shield Security in SAED32nm Library

		Shield Layer									
Target Layer	9	8	7	6	5	4	3	2			
8	0.46		N/A								
7	0.86	0.64		N/A							
6	1.26	1.28	0.64			N/A					
5	1.66	1.91	1.28	1.81		N/	A				
4	2.06	2.55	1.91	3.61	1.81 N/A						
3	2.46	3.19	2.55	5.42	3.61 4.41 N/A						
2	2.86	3.83	3.19	7.23	5.42	8.82	4.41	N/A			
1	3.26	4.47	3.83	9.04	7.23	13.24	8.82	INF			

where D_{s2t} is the depth from shield layer to target layer, P_s is the pitch size of shield layer, W_s is the width of shield wire, M_{pv} is the process variation margin, and S_{s2h} is the minimum space between shield wire and milling hole.

As shown in Fig. 10, the maximum FIB aspect ratio that the shield can protect against is defined as the depth of the milling hole over the largest diameter of the hole that it can achieve without d_{faredge} violations. The hole depth is determined by the layer of shield and target wires. The diameter of the hole is constrained by the pitch of the shield layer, which is the minimum spacing that the shield wires can achieve, and the exclusive mode probing requirements to guarantee the integrity of the shield signal. If the attacker's capability is less than the maximum FIB aspect ratio, the probing attack cannot be implemented successfully without violating the exclusive mode probing requirements.

Table I shows the maximum FIB aspect ratio that the single layer shield can protect in the exclusive probing mode when the shield layer and the target layer vary using the layout parameter from the Synopsys SEAD32nm Library. High layer shield may benefit from the large shield layer to target layer depth, but the wide pitch may result in a large hole diameter. Similarly, low layer shield has a small hole diameter, but the hole depth will decrease accordingly. Therefore, the shield security is technology dependent. Considering the Synopsys SEAD32nm Library, the highlighted cells in Table I show the best shield layer for protecting target wires across layers. The infinite cell in Table I means that no FIB can bypass the shield on the corresponding layer under the exclusive probing mode. Since we are only considering front-side probing, it is not applied (N/A) when target layer is higher than shield layer.

Similarly, the max FIB aspect ratio that the shield can protect against in obstructive probing mode can be achieved as follows:

$$R_{FIB_o} = \frac{D_{s2t}}{P_s - W_{s_{\min}} - 2M_{pv} - 2S_{s2h}}$$
(5)

where $W_{s_{\min}}$ is the minimum shield wire width to guarantee the current density. Since $W_{s_{\min}}$ is less than W_s , R_{FIB_o} is smaller than R_{FIB_e} , which means that the shield is more vulnerable in obstructive probing mode than in exclusive probing mode as shown in Table II. The difference between Tables I and II is not too much because in SAED32nm library, W_s on M2 ~ M8 is only 6 nm wider than $W_{s_{\min}}$.

Tables III and IV show the shield security in SAED90nm library for exclusive and obstructive modes, respectively. Com-

TABLE II Obstructive Mode Shield Security in SAED32nm Library

	Shield Layer									
Target Layer	9	8	7	6	5	4	3	2		
8	0.46		N/A							
7	0.86	0.63	N/A							
6	1.26	1.27	0.63	N/A						
5	1.66	1.90	1.27	1.78	78 N/A					
4	2.06	2.54	1.90	3.55	1.78 N/A					
3	2.46	3.17	2.54	5.33	3.55	4.23 N/A				
2	2.86	3.81	3.17	7.10	5.33	8.45	4.23	N/A		
1	3.26	4.44	3.81	8.88	7.10	12.68	8.45	INF		

TABLE III Exclusive Mode Shield Security in SAED90nm Library

	Shield Layer									
Target Layer	9	8	7	6	5	4	3	2		
8	0.40		N/A							
7	0.64	0.27	N/A							
6	0.88	0.54	0.43	0.43 N/A						
5	1.12	0.80	0.87	1.13	N/A					
4	1.36	1.07	1.30	2.25	1.13	13 N/A				
3	1.60	1.34	1.73	3.38	2.25	5.63 N/A				
2	1.84	1.61	2.16	4.50	3.38	11.25	5.63	N/A		
1	2.07	1.88	2.60	5.63	4.50	16.88	11.25	INF		

TABLE IV
OBSTRUCTIVE MODE SHIELD SECURITY IN SAED90NM LIBRARY

	Shield Layer									
Target Layer	9	8	7	6	5	4	3	2		
8	0.35		N/A							
7	0.55	0.26		N/A						
6	0.76	0.53	0.42	N/A						
5	0.96	0.79	0.85	1.07		N/	A			
4	1.17	1.06	1.27	2.14	2.14 1.07 N/A					
3	1.37	1.32	1.70	3.21 2.14 4.50 N/A						
2	1.58	1.59	2.12	4.29	3.21	9.00	4.50	N/A		
1	1.78	1.85	2.55	5.36	4.29	13.50	9.00	INF		

pared with the 32nm library as shown in Tables I and II, the shield security in SAED90nm technology is lower, which indicates it is more vulnerable to probing attack mainly because of the larger pitch size. Furthermore, it is very clear in the SAED90nm library that the shield is more vulnerable to probing attacks in the obstructive mode than that in the exclusive mode. Note that, according to (1) \sim (5), these assessments are functions of many factors such as pitch size, metal width, and thickness of dielectric between layers. Therefore, technologies with the similar feature size and different dielectric thickness values may result in a large disparity in terms of the vulnerabilities to probing attack. Generally, as for shield security is concerned, smaller technology node may benefit from the smaller pitch size, while larger technology node may benefit from the larger dielectric thickness. Thus, without a specific design rule of a technology, it is difficult to report the vulnerability of the probing attack.

C. Reroute Attack Assessment

Though bypass attack using low aspect ratio FIB could be effectively deterred by building thin and dense active shield, do not forget FIB's circuit editing capability that



Fig. 11. Classification of shield structures.



Fig. 12. Single-layer shields: (a) snake-like wires and (b) parallel wires. Two-layer shields: (c) orthogonal and (d) parallel.

allows attackers to only use low aspect ratio FIB and build a copy path between two equipotential points, as shown in Fig. 12(a) and (b), so that the original shield wire would be free of cutting [3], which is called reroute attack. Bypass attack utilizes the small footprint of high aspect ratio FIB and the limited space between shield wires to access target nets below, while reroute attack breaks the shield wire space limit by only using low aspect ratio FIB to reconnect shield wires above top metal layer to avoid detection. Despite being more powerful, reroute attack requires more work on building vias and adding traces. The difficulty to perform reroute attack on active shield varies with the structure of shield. In this section, we develop a metric to assess the shield's vulnerability to reroute attack by the calculation of length of added traces.

1) Shield Structure Classification: The active shield to protect a chip against probing attack can take many structures. We decompose the shield structures into two principal categories according to the number of layers that the shield occupies as shown in Fig. 11.

In single layer category, the shield structures are further classified into two subcategories by the shape of shield wires: snake-like wires and parallel wires. The snake-like shield, as shown in Fig. 12(a), can cover a large surface area on



Fig. 13. Reroute attack on single-layer shields. (a) Snake-like wires. (b) Parallel wires.

the chip with only few driving signals [22]. However, it is very vulnerable to the same layer reroute attack, which forces active shield designs to use only parallel wires to make the same layer reroute much harder [6].

In multiple layer category, the shield structures are further partitioned into three groups by the relative position of shield wires at upper and lower layers. Two-layer orthogonal shield and parallel shield are composed with two single-layer parallel shields but at different angles as shown in Fig. 12(c) and (d), respectively. To get the optimal protection, the two-layer orthogonal shield usually keeps the minimal width and spacing for each single layer shield (the width and spacing of shield wires at different layer may vary). However, to achieve a comprehensive protection from two-layer parallel shield, the pitch size for upper layer shield and lower layer shield are maintained the same. In addition, a 50% offset may add to the lower layer shield of a two-layer parallel shield to increase the overall coverage as shown in Fig. 12(d). To make the geometry of the shield difficult to recognize, random active shield was proposed in [22]. The random active shield typically occupies two routing layers with randomized spaghetti routing, which is actually a random mixture of two-layer orthogonal and parallel shields. It could deter the probing attacker who has limited knowledge of the design's layout to a certain degree.

2) Added Traces Length: We develop a metric to evaluate reroute attack difficulty on different shield structures based on the calculation of added traces length. As an example shown in Fig. 13(a), to open a 3×3 pitch² unprotected area on a single layer snake-like shield, two traces with two pitches long in total need to be added on the same layer with shield to short shield wires. If the same layer rerouting is not available, two vias at the ends of each added traces need to be created to build connecting path from shield wires on lower layer to added traces on upper layer. Similarly, to open a 3×3 pitch² unprotected area on a single layer parallel shield, six vias and three traces with 14 pitches long in total need to be added on the shield as shown in Fig. 13(b). If considering a two-layer orthogonal or parallel shield, the areas which need to be opened are a 6×6 pitch² region on upper layer and a 3×3 pitch² area on lower layer.

In a more general case, to open a $n \times n$ pitch² area on a shielded design by reroute attack, Table V shows the cost

TABLE V
REROUTE ATTACK DIFFICULTY FOR DIFFERENT SHIELD STRUCTURES

Shield Structure	Vias	Traces	Trace Length
	0	(n+1)/2, n is odd n/2, n is even	(n+1)/2, n is odd n/2, n is even
	2n	n	$(5n^2-4n+3)/2$, n is odd $(5n^2-4n)/2$, n is even
	2n on lower shield 4n on upper shield 6n in total	n on lower shield 2n on upper shield 3n in total	$(25n^2-12n+3)/2$, n is odd $(25n^2-12n)/2$, n is even

for different shield structures by induction. The number of vias, number of traces, and total length of added traces are calculated in this metric. The longer the added traces, the more time and complexity to perform reroute attack. As we can see from Table V, the single layer snake-like shield is the most vulnerable one against reroute attack with complexity of just O(n). Although two-layer shield and single-layer parallel shield have the same reroute attack complexity, which is $O(n^2)$, generally two-layer shield in terms of added trace length.

Since there is no uniform structure for random active shield, its reroute attack complexity is not calculated here. However, as mentioned in [22], if the layout of the design is known to attackers, the random shielding approach should not deter better than regular shield. Hence, it is safe to conclude that the reroute attack complexity of random active shield is not higher than the regular two-layer shield as listed in the last row of Table V, which is $O(n^2)$.

IV. EVALUATION RESULTS

In this section, we present the evaluations on the proposed assessment method of bypass attack and reroute attack on shielded designs. The objective is to find out how difficult to perform a typical probing attack in antiprobing designs under different shield structures. For this purpose, the layout of a SoC using Synopsys SAED 32 nm technology library is chosen for the methodology to inspect. Fig. 14(a) shows the architecture of the SoC. This SoC is developed by the Massachusetts Institute of Technology [23] and the register-transfer level descriptions of the SoC are from GitHub [24]. This SoC contains one OpenRISC processor, one DSP core, one AES encryption core, one SPI controller, one Arbiter data bus structure, and one clock generator. The OpenRISC OR1200 processor is randomly obfuscated with 64 locking gates [25].

A. Evaluation of Bypass Attack

1) Three Case Studies: For the purpose of assessing bypass attack difficulty, three groups of nets are selected to serve as targeted wires: encryption key nets in AES module, data bus nets form OpenRISC processor to AES, and obfuscation key nets in OpenRISC processor, as shown in Fig. 14(b). The keys of an encryption module are archetypal assets. If the key is leaked, the root of trust it provides will be compromised, and may serve as a gateway to more damaging attacks. Hence, key



Fig. 14. (a) Diagram of the SoC used to evaluate our algorithm. (b) Three probing target groups: encryption key nets, data bus nets, and obfuscation key nets.

nets are very likely to be targeted in a probing attack. Usually, the key values are stored in nonvolatile memory on the chip and transferred by the processor through data bus, and hence data bus nets could also serve as prime targets in probing attacks. Indeed, many assets, such as firmware, configuration data, and confidential data, are all transferred among modules through data bus, which makes data bus nets to become the best probing attack target. Furthermore, data bus nets tend to be long and wide as shown in Fig. 14(b), which leaves a huge probing opportunity for attackers. There are many data bus nets in an SoC; however, we only take 32-bit data bus nets from processor to AES as an example in this paper. With

TABLE VI MINIMUM SPACING BETWEEN SHIELD AND MILLING HOLE

Milling Hole Diameter	Min. Shield to Hole Spacing
$< 0.15 \ \mu { m m}$	$0.056 \ \mu \mathrm{m}$
$< 0.3 \ \mu \mathrm{m}$	0.064 µm
$< 1.5 \ \mu \mathrm{m}$	0.11 μm
$< 3 \ \mu m$	0.6 µm
\geq 3 μ m	0.7 µm



Fig. 15. (a) Total EA of encryption key nets across FIB aspect ratio in three probing modes. (b) Average EA per net of three target groups. (c) Ratio of EA over the total target nets area. (d) Average net length of three target groups.

the development of globalization in semiconductor industry, obfuscation technologies might be used in the design to prevent unauthorized usage of third-party IPs and unauthorized production of ICs [26], which makes the obfuscation key nets another potential target in probing attacks.

For evaluation, Equations (1)-(3) are used to calculate the dfaredge in classical, exclusive, and obstructive modes, respectively. The physical parameters of the layout are retrieved from Synopsys SAED32 nm technology library. The process variation margin for both shield and target wires are taken to be 10% of the wire width. The minimum shield to hole spacing is referring the layout design rules of the technology as shown in Table VI. Also, we use a resolution of 10 nm, and we assume the maximum $R_{\text{FIB}} = 10$. Fig. 15(a) shows the total EA of encryption key nets across FIB aspect ratio in three different probing modes. The classical probing mode has the largest EA when assumed that the shield wires with the shortest d_{faredge} are completely cut off. In more realistic probing modes, the EA of obstructive probing is just a little bit larger than exclusive probing because, in SAED32nm technology, the metal width of M2 to M8 is only 6 nm wider than the metal width of M1 which is used as the minimal metal width to guarantee the current density on shield wires. If the metal width in other technology differs a lot among different metal layers, the EA difference between obstructive probing mode and exclusive probing mode will be more notable. Considering the small metal width difference in SAED32nm



Fig. 16. (a)–(c) Layer distribution of routing length for data bus nets, encryption key nets, and obfuscation key nets, respectively. (d) Exposed ratio across metal layers for three target groups when FIB aspect ratio is 5.

TABLE VII Shield Structure Configurations

No.	Shield	Layer(s)	Wire Width (nm)	Pitch (nm)	Direction
1	Single Layer	M6	56	608	Vertical
2	Single Layer	M7	56	1216	Horizontal
3	Single Layer	M8	56	1216	Vertical
4	Single Layer	M9	160	2432	Horizontal
5	Two-layer	M6	56	608	Vertical
5	Orthogonal	M7	56	1216	Horizontal
6	Two-layer	M7	56	1216	Horizontal
0	Orthogonal	M8	56	1216	Vertical
7	Two-layer	M8	56	1216	Vertical
/	Orthogonal	M9	160	2432	Horizontal
0	Two-layer	M6	56	1216	Vertical
0	Parallel	M8	56	1216	Vertical
0	Two-layer	M7	56	2432	Horizontal
9	Parallel	M9	160	2432	Horizontal

technology, in the rest of this paper, the EA is only calculated in exclusive probing mode.

Fig. 15(b) shows the average EA per net of three target groups across FIB aspect ratio and Fig. 15(c) shows the ratio of EA over the total area of target nets for three target groups. As we can see from Fig. 15(b) and (c), data bus nets have much more EA and exposed ratio than encryption key and obfuscation key nets, which indicates data bus nets are most vulnerable to probing attack. Meanwhile, encryption key nets have the minimum EA and exposed ratio, which represents the minimal probing attack threat among three target groups, and the probing vulnerability of obfuscation key nets are in the middle. Fig. 15(d) shows the average net length of three target groups and Fig. 16(a)–(c) shows the layer distribution of routing length for three target groups. As we can see from Fig. 15(d) and Fig. 16(a)–(c), data bus nets have longer net length and are positioned in higher metal layers, while

No.	Enc. Key		Data Bus			Obf. Key			All Target			
	Vias	Traces	Length (mm)	Vias	Traces	Length (mm)	Vias	Traces	Length (mm)	Vias	Traces	Length (mm)
1	494	247	93	2140	1070	1739	594	297	134	2304	1152	2016
2	248	124	47	1070	535	869	298	149	68	1152	576	1008
3	248	124	47	1070	535	869	298	149	68	1152	576	1008
4	124	62	24	536	268	436	150	75	34	576	288	503
5	990	495	279	4280	2140	5217	1190	595	403	4608	2304	6048
6	744	372	233	3210	1605	4347	894	447	337	3456	1728	5039
7	496	248	140	2142	1071	2613	598	299	204	2304	1152	3022
8	744	372	233	3210	1605	4347	894	447	337	3456	1728	5039
9	372	186	116	1608	804	2180	450	225	170	1728	864	2518

TABLE VIII Reroute Attack Assessment on Different Shield Structures

encryption key nets have shortest net length and more low layer wires. Hence, the large EA of data bus nets are probably because they have much longer net length and over 50% of wires are routed on upper layers (M7, M8, M9). Fig. 16(d) reconfirms this conclusion, which shows the exposed ratio across layers for three target groups when FIB aspect ratio is 5. As we can see, generally, higher layer has higher exposed ratio, which indicates they are more vulnerable to probing attack.

2) Evaluation of Different Shield Structures: This evaluation investigates the protection efficiency of shield with different structures at different layers against bypass attack in the exclusive mode. The evaluations are performed on the same layout as shown in Fig. 14 but under shield with different structures as illustrated in Section III-C1. The existing wires on the shielding layers will be removed. To avoid removal of target net wires, encryption key nets are used as target nets in this evaluation as all encryption key nets are routed under M5 as shown in Fig. 16(b). Single-layer shield, two-layer orthogonal shield, and two-layer parallel shield are all evaluated in this section. Shield structure configurations are shown in Table VII, which specifies the layer(s) of the shield, wire width, pitch, and direction in the technology library. Shields 1–4 are single-layer shields, Shields 5-7 are two-layer orthogonal shields, and Shields 8 and 9 are two-layer parallel shields. Minimum pitch size is maintained in single-layer and two-layer orthogonal shield structures. However, in two-layer parallel shield, pitch of lower layer shield is set to match the upper layer shield pitch to build the periodic parallel structure with constant 50% offset to upper layer shield.

Fig. 17(a)–(c) shows the EA of designs under single-layer shield, two-layer orthogonal shield, and two-layer parallel shield at different layers, respectively. As we can see, shield on M6 is the best among single-layer shields, which is consistent with the shield security analysis in Table I. Among two-layer orthogonal shield structures, the design with shield on M6/M7 has the minimal EA. Among two-layer parallel shield structures, the design with shield on M6/M8 is the best with minimal EA. Fig. 17(d) compares the EA result of designs under the optimal shield structure in each category. As we can see, a two-layer orthogonal shield on M6/M7 is the best shield structure in all designs taking advantage of multilayer shielding and minimum pitch on M6. In addition, the protection from two-layer parallel shield on M6/M8 is not significantly better than single-layer shield on M6. It is because to build the periodic parallel shield structure, the minimum pitch on M6 is



Fig. 17. (a) EA of designs under single-layer shield. (b) EA of designs under two-layer orthogonal shield. (c) EA of designs under two-layer parallel shield. (d) EA of designs under optimal shield in each category.

sacrificed to match the pitch size on M8. Therefore, by comparing the EA of designs under different shield structures, we find the two-layer orthogonal shield is the best against bypass attack. However, compared with the no shield result, protection of active shield does not decrease the EA a lot with considerable EA left, which indicates the active shield approach is not quite efficient.

B. Evaluation of Reroute Attack

The reroute attack vulnerability of different probing targets and the resilience of different shield structures against reroute attack are evaluated. The same layout [see Fig. 14(b)], target nets definition (encryption key nets, data bus nets, and obfuscation key nets), and shield structures (see Table VII) discussed in Section IV-A are still used for investigation in this section. Table VIII shows the cost to reroute shield wires and expose corresponding target nets area for different shield structures. The number of vias, number of traces, and total length of added traces are calculated for different target nets and different shield structures in Table VIII.

One interesting observation from Table VIII is that data bus nets are the least vulnerable against reroute attack with highest attack cost among all three target groups, while they are the most vulnerable one against bypass attack as discussed in Section IV-A. It is because data bus nets are relative long and occupy a large area on the chip, which involves more shield wires to be rerouted and thus increase the cost. In turn, encryption key nets, which occupy a relative small region on the chip and have the smallest EA to bypass attack, take the least cost to perform a reroute attack. It indicates that when bypass attack is not available or too expensive, reroute attack might be a good alternative approach in a probing attack.

By comparing the reroute attack cost for different shield structures, Shields 1, 5, and 8 are still the optimal shield structures against reroute attack in respective category, which is consistent with bypass attack results. Furthermore, Shield 5, which is the two-layer orthogonal shield on M6 and M7, is still the overall best shield against reroute attack. Hence, weighing up all results from bypass attack assessment and reroute attack assessment, we find that among all discussed shield structures, generally, shield consisted of intermediate layers is better than shield consisted of top layers, two-layer shield is better than one-layer shield, and orthogonal shield is better than parallel shield. When considering active shield designs for future products, IC designers could use the proposed probing assessment framework to evaluate the protection of different shield solutions using the technology library parameters of the design under evaluation and choose the design with minimum EA and added trace length to maximize the resistance against probing attack.

V. CONCLUSION

To the best of our knowledge, the proposed framework provides the first quantifiable way to verify and evaluate realistic probing vulnerabilities. In this paper, we presented a comprehensive layout-driven framework to assess designs for vulnerabilities to probing attacks. An EA-based metric is developed to evaluate bypass attack and an added trace length-based metric is developed to assess reroute attack in realistic probing scenarios. We further summarize common shield structures. An SoC benchmark with different shield structures are evaluated using the proposed methodology. The results show that long net and high layer wires are vulnerable to bypass attack. Meanwhile, nets that occupy small area on the chip are probably compromised through reroute attack. On the other hand, multilayer internal orthogonal shield performs the best against both the bypass and reroute attacks among all the discussed shield structures, but still it does not completely protect the assets.

REFERENCES

- S. Skorobogatov, "Physical attacks on tamper resistance: Progress and lessons," in *Proc. 2nd ARO Special Workshop Hardw. Assurance*, Washington, DC, USA, 2011, pp. 1–37.
- [2] V. Sidorkin, E. van Veldhoven, E. van der Drift, P. Alkemade, H. Salemink, and D. Maas, "Sub-10-nm nanolithography with a scanning helium beam," *J. Vac. Sci. Technol. B, Microelectron.*, vol. 27, no. 4, pp. L18–L20, 2009.
- [3] C. Tarnovsky. Tarnovsky Deconstruct Processor. Accessed: Apr. 3, 2019.
 [Online]. Available: https://www.youtube.com/watch?v=w7PT0nrK2BE
- [4] V. Ray, "Freud applications of fib: Invasive fib attacks and countermeasures in hardware security devices," in *Proc. East-Coast Focused Ion Beam User Group Meeting*, Feb. 2009, pp. 2–28.
- [5] R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems. Hoboken, NJ, USA: Wiley, 2001.
- [6] J.-M. Cioranesco et al., "Cryptographically secure shields," in Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust (HOST), May 2014, pp. 25–31.

- [7] M. Ling, L. Wu, X. Li, X. Zhang, J. Hou, and Y. Wang, "Design of monitor and protect circuits against FIB attack on chip security," in *Proc.* 8th Int. Conf. Comput. Intell. Secur. (CIS), Nov. 2012, pp. 530–533.
- [8] S. Manich, M. S. Wamser, and G. Sigl, "Detection of probing attempts in secure ICs," in *Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust* (HOST), Jun. 2012, pp. 134–139.
- [9] Y. Ishai, A. Sahai, and D. Wagner, "Private circuits: Securing hardware against probing attacks," in *Advances in Cryptology—CRYPTO*. New York, NY, USA: Springer, 2003, pp. 463–481.
- [10] H. Wang, D. Forte, M. M. Tehranipoor, and Q. Shi, "Probing attacks on integrated circuits: Challenges and research opportunities," *IEEE Des. Test*, vol. 34, no. 5, pp. 63–71, Oct. 2017.
 [11] Y. K. Lee *et al.*, "2T-FN eNVM with 90 nm logic process for smart
- [11] Y. K. Lee et al., "2T-FN eNVM with 90 nm logic process for smart card," in Proc. Joint Non-Volatile Semicond. Memory Workshop Int. Conf. Memory Technol. Design, 2008, pp. 26–27.
- [12] C. Boit, "Fundamentals of photon emission (PEM) in siliconelectroluminescence for analysis of electronic circuit and device functionality," in *Microelectronics Failure Analysis: Desk Reference*. 2004, pp. 356–368.
- [13] 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.
- [14] ZEISS ORION NanoFab. Accessed: Apr. 3, 2019. [Online]. Available: https://www.zeiss.com/microscopy/us/products/multipleion-beam/orion-nanofab-for-materials.html
- [15] O. Scholder, K. Jefimovs, I. Shorubalko, C. Hafner, U. Sennhauser, and G.-L. Bona, "Helium focused ion beam fabricated plasmonic antennas with sub-5 nm gaps," *Nanotechnology*, vol. 24, no. 39, 2013, Art. no. 395301. [Online]. Available: http://stacks.iop.org/0957-4484/24/i=39/a=395301
- [16] Y. Fu and K. A. B. Ngoi, "Investigation of aspect ratio of hole drilling from micro to nanoscale via focused ion beam fine milling," in *Proc.* 5th Singapore-MIT Alliance Annu. Symp., 2005, pp. 1–5.
- [17] H. Wu *et al.*, "Focused helium ion beam deposited low resistivity cobalt metal lines with 10 nm resolution: Implications for advanced circuit editing," *J. Mater. Sci., Mater. Electron.*, vol. 25, no. 2, pp. 587–595, 2014.
- [18] H. Wu, D. Ferranti, and L. Stern, "Precise nanofabrication with multiple ion beams for advanced circuit edit," *Microelectron. Rel.*, vol. 54, no. 9, pp. 1779–1784, 2014.
- [19] C. Helfmeier, C. Boit, and U. Kerst, "On charge sensors for FIB attack detection," in *Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust (HOST)*, Jun. 2012, pp. 128–133.
- [20] C. Tarnovsky, "Security failures in secure devices," Black Hat Briefings, vol. 74, Feb. 2008, pp. 2–54.
- [21] Q. Shi, N. Asadizanjani, D. Forte, and M. M. Tehranipoor, "A layoutdriven framework to assess vulnerability of ICs to microprobing attacks," in *Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust (HOST)*, May 2016, pp. 155–160.
- [22] S. Briais, J.-M. Cioranesco, J.-L. Danger, S. Guilley, D. Naccache, and T. Porteboeuf, "Random active shield," in *Proc. Workshop Fault Diagnosis Tolerance Cryptogr. (FDTC)*, Sep. 2012, pp. 103–113.
- [23] Massachusetts Institute of Technology. Accessed: Apr. 3, 2019. [Online]. Available: https://www.mit.edu/
- [24] *GitHub*. Accessed: Apr. 3, 2019. [Online]. Available: https://github.com/mit-ll/CEP
- [25] M. Yasin, J. Rajendran, O. Sinanoglu, and R. Karri, "On improving the security of logic locking," *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, vol. 35, no. 9, pp. 1411–1424, Sep. 2016.
- [26] D. Forte, S. Bhunia, and M. M. Tehranipoor, *Hardware Protection Through Obfuscation*, 1st ed. Springer, 2017.



Huanyu Wang (S'16) received the B.S. degree from the Huazhong University of Science and Technology, Wuhan, China, in 2014, and the M.S. degree in electrical engineering from Northwestern University, Evanston, IL, USA, in 2016. He is currently working toward the Ph.D. degree in computer engineering at the Florida Institute for Cyber Security, University of Florida, Gainesville, FL, USA.

His current research interests include hardware security and trust, VLSI CAD, VLSI physical design, and clam chowder recipe.



Qihang Shi (S'10–M'17) received the Ph.D. degree in computer engineering from the University of Connecticut, Mansfield, CT, USA, in 2017.

He is currently a Postdoctoral Associate with the Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL, USA. His research interests include hardware security and trust, and VLSI test and reliability.



Domenic Forte (S'09–M'13–SM'18) received the B.S. degree in electrical engineering from the Manhattan College, Riverdale, NY, USA, in 2006, and the M.S. and Ph.D. degrees in electrical engineering from the University of Maryland at College Park, College Park, MD, USA, in 2010 and 2013, respectively.

He is currently an Assistant Professor with the Electrical and Computer Engineering Department, University of Florida, Gainesville, FL, USA. His current research interests include the domain of

hardware security, including the investigation of hardware security primitives, hardware Trojan detection and prevention, electronics supply-chain security, and antireverse engineering.

Dr. Forte was a recipient of the Young Investigator Award from the Army Research Office, the NSF CAREER Award, and the George Corcoran Memorial Outstanding Teaching Award from the Electrical and Computer Engineering Department, University of Maryland. His work has also been recognized through several best paper awards and nominations from venues, such as HOST, DAC, and AHS. He is serving on the organizing committees of HOST and AsianHOST and the technical program committee of several other top conferences. He was the Guest Editor of the IEEE Computer Special Issue on Supply-Chain Security for Cyberinfrastructure. He is currently serving as an Associate Editor for the *Journal of Hardware and Systems Security*.



Mark M. 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 for CHASE and CSI centers at the University of Connecticut, Mansfield, CT, USA. He is currently the Intel Charles E. Young Preeminence Endowed Chair Professor in Cybersecurity with the University of Florida, Gainesville, FL, USA. He is currently serving as a Founding Director of the Florida Institute for Cybersecurity Research, Gainesville, FL, USA. He has published

over 400 journal articles and refereed conference papers and has given about 200 invited talks and keynote addresses. He has published 11 books and more than 20 book chapters. His current research interests include hardware security and trust, supply chain security, IoTs Security, and VLSI design, test, and reliability.

Dr. Tehranipoor is a Golden Core Member of the IEEE Computer Society (CS) and a member of ACM and ACM SIGDA. He was a recipient of a dozen best paper awards and nominations, as well as the 2008 IEEE CS Meritorious Service Award, the 2012 IEEE CS Outstanding Contribution, the 2009 NSF CAREER Award, and the 2014 AFOSR MURI Award. He serves on the program committee of more than a dozen leading conferences and workshops. He has also served as the Program Chair of a number of IEEE and ACM sponsored conferences and workshops (HOST, ITC, DFT, D3T, DBT, and NATW). He co-founded the IEEE International Symposium on Hardware-Oriented Security and Trust (HOST) and served as an HOST-2008 and HOST-2009 General Chair. He is currently serving as the Founding Editor-in-Chief for the Journal on Hardware and Systems Security and the 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 ACM Transactions on Design Automation of Electronic Systems.