iPROBE V2: Internal Shielding-based Countermeasures against Both Back-side and Front-side Probing Attacks*

Minyan Gao, Huanyu Wang, Mark M. Tehranipoor, and Domenic Forte

***Abstract*—Microprobing attacks poses a serious threat to security-critical applications by enabling attackers to steal assets and/or secrets within integrated circuits (ICs). With the assistance of focused ion beam (FIB), microprobing attacks are even more powerful. Although there are some existing countermeasures like active shields, analog shields, and t-private circuits, the FIB's capabilities are not taken into consideration and thus these countermeasures are inefficient and only provide limited resistance against the FIB-enhanced microprobing attacks. To counter the attack, we previously proposed a FIB-aware anti-probing physical design flow that utilizes computer-aided design (CAD) tools to detect and prevent microprobing attack from the IC front-side with minimal extra design effort. In this paper, we expand this flow to protect not only front-side of the IC, but provide simultaneous protection of both front-side and back-side. Results in an Advanced Encryption Standard (AES) benchmark show that, by using the proposed flow, the vulnerable area exposed to front-side probing on security-critical nets is reduced to zero at low FIB aspect ratios with less than 2% timing and area overhead.**

I. Introduction

The growing threat of physical attacks on integrated circuits (ICs) is a major concern for security-critical applications. In particular, focused ion beam (FIB) is a powerful circuit editing tool, with which the material can be milled or deposited on silicon dies with sub-10-nm level precision [1], [2]. Using FIB, an attacker can extract an asset's value by milling to its location in the IC layout, creating a metal contact to it, and later probing the contact while the chip runs.

In recent literature, various countermeasures have been proposed to protect security-critical applications from microprobing attacks, which can be classified into two categories: prevention- and detection-based approaches. The preventive strategy incorporates active or analog shields as meshes while the detection strategy monitors for attacks by sensing any mechanical thinning, FIB deposition, microprobing or circuit editing and raising an alarm. A widely studied and implemented prevention-based approach, active shield, detects hardware tampering by building a mesh of shield wires that covers the entire design in the top-most layers pf the IC. Another prevent-based strategy, anti-tamper active shield, was proposed in [3], which is a random plane that is built in top level metal over specific IP or sensitive areas of the ASIC. The assets will be erased upon the detection of probing attempts, i.e., when the shield is damaged. For the detection-based approaches, they rely on the ability to detect disturbances such as the capacitance, delay, etc. To this end, sensors such as Probe Attempt Detector (PAD) [4], Low Area Probing Detector (LAPD) [5] and Calibratable Detector (CaLIAD) [6] have been proposed. In addition to hardware-based detection approaches, one cryptographic approach called t-private circuits [7] modifies the circuit so that at least $t+1$ probes are required to extract one bit of information. However, its high area overhead makes it less practical.

The prohibitive area, timing, and power overhead are among the main issues of common countermeasures against probing attacks. [8] proposed an approach that can be easily incorporated into the conventional ASIC design flow in order to protect the ICs security-critical applications from FIB-based front-side probing attack with limited overhead, but the back-side of the IC is still unprotected. Here, we mainly focus on contact-to-metal probing attacks. Front-side and back-side refers to the side of the IC that contains the metallization and the side consists solely of the silicon substrate respectively. In this paper, we propose a comprehensive countermesaure against both front-side and back-side probing attacks. Our major contributions are summarized as follows:

- We develop a metric to identify the 'best' shield layers, i.e., the one that can provide the optimal protection to assets from both front-side and back-side probing attack.
- We exploit the transistor shielding capabilities for the back-side vulnerability assessment.
- We evaluate AES modules with different level of protections: without any protection, with only front-side protection, with only backside protection, and with both front-side and back-side protection. Results show that the proposed approach can reduce the front-side vulnerable area exposed to probing to zero for lower FIB aspect ratios with less than 2% timing and area overhead and less than 8% power overhead.

The rest of this paper is organized as follows. Section II describes the threat model. Section III illustrates the anti-probing design flow, including shield layer identification and vulnerability assessment. Section IV discusses the results and Section V concludes the paper.

II. THREAT MODEL

In this paper, we concentrate on electrical probing from both the front-side and back-side of the IC and we intend to deter the attackers who aim to extract assets stored in a device through electrical probing attacks with advanced circuit edit tools such as FIB. We assume a strong attacker who has full layout information of the design, by either reverse engineering or obtaining it from an untrusted foundry. We also assume attack detection to be conservative, i.e., a complete cut on the shield net is required to be detected by the proposed countermeasure due to the low reliability of partial cuts detection.

III. ANTI-PROBING DESIGN FLOW

Our objective is to develop a FIB-aware anti-probing physical design flow that incorporates automated security-aware floor-planning, cell placement, and routing steps into the conventional ASIC design flow, for the protection of the security-critical nets in a design against *both* front-side and back-side probing attacks.

*This work was supported in part by Semiconductor Research Corporation (SRC) and National Science Foundation (NSF).

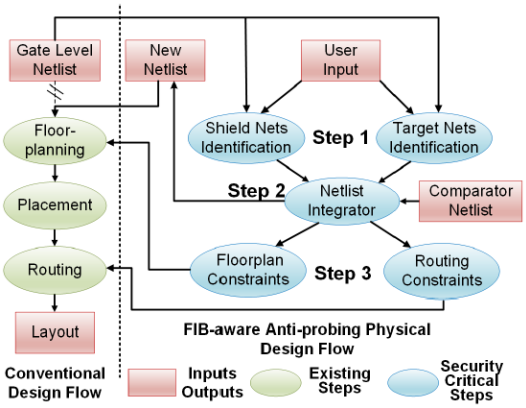

Fig. 1: Overall FIB-aware anti-probing physical design flow [8].

.

TABLE I: Frontside Shield Security in SAED32nm library

MAX R_{FIB}	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

TABLE II: Backside Shield Security in SAED32nm library

MAX RFIB	Shield Layer						
Target Layer	8	7	6	5	4	3	2
9	0.64	1.28	5.42	7.23	22.06	26.47	INF
8	N/A	0.64	3.61	5.42	17.65	22.06	INF
7	N/A		1.81	3.61	13.24	17.65	INF
6	N/A			1.81	8.82	13.24	INF
5	N/A				4.41	8.82	INF
4	N/A					4.41	INF
3	N/A						INF

A. Overview

As proposed in [8], by routing shield nets (identified from functional nets) in an upper layer on top of the target nets (i.e., those nets carrying asset signals) and creating a copy of the shield signals in the lower layers. Once a complete cut is detected on a shield net, a comparator will detect the mismatch between the signal on that shield net and its corresponding copy, and an alarm will be triggered to take appropriate actions, such as chip reset or destruction of all asset information. The overall workflow of the anti-probing physical design flow is shown in Fig. 1. First, appropriate shield nets and target nets are automatically identified to achieve optimal protection against probing attacks. Then, comparators are inserted to the gate-level netlist of the original design to detect the mismatch between upper shield and lower copy. Finally, floor-planning and routing constraints are added to the design to build the internal shield and provide protection against probing attacks. When it comes to the protection of both front-side and back-side, there are two sets of shield nets, with one being routed on a layer to prevent front-side probing attack and the other aiming for back-side probing attack, and assets nets will be routed on the layers between these two.

B. Target Net and Shield Net Identification

Following the same technique discussed in [8], target nets are identified using the target score metric, and the shield nets are identified using a mixed metric considering: target score, toggle frequency, switching probability, controllability, and delay slack.

C. Best Shield Layer

After the identification of shield nets, the routing layer of the shield nets need to be determined for the best protection. The shield security metric [8] which is defined by the maximum FIB aspect ratio that the shield can protect against is used to evaluate how much protection that a shield can provide to the assets. A higher value of the shield security means the better protection. Shield security is determined by layout technology dependent parameters, such as the width and thickness of wires. Table I and Table II show the shield security calculated from SAED32nm library from front-side and back-side respectively.

From Table II (shield security of layer 1 is not calculated because of the layer 1 is needed for standard cell and local routing), we can see that the backside shield is much better than the frontside shield especially for the shield on layer 2. No FIB can bypass the shield on layer 2, because the required shield to hole space is larger than the pitch space between the adjacent shield metals on layer 2. Besides, the pitch size and wire width decrease dramatically at the layers near the transistor level (e.g., layer 1 and 2), resulting in a higher shield security value. As we can see, layer 2 is the best back-side shield layer. Layer 6 is the best front-side shield layer because it has the best shield security for target nets on layer 3 and 4 and it has the advantage for not causing serious routing congestion issues compared to shield layer 4 (In order to take the advantage of this approach, target nets will have to be routed under shield layer. When it is the shield layer 4, target nets will be routed within layer 1 and 2 only and it increases the possibility of routing congestion issues)

D. Floor Planning Constraints

In conventional design flows, target nets and the blocks containing them are distributed randomly in the design, making it neither easy nor efficient to protect them with such placement. Therefore, it is more desirable to constrain them in a regularly shaped region, e.g., rectangle, as shown in Fig. 2. In addition, the comparator nets should be protected like target nets because the comparator results may be tampered by the probing attack. Therefore, the comparator gates are constrained in a shaped floorplan group adjacent to the target block. To implement front-side and back-side protection, shield gates are divided into four groups: lower shield nets driver and load groups, and upper shield nets driver and load groups. The driver and load groups are constrained to locations at opposite ends of the target gates and comparator gates. Thus, routing of shield nets crosses the target and comparator area and a vertical protection can be provided with shield nets routed above *and* below the target and comparator area.

E. Routing Constraints

Section III-C has revealed that routing shield wires on M6 and M2 with target wires and comparator wires in between can maximize the protection of shield against both front-side and back-side probing attack since a more advanced FIB with large aspect ratio is required to implement the attack without leaving a complete cut. However, in practice, we have initially observed that this brings routing congestion issues. Hence, we have implemented the upper shield on M8 instead with target nets and comparator nets on layers 3 to 7 as shown in Fig. 3. To avoid design rule violation, part of shield nets have to be routed under M2. In future, we will explore alternative area and keep-out region sizes to overcome congestion issues.

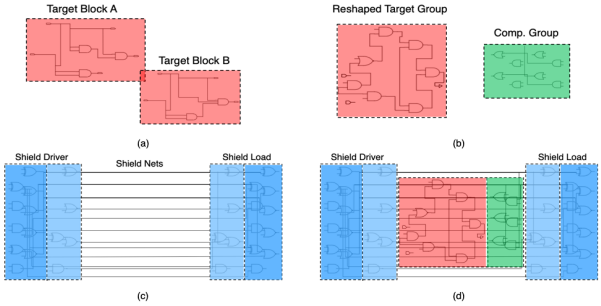

Fig. 2: Placement Constraints (a) Irregular location of target nets; (b) Reshape the target nets to fit one regular rectangle block (red) and comparator block (green); (c) Shield gates (blue) are divided into lower shield nets driver/load block (light blue) and upper shield nets driver/load block (dark blue); (d) Shield gates are placed surrounding the target and comparator blocks which will be covered by shield nets.

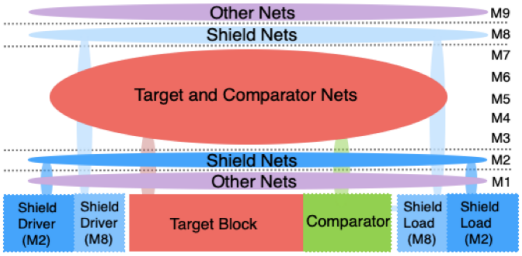

Fig. 3: Routing layer constraints for target and shield nets.

F. Exposed Area (EA) Calculation

Exposed area metric [9] is proposed to assess the design's vulnerability to probing attacks. The complementary part is the milling exclusion area (MEA). Fig. 4 shows how the exposed area (EA) can be found for any given target wire and covering wires on higher layers which are capable of protecting the milling exclusion area. White region represents the targeted wire and the green and purple regions are the covering wires at upper layers. The shaded region is the MEA, indicating that a complete cut will happen to the covering wires if the milling center falls in this area and larger EA represents a higher level of vulnerability to probing attacks.

1) Transistor-level Shield Extension

When considering back-side protection, we know that electrical probing attacks from back-side need to go through transistor level. For example, Fig. 5 shows the structure (schematic, top-view and section-view) of a NAND2 gate. Suppose there is an asset region in the middle and probing from the back-side will have to make contact to poly-Si of the cell, as shown in the cross-section view. In this scenario, attackers would try to avoid touching target and comparator cells, because with components of a cell, e.g., n-well, poly-Si, etc., getting in the way of probing from the back-side of

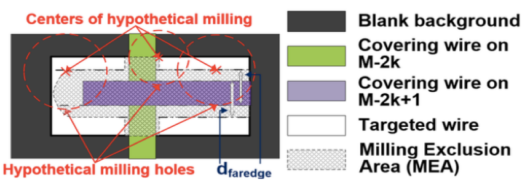

Fig. 4: Exposed area calculation [8].

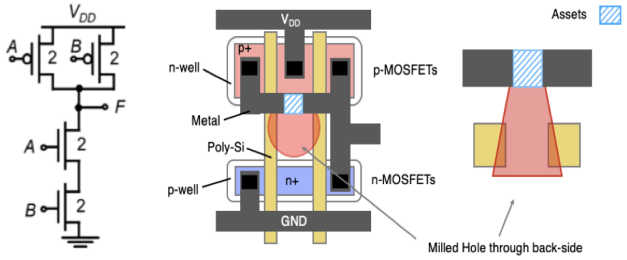

Fig. 5: NAND2 gate schematic, top view and cross-section view of the layout.

ICs, sabotaging them will affect the probing attack results. Therefore, target and comparator transistors will act as yet another set of back-side shields. Thus, we also take the contacts and poly-silicon of a cell into consideration of EA for back-side. (Other components of a cell and their shielding ability will be left for future work)

IV. EVALUATION

In this section, we evaluate our proposed FIB-aware anti-probing physical design flow on the layout of AES.

A. Implementation of Proposed Design Flow

The AES module used is from OpenCores [10]. It is described in register-transfer level (RTL) code and synthesized using Synopsys Design Compiler with Synopsys SAED 32nm technology library. The layout of AES is generated and constrained using Synopsys IC Compiler. The asset in the AES module is taken to be the encryption key.

Target gates and key memory cells are grouped and reshaped into a rectangular target block as shown in Fig. 6 and comparators are inserted into the design and also grouped and reshaped into a rectangular target block (green). As discussed in Section III-E, target nets and comparator nets are routed between M3 and M7. Besides, driver gates and load gates connected to the shield nets are reshaped into four groups and placed at the opposite ends of target and comparator block (light blue and dark blue represents shield nets routed at M8 and M2 layer, respectively). Fig. 7 shows the routing of target and shield nets, and their layer distribution are demonstrated in Fig. 8. Target nets, comparator nets, and shield nets are constrained in the reshaped region and routed between M3 to M7. Most shield nets are routed on M2 and M8 layers to provide optimal coverage. Note that, the reason why M2 shield nets are more dense is due to its smaller pitch size compared to that in M8 layer, resulting in a greater number of shield nets.

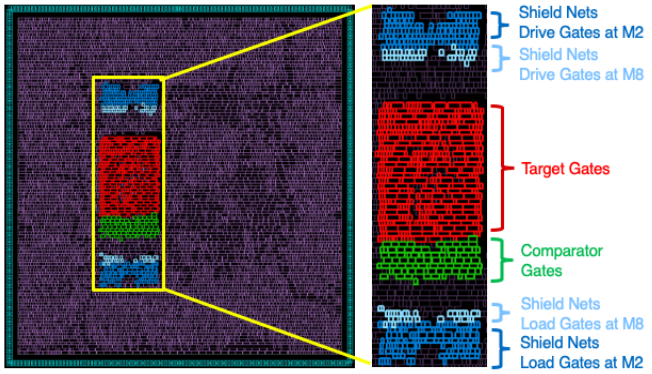

Fig. 6: Grouped/reshaped target, comparator, and shield gates in AES.

Table III shows the description of implemented designs and the exposed area calculation for AES design. Note that, the exposed area of Design 3.3 is added to prove the transistors' shielding ability. Table IV shows the timing, power, area and routing overhead of all these designs compared to the original AES design without any constraints. As we can see from the table, the overhead of these two designs is less than 2% in timing and area. The power overhead of Design No. 3 is larger than Design No. 2 in order to provide protection to the backside.

B. Exposed Area (EA)

The proposed internal shielding approach is evaluated by the exposed area metric as discussed in Section III-F. Fig. 9 shows the normalized exposed area for all types of designs in Table. III for AES. The exposed area is calculated across FIB aspect ratio from 1 to 10. The front-side exposed area of all internal shield designs (Design No. 2.1 and No. 3.1) can be reduced to 0 when the FIB aspect ratio is low. As the FIB aspect ratio increases, the exposed area for all designs also increases since the FIB hole diameter decreases with larger FIB aspect ratio [8], which results in smaller milling exclusion area and thus larger exposed area.

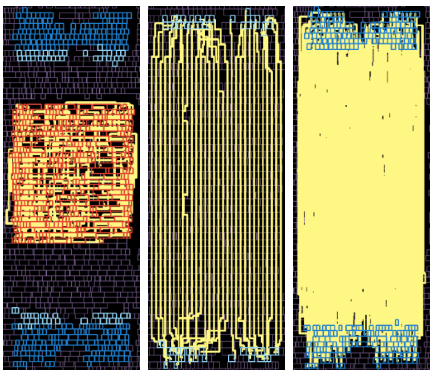

Fig. 7: AES shield gates (light blue at M8 and dark blue at M2), target gates (red), and highlighted nets (yellow).

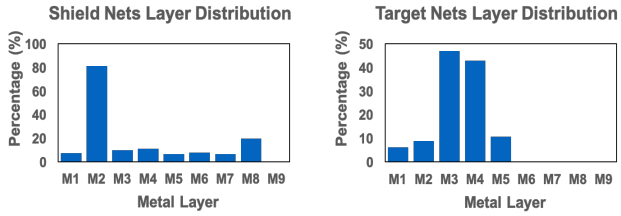

Fig. 8: Shield nets and target nets layer distribution.

Comparing Design 2.2 with 3.2, backside exposed area is reduced at least to 20% and transistor's shielding ability is also quite obvious with the decrease, minimum 4%, in exposed area with the comparison between Design 3.2 and 3.3. Besides, exposed area results of Design 2.1 and 3.1 reveal that larger frontside exposed area is brought about by Design 3.1, i.e., there is loss of front-side protection in the Design 3.1, compared to the Design 2.1, with only front-side protection. This occurs because single layer shields on M2 and on M6 cannot yet be performed due to routing congestion, but we plan to improve this in future work.

TABLE III: Description of implemented designs and exposed area calculation for AES.

No.	Description	No.	EA calculation
1	Original design without shield	1.1	Frontside
		1.2	Backside
2	Single layer shield on M6	2.1	Frontside
		2.2	Backside
3	Single layer shield on M8 and single layer shield on M2	3.1	Frontside
		3.2	Backside
		3.3	Backside (with poly-Si and contacts)

TABLE IV: Overhead of different AES designs.

Design	Total Gates	Target Nets	Target Gates	Timing	Power	Area	Routing
2	10547	256	384	0.36%	2.79%	0.74%	11.60%
3	10680	256	384	0.56%	7.18%	1.86%	23.69%

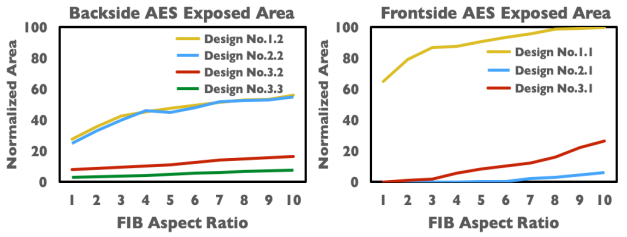

Fig. 9: Front-side and back-side exposed area results.

V. CONCLUSION

In this paper, we investigate the FIB-aware anti-probing physical design flow to explore the approaches to prevent ICs from microprobing attacks from both front-side and back-side. Evaluations on different implementations of AES modules demonstrate that the exposed area from both frontside and backside decreases by nearly 80% compared to the original design. In addition, the timing and area overhead is less than 2%. In future work, we hope to resolve the routing congestion issues to further reduce the exposed area.

REFERENCES

[1] 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," *Journal of Vacuum Science & Technology B: Microelectronics and Nanometer Structures Processing, Measurement, and Phenomena*, vol. 27, no. 4, pp. L18–L20, 2009.

[2] H. Wu, L. Stern, D. Xia, D. Ferranti, B. Thompson, K. Klein, C. Gonzalez, and P. Rack, "Focused helium ion beam deposited low resistivity cobalt metal lines with 10 nm resolution: implications for advanced circuit editing," *Journal of Materials Science: Materials in Electronics*, vol. 25, no. 2, pp. 587–595, 2014.

[3] https://www.onsemi.com/applications/aerospace-defense.

[4] S. Manich, M. S. Wamser, and G. Sigl, "Detection of probing attempts in secure ics," in *2012 IEEE International Symposium on Hardware-Oriented Security and Trust*. IEEE, 2012, pp. 134–139.

[5] M. Weiner, S. Manich, R. Rodríguez-Montañés, and G. Sigl, "The low area probing detector as a countermeasure against invasive attacks," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 26, no. 2, pp. 392–403, 2017.

[6] M. Weiner, W. Wieser, E. Lupon, G. Sigl, and S. Manich, "A calibratable detector for invasive attacks," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 27, no. 5, pp. 1067–1079, 2019.

[7] Y. Ishai, A. Sahai, and D. Wagner, "Private circuits: Securing hardware against probing attacks," in *Annual International Cryptology Conference*. Springer, 2003, pp. 463–481.

[8] H. Wang, Q. Shi, A. Nahiyan, D. Forte, and M. M. Tehranipoor, "A physical design flow against front-side probing attacks by internal shielding," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2019.

[9] Q. Shi, N. Asadizanjani, D. Forte, and M. M. Tehranipoor, "A layout-driven framework to assess vulnerability of ics to microprobing attacks," in *2016 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. IEEE, 2016, pp. 155–160.

[10] https://opencores.org/projects/aescore.