iPROBE-O: FIB-aware Place and Route for Probing Protection Using Orthogonal Shields

Minyan Gao, Domenic Forte

Department of Electrical and Computer Engineering, University of Florida
{minyan.gao}@ufl.edu, {dforte}@ece.ufl.edu

***Abstract*—Focused ion beam (FIB) probing attacks rely on advanced milling and deposition capabilities to significantly threaten the confidentiality of on-chip security assets such as private keys and device configuration. The existing countermeasures either suffer from the prohibitively high area overhead or low reliability, failing to serve as a perfect fit to address the issues. Recently, iPROBE framework has been proposed as a physical design flow enhancing the layout/device security against FIB attacks by adding additional shield nets at a minor cost. However, the parallel shielding methodology and metrics of iPROBE merely focus on the perpendicular FIB model instead of covering a more threatening one, *tilted* probing. In this paper, we present iPROBE-O to enable FIB-aware placement and routing using orthogonal shields to thwart both perpendicular and titled FIB intrusions. Besides, we extend the definition of *shield coverage* in the previous iPROBE work and propose the *tilted shield security* metric to comprehensively quantify the shield protection on every layer beneath the shield against *tilted* probing attacks. This metric allows users to choose the desired scheme such as shield layers and density accordingly for the optimal trade-off between overhead and security. Moreover, to alleviate the routing congestion risks from the orthogonal shields, we introduce *keepout region* between the shield drivers and target cells allowing more space and analytically assessing how the factors keepout region and a total number of gates jointly impact the overall protection strength. We demonstrate the effectiveness of iPROBE-O framework on a variety of benchmarks including AES, DES, and Simon by reducing up to 80% decrease on the exposed area can be achieved and the timing and area overhead is less than 3%.**

***Index Terms*—Hardware security, probing attack, focused ion beam (FIB).**

I. Introduction

Over the past decades, we have witnessed a surge of integrated circuits (ICs) for various applications in telecommunications, military infrastructure, industrial control, etc. However, the emerging physical attacks pose serious threats to the availability, confidentiality, and integrity of these electronic devices and their on-chip security assets. Considering the modality of these attacks, they can be non-invasive or invasive. Non-invasive attacks do not need specific sample preparations and leave negligible footprints on the target devices. For example, passive side-channel attacks are originally proposed to break cryptographic implementations by measuring the observable physical properties such as power [1], electromagnetic (EM) [2], and timing [3]. On the other hand, active fault injection attacks [4] can impact the original behaviors of the target without inducing permanent damage as well. An adversary can apply power, clock, and EM glitches to result in timing faults inside the circuitry to bypass the built-in security routine and/or escalate her privilege. In contrast, invasive attacks can be even more dangerous since the attackers have access to advanced equipment and broader knowledge of the ICs.

Among a variety of invasive attacks like reverse engineering [5], [6], focused ion beam (FIB), originally as a prevalent failure analysis tool, has raised a great physical security concern due to its powerful milling and deposition capabilities. One can launch so-called *micro-probing* attacks by electrically eavesdropping the valuable assets from the internal metal wires to the accessible chip surface in a fine-grained manner [7]. As reported in [8], [9], without proper protection, mid-end FIB equipment can exploit more than 90% of chip surface as its footholds. Obviously, micro-probing attacks significantly challenge the confidentiality of on-chip secrets, calling for effective countermeasures to be deployed.

In order to counteract the FIB probing attacks, quite a few approaches have been proposed but they, unfortunately, suffer from the following limitations and thus fail to become a perfect fit to thwart the threats.

- **High overhead.** Traditional active shields [10], [11] have been presented to detect the probing attacks at run-time by checking the possible FIB-induced mismatches between the reference pattern and the transmitted one on shield nets in the chip. However, the deployment of these shield metal wires incurs a large area overhead (one or two top-layer metal layers) and may cause routing congestion. Similarly, *t*-private circuit [12] can harden the design by rendering a successful probing attack much more difficult by increasing the number of required probes but inevitably stress the overhead budget as well.
- **Low reliability.** Sensors like the probe attempt detector (PAD) [13] can detect the variations of capacitance and timing delay from the attached FIB probes but be prone to process and environmental variations, leading to low reliability.
- **Insufficient vulnerability analysis.** Most of the existing works lack in-depth analysis and quantification of the FIB probing attack surface on the target physical design, making the subsequent countermeasures be *proactive* without achieving better protection.

Recently, [8] proposed an anti-probing physical design flow named iPROBE which can add *internal, parallel* shields in the original layout, manifesting good effectiveness against perpendicular probing attacks. However, the shortcomings stand out that this work fails to implement theoretically optimal *orthogonal* shields because of potential routing congestion concerns, thereby becoming less resistant when coming to more advanced *tilted* FIB intrusions [9]. To address the limitations mentioned above, we propose iPROBE-O, a computer-aided design (CAD) framework targeting the pre-silicon probing vulnerabilities assessment and automatic *orthogonal* shield nets deployment for enhancing the resistance against both perpendicular and tilted FIB attacks. We summarize our contributions below.

- We propose the *keepout region* metric and extend the conventional 1-layer protection to *orthogonal* 2-layer schemes for protection enhancement. In this way, the defined vulnerability metric *exposed area* can get further minimized without causing any routing congestion issues. *Exposed area* refers to the region on the target nets that FIB probing attack can have access to without sabotaging the normal function of the IC or being detected.
- We propose the *intersection width* metric to demonstrate the better shielding ability of the *orthogonal* 2-layer shield against tilted probing than *parallel* shield structure.

- We demonstrate the effectiveness and improvement of iPROBE framework with respect to the 1-layer versus 2-layer protection, orthogonal versus parallel protection, and different combinations of protection metal layers on an AES implementation.
- We implement the framework based on the state-of-the-art electronic design automation (EDA) tool, specifically, Synopsys ICC II in this paper. Also, we comprehensively evaluate the impacts on the performance of our framework from different EDA environments using the implemented *orthogonal* and *parallel* 2-layer structures.

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

II. Background

In this section, we will first discuss the existing micro-probing countermeasures and then state our threat model.

A. Focused Ion Beam (FIB)

Focused Ion Beam, or FIB, circuit edit allows an attacker to cut traces or add metal connections within a chip [14]. It employs a finely focused gallium (Ga+)/ platinum(pt)/ tungsten (W) ion beam to image, etch and deposit materials on an integrated circuit (IC). Most of the time, it is used in conjunction with micro-probing. With the circuit edit and microprobing, it is possible to read and/or change the stored secure values, thus compromising the confidentiality and integrity of ICs. A FIB's edit resolution is referred to as the FIB aspect ratio R_{FIB}, which is defined as the maximum ratio between the depth D and diameter d of the milling hole. A higher aspect ratio means that the FIB edit is thinner and more narrow; thus, it destroys less material when milling into the IC.

B. General Micro-probing Attack and Steps

FIB-based micro-probing has been investigated by researchers in the past decade. The fundamental preparations and steps of typical FIB attacks involve (i) decapsulating the chip package using acid chemical to expose the silicon die; (ii) reverse engineering the physical silicon die for recovering netlist to understand the design[1]; (iii) locating the exact coordinates of target wires carrying security assets, such as keys, proprietary firmware, etc.; (iv) using FIB to mill holes and deposit materials to access and create probing pads for the internal target wires, respectively. Given the fact that FIB technology can mill holes at a nanometer resolution, micro-probing attacks can be very stealthy and effective; (v) powering the IC so that sensitive signals are transmitted through the target wires where that can be probed by making contact with the deposited FIB materials.

C. Tilted Probing Attack Variant

The FIB milling cone will cut off a section of shield nets, as shown in Figure 2. Tilt angle, θ, and rotation angle, φ are two important parameters in the model during the microprobing attack. θ, refers to the tilt of the milling, defined as the angle between the FIB milling cone axis and its projection on the surface of the IC, and φ describes the rotation of the milling, defined as the angle between the projection of FIB milling cone axis on the surface of the IC and line in the perpendicular direction staring from the apex of the milling cone. Tilted probing differs from the top-down case by introducing these two angles. In this paper, we will mainly focus on two corner cases of rotation angle, φ, perpendicular scenario ($\varphi = \pi/2$), and parallel scenario ($\varphi = 0$).

D. Micro-probing Countermeasures

Active shield is the most prevalent countermeasure against probing attacks. With this solution, the target wires carrying the security assets will be protected by the shield nets at the top-most metal layer. The shield nets are "active" since they carry specific signals being monitored continuously to see whether milling cut any of them off [10]. For example, [10] adopts a Simon crypto core to generate random ciphertext to be transmitted in the metal shield layer, rendering the signals to be unpredictable to the adversary for spoofing. However, the protection is based on the assumption that the milling procedure would cut open one or more shield nets which might not hold for advanced FIB technology at a high resolution, e.g., a state-of-the-art FIB probe ($\tilde{1}0$ aspect ratio) can effectively bypass sparse active shield nets avoiding destroying them [8]. Moreover, active shields incur a high area overhead and consequent routing congestion issues, even up to more than 100% area overhead, e.g., [10]. *t-private technique* [12] leverages the limited number of probing channels an adversary has, to transform the original design in a way that a bit of information is split into *t*+1 shares, requiring the identical amount of probes working simultaneously for decoding the data. Such solutions, albeit effective, still suffer from the prohibitively high area overhead which can be up to multiple times. However, an advantage of masking is that it helps to prevent non-invasive side-channel attacks.

As for *analog sensors*, PAD [13] is a good representative of measuring the additional capacitance and delay induced by the attached FIB probing to avoid the high overhead. This is often accomplished by comparing the interconnects being probed with a reference interconnect which is not being probed. Nevertheless, the introduced parasitic parameters from FIB probes are typically small and might get masked by the process variations, especially at a small technology node [7]. Analog sensors are, however, well-suited for protecting long interconnects like data buses.

As mentioned, despite that existing solutions exhibit somewhat good effectiveness with respect to probing detection and deterrence, they are either expensive to implement or less reliable. A root cause comes down to the insufficient awareness of FIB vulnerabilities in the physical design flow, i.e., *how susceptible a given physical layout is to the FIB attack*, and thus did not get efficient protection. Although iPROBE framework in [8] can assess the vulnerabilities and add *parallel* shield nets for layout protection, it cannot provide the optimal *orthogonal* scheme, rendering it a less effective solution against tilted probing attacks. In this paper, our iPROBE-O framework will quantify the vulnerabilities and use this information to guide the orthogonal shield nets placement for an optimized floorplan, meeting both security and performance criteria.

E. Threat Model

We assume a strong threat model here; the adversary can be someone with physical access to the target electronic device. She also has a good grasp of probing technology and owns/rents a FIB machine for probing attacks. Besides, she has knowledge of sample preparations (e.g., decapsulation and hardware reverse engineering) for netlist recovery and the coordinates of target wires. The attacker may possess and destroy one than more sacrificial chips in order to recover the design layout, understand the depth of each layer, its

[1] This step can be skipped if the attacker, e.g., untrusted foundry, already has the design and its associated layout. The attacker may also have knowledge of the hard IP in the design by purchasing it from a 3rd party vendor.

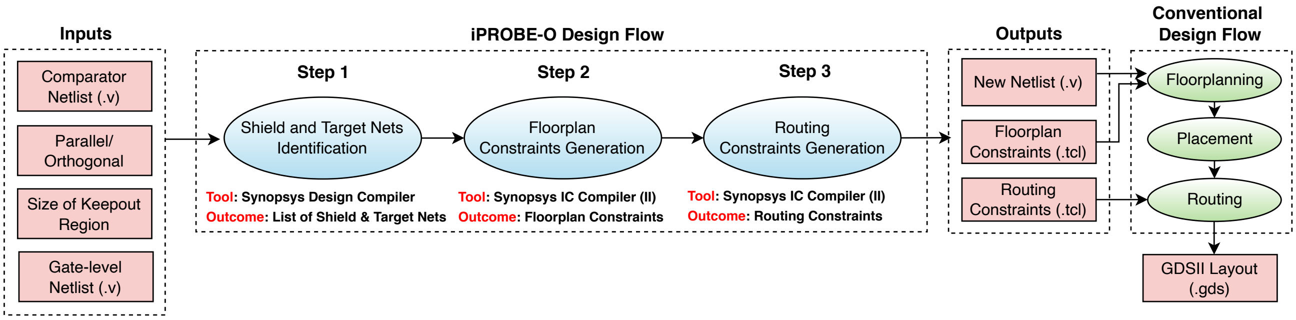

Inputs
Comparator Netlist (.v)
Parallel/ Orthogonal
Size of Keepout Region
Gate-level Netlist (.v)
iPROBE-O Design Flow
Step 1
Shield and Target Nets Identification
Tool: Synopsys Design Compiler
Outcome: List of Shield & Target Nets
Step 2
Floorplan Constraints Generation
Tool: Synopsys IC Compiler (II)
Outcome: Floorplan Constraints
Step 3
Routing Constraints Generation
Tool: Synopsys IC Compiler (II)
Outcome: Routing Constraints
Outputs
New Netlist (.v)
Floorplan Constraints (.tcl)
Routing Constraints (.tcl)
Conventional Design Flow
Floorplanning
Placement
Routing
GDSII Layout (.gds)

Fig. 1: iPROBE-O: FIB-aware anti-probing physical design flow to place and route orthogonal shields.

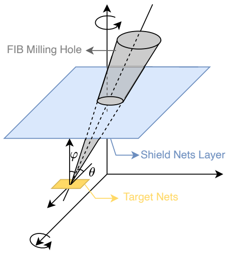


Fig. 2: Model of FIB-based milling in microprobing attacks.

.

TABLE I: Definition of notations

Notation	Definition
θ	Angle of the rotation of the milling
φ	Angle of the tilt of the milling. $\varphi = \frac{1}{2}\pi$, and 0 for a parallel and perpendicular tilted milling, respectively
α	Half of opening angle of the milling hole
D	Depth of the FIB milling.
T	Thickness of the shield wire

underlying materials, etc. By using FIB probing attacks, adversaries intend to compromise the confidentiality of on-chip security assets including but not limited to private cryptographic keys, self-generated random numbers, device firmware, and configuration [15].

The trusted engineers in the design house will utilize our iPROBE-O framework to assess and quantify the probing vulnerabilities of the original physical design to efficiently deploy orthogonal shields before tape-out, allowing flexibility for design-time countermeasures.

III. iPROBE Framework

In this section, we will present the overview of our iPROBE-O framework first and then elaborate on each main step in detail.

A. Overview

Figure 1 illustrates the overview of our iPROBE-O, which is an enhanced physical design flow with FIB-aware anti-probing capabilities. A conventional design flow involves only floorplanning, placement, and routing stages with a focus on meeting traditional metrics such as power, performance, and area. With iPROBE-O, one can empower the original design with shield nets-based security enhancement against micro-probing attacks. More specifically, iPROBE-O can first identify the shield and target nets in the gate-level netlist according to signal propagation and structural analysis. Besides, a larger keepout region in the design layout would reduce exposed area further but bring about relatively higher design overhead. The flexibility provided on the size of keepout region in the iPROBE-O structure gives users the freedom to choose whether to minimize exposed area or design overhead. A comparator design will be inserted into the netlist later for checking the potential FIB-induced mismatches on the shield nets continuously. Next, we will generate a set of floorplan constraints to shape the physical cells into the desired pattern for comprehensive coverage of security assets. Finally, routing constraints are produced as well to place the shield nets at appropriate layers. As such, the milling cavity of FIB probing will partially or even fully cut off the shield nets in the protected layout at a great chance, which can be detected by the embedded comparator during run-time to raise the alert for subsequent termination of operations or erasure of on-chip secrets.

B. Target and Shield Nets Identification

In this step, we need to identify two categories of critical nets in the gate-level netlist, i.e., target and shield nets. Target nets refer to the items of interest to the adversary while shield nets are the proper candidates to be extended for protection purposes. Apart from the input gate-level netlist, users need to specify several inputs to make the iPROBE framework aware of hyperparameters such as the asset signals (e.g., an internal net or input port) and the threshold level for target nets identification.

Different from dedicated shield nets in conventional active shield schemes, our shield nets are from the original netlist and will be placed in the internal metal layers instead of the top-most layer to harden the design against probing and reroute attacks [7]. Additionally, utilizing the original functional nets can eliminate the need for a cryptographic pattern generator [10] to avoid high area overhead. Nevertheless, iPROBE-O could easily incorporate cryptographic patterns for its shield nets to provide greater security. A shield net is anticipated to satisfy five criteria, i.e., (i) low target score implying it does not carry sensitive information, (ii) high toggle frequency such that the adversary cannot replace them with constant values, (iii) balanced switching probability between 0 and 1, (iv) low controllability that the attackers cannot manipulate arbitrarily, and (v) small performance degradation causing negligible impacts on the critical path delay. Thresholds of each metric can be specified by users to get a set of shield nets which will have two branches in the physical design, i.e., one branch locates at a higher level for protection purposes while a copy of the net goes through the lower layer. Both branches will be fed into the embedded hardware comparator, which is integrated into the original netlist as well, for run-time mismatch detection. If a mismatch is detected, it is assumed that the chip will

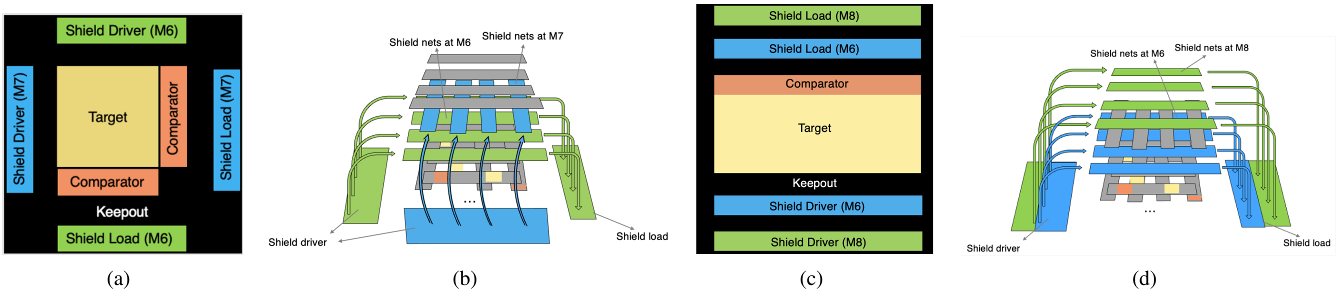


Fig. 3: iPROBE-O floorplan and routing constraints – (a) Orthogonal two layer protection cells floorplan; (b) Orthogonal two layer protection 3D diagram; (c) Parallel two layer protection cells floorplan; (d) Parallel two layer protection 3D diagram.

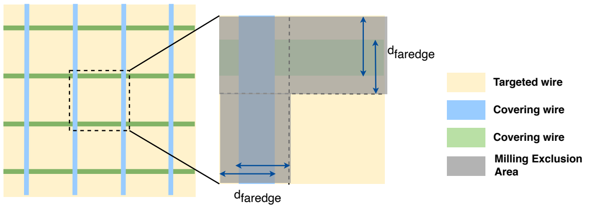


Fig. 4: Example calculations for the tilted shield security metric.

.

respond by zeroization of sensitive data, self-destruction, reset, etc.[2]

C. Floorplan Constraints Generation

Floorplan constraints are critical to integrating FIB awareness into the conventional physical design flow where only power, performance, and area are the main concerns. From the perspective of FIB adversaries, such floorplans might manifest plenty of exploitable intrusion space since the upper-layer nets might not protect the asset targets very well because of their sparse and random distribution. Therefore, in our iPROBE-O framework, we constrain the security-sensitive cells such as the driver components of target nets in a concentrated manner (see Figure 3(a) and 3(c)) so that the shield nets can achieve the maximum coverage and protection effectiveness.

Compared to the perpendicular probing model which has been thoroughly discussed in [7], [8], [16], it is likely to use tilted probing to evade the perpendicular-orientation shield protection by finding an appropriate probe tapping the sensitive metal wire. In order to assess the security vulnerabilities under the tilted probing and identify the optimal shield layer combinations of the theoretically minimum exposed area, we propose a new metric termed as *tilted shield security (TSS)* which is defined as follows (See also in Figure 4).

$$TSS = \frac{d_{faredge} * (P_{sa} * P_{sb} - d_{faredge})}{P_{sa} * P_{sb}} * 100\% \qquad (1)$$

where P_{sa} and P_{sb} are the respective pitch size in the parallel and orthogonal orientations, as well as $d_{faredge} = 2 * D_{s2t}[tan\varphi - tan(\varphi - \alpha)]$. Note that D_{s2t}, φ, α refer to the distance between the target net and the associated shield net, angle of the tilted milling, and half of the opening angle of the milling hole, respectively. For clarity and convenience, we denote notations that are used throughout this paper in Table I. α is inversely proportional to the FIB aspect ratio parameter, i.e., a small α indicates a powerful probe. Besides, we did not cover the angle of the milling rotation θ in the TSS definition because $d_{faredge}$ targets the maximum range the semi-major axis of the ellipse (the intersection of the titled milling cone) can reach, where θ can only determine its spatial location instead of the value. The TSS metric is technology-dependent since different libraries would impact the parameters such as the pitch size of the shield layer and target layer, as well as the width of shield wire. For example, Figure 6(a) shows the TSS results calculated from SAED32nm library where we can see that shield layer M6+M8 has the best TSS.

As depicted in Figure 3, we propose a two-layer shield schemes in *orthogonal* form. Thanks to more shield nets, a better protection is expected than the one-layer shield solution as presented in [8]. In both *orthogonal* and *parallel* cases, the target cells/nets reside in the center of the layout along with the comparator since attackers might tamper with it to affect the detection results stealthily.

D. Routing Constraints Generation

In addition to floorplan constraints, routing constraints are crucial for the effectiveness of iPROBE-O framework as well. The orthogonal and parallel schemes in Figure 3 partially[3] utilize two top metal layers for routing shield nets. To be specific, we put the shield nets in the M6 and M7 layers for the orthogonal scenario (see Figure 3(a) and 3(b)) and parallel shield nets in the M6 and M8 layers (See Figure 3(c) and Figure 3(d)). The target nets and the reference copy of shield nets (the latter are used to detect changes to the shield nets in upper metal layers caused by FIB edit) are routed in the lower layers under the protection of the shield ones.

A possible downside of our two-layer protection scheme is routing congestion because of the concentrated shield nets and relatively smaller pitch size in M6 and M7. To address the issues, we introduce the *keepout region* (the black regions in both Figure 3(a) and 3(c)) in the floorplan constraints, separating the shield drivers/loads from the target cells/comparators at a distance. Using this new parameter, the stress of routing congestion can be significantly alleviated without loss of resilience against probing attacks.

IV. Experimental Results

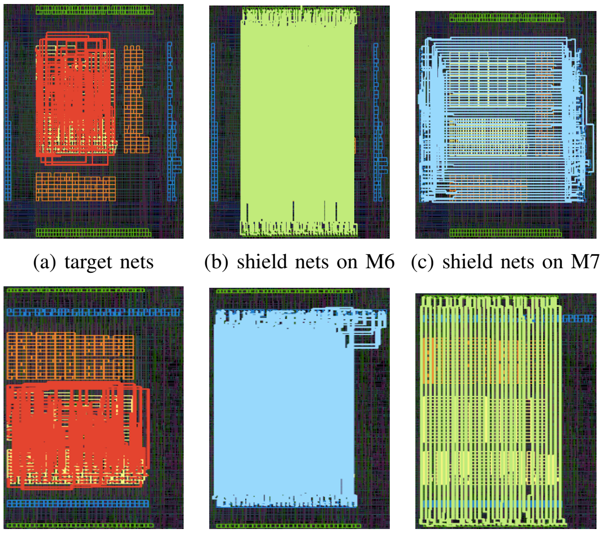
In this section, we will evaluate the orthogonal and parallel iPROBE structure in terms of exposed area and design overhead, and their shielding ability will be further assessed with TSS metric.

[2] Note that we consider the response itself to be outside the scope of this paper.

[3] By partially, we mean that we do not use an entire layer for shields. Rather, the shields are only placed directly above the target nets which are routed within a regular shape in the layout.

TABLE II: Design types used for comparison.

No.	Shield Type	Description
1	Original Design (No Shield)	Conventional physical design
2	Two-layer Parallel Shield	Shield on M6 and M8
3	Two-layer Orthogonal Shield	Shield on M7 and M8
4	Two-layer Orthogonal Shield	Shield on M6 and M7
5	Two-layer Parallel Shield	Shield on M5 and M7
6	Two-layer Orthogonal Shield	Shield on M5 and M6


(a) target nets (b) shield nets on M6 (c) shield nets on M7

(d) target nets (e) shield nets on M6 (f) shield nets on M8

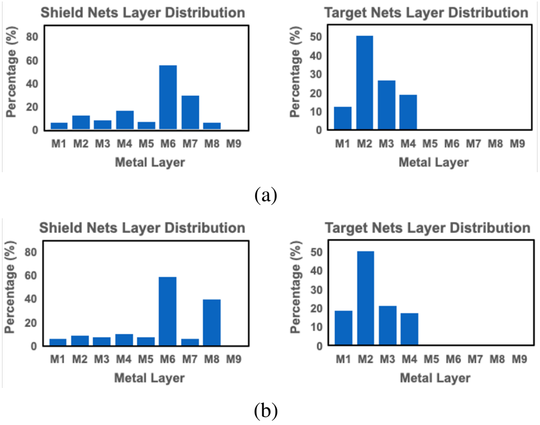
Fig. 5: (a)-(c) AES orthogonal shield structure on M6 and M7 layers. (d)-(f): AES parallel shield structure on M6 and M8 layers.

A. Experimental Setup

Four benchmark cryptographic implementations are selected for our experiments, i.e., AES, DES, Simon, and Present [17]–[19]. These designs are described in register-transfer level (RTL) using Synopsys Design Compiler [20]. Physical design and iPROBE/iPROBE-O are implemented in ICC II [21]. The technology cells used are from the SAED 32nm library [22]. AES design is taken as an example while the other three benchmarks follow a similar pattern. Table II shows all the shield structures that are tested using iPROBE and iPROBE-O.

As one can observe from Figure 5, cells are separated into different placement groups, i.e., target gates, comparator gates, orthogonal/parallel shield nets driver gates, and orthogonal/parallel shield nets load gates. In detail, target gates, which serve as the drivers of target nets carrying sensitive data, are grouped together and reshaped into the yellow rectangular region. The shield nets placed at M6+M8 or M6+M7 metal layers will provide shields against the potential frontside intrusions while their drivers (green and blue cells) are placed at the peripheral. In addition, we will insert a set of comparators into the post-synthesis netlist to serve as the monitor and will alarm when the signal comparison results are not the same. The corresponding units (in orange) locate in between the target gates and shield gates.

The distributions of shield and target nets across all 8 layers are demonstrated in Figure 6 shows and they are consistent with our intention, i.e., the target nets are concentrated on from M1 to M4 layers (more than 90%) while shield nets mainly reside in M6 and M8 or M6 and M7 for orthogonal and parallel structure, respectively, in order to prevent the external probes from reaching the internal assets nets.



(a)

(b)

Fig. 6: Shield and target nets layer distribution for (a) orthogonal structure using metal M6 and M7 layers, and (b) parallel structure using metal M6 and M8 layers.

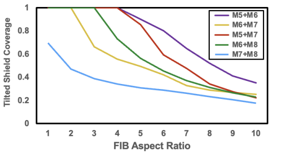
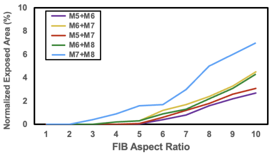
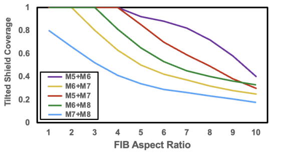
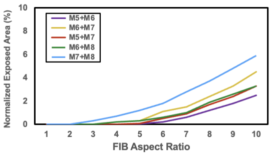
Scenario	Tilted Shield Security	Exposed Area
Worst		
Best		

TABLE III: Tilted shield security and exposed area in different scenarios in AES design.

B. Security and Overhead Analysis

We illustrate the probing security analysis of the AES layouts with the iPROBE-O protection in terms of TSS and EA in Table. III. A larger TSS indicates better protection while a small exposed area implies less exploitable space reserved for adversaries. We investigate the security metrics with respect to the probing capabilities in terms of FIB aspect ratio ranging from 1 to 10 while considering the worst and best scenarios in terms of security resilience against FIB of attack as illustrated in Table III.

From Table III, we can observe that as discussed before, larger TSS and smaller EA indicate stronger shielding ability, i.e, the TSS results (left column in table III) and EA results are consistent to indicate that the smallest FIB aspect ratio can enable the most powerful attack capabilities. Moreover, regardless of the scenarios, M5+M6 and M7+M8 can provide the strongest and weakest protection, respectively, according to our analysis results. Note that since the state-of-the-art FIBs have large aspect ratios, the orthogonal shield (M5+M6) is the best for protecting modern chips from probing attacks.

Effect of keepout region and number of shield gates on the exposed area on the target nets is also demonstrated in Figure 7, from which, we can observe that exposed area would get reduced with increasing the size of keepout region and the number of shield gates. This agrees

TABLE IV: Overhead of different AES designs

Design	Total Gates	Timing	Power	Area	Routing
No.2	22253	2.29%	4.55%	1.23%	21.62%
No.3	21569	2.06%	9.03%	1.31%	24.66%
No.4	19339	2.00%	9.93%	1.59%	25.16%
No.5	19735	2.12%	13.21%	1.69%	26.99%
No.6	20210	2.55%	14.17%	2.13%	27.20%

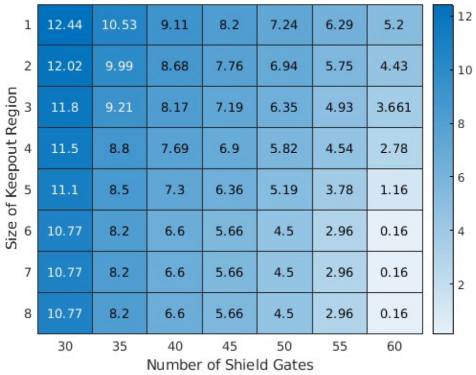


Fig. 7: Effect of keepout region and number of shield gates on the exposed area.

with our intuition: The larger the keepout region, the lower the routing congestion and easier to add shields; and the more shield nets, the better the target area is covered by the shield and therefore the lower the exposed area. Also, we tabulated the detailed results of overhead of shield nets on four cryptographic implementations including AES, DES, Simon, and Present, in Table V. Although the results show that the orthogonal shield schemes proposed in this paper is slightly larger than the previous parallel scheme (roughly 5%), the orthogonal one can provide a much more thorough protection effectiveness as demonstrated in aforementioned statistics.

V. Conclusion

In this paper, we presented and demonstrated the orthogonal 2-layer iPROBE-O structure, which follows the anti-probing physical design flow to protect ICs against frontside probing attacks and reduces the exposed area further compared to previous work. Evaluations on different implementations of four designs demonstrate that compared to the original design, nearly 80% decrease on the exposed area can be achieved and the timing and area overhead is less than 3%. In addition, the exposed area results are demonstrated to be consistent with tilted shield security.

References

[1] T. Zhang, J. Park, M. Tehranipoor, and F. Farahmandi, "Psc-tg: Rtl power side-channel leakage assessment with test pattern generation," in *2021 58th ACM/IEEE Design Automation Conference (DAC)*. IEEE, 2021, pp. 709–714.

[2] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi, "The em side—channel (s)," in *International workshop on cryptographic hardware and embedded systems*. Springer, 2002, pp. 29–45.

[3] R. Hund, C. Willems, and T. Holz, "Practical timing side channel attacks against kernel space aslr," in *2013 IEEE Symposium on Security and Privacy*. IEEE, 2013, pp. 191–205.

[4] H. Wang, H. Li, F. Rahman, M. M. Tehranipoor, and F. Farahmandi, "Sofi: Security property-driven vulnerability assessments of ics against fault-injection attacks," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2021.

TABLE V: Design overhead in parallel vs. orthogonal shield structures.

Design	Target Nets	Target Gates	Total Gates	iPROBE structure	Timing	Power	Area	Routing
AES	256	384	19339	M6+M8	2.00%	9.93%	1.12%	25.16%
			19735	M6+M7	2.12%	13.21%	1.69%	26.99%
DES	496	880	14082	M6+M8	1.66%	12.99%	0.74%	25.23%
			14799	M6+M7	1.69%	13.92%	1.22%	27.89%
Simon	112	496	8775	M6+M8	1.27%	11.99%	0.4%	20.41%
			9665	M6+M7	1.35%	11.67%	0.49%	21.70%
Present	80	160	6910	M6+M8	1.19%	11.50%	0.29%	19.22%
			7790	M6+M7	1.21%	11.67%	0.33%	20.50%

[5] A. Baumgarten, A. Tyagi, and J. Zambreno, "Preventing ic piracy using reconfigurable logic barriers," *IEEE design & Test of computers*, vol. 27, no. 1, pp. 66–75, 2010.

[6] T. Zhang, J. Wang, S. Guo, and Z. Chen, "A comprehensive fpga reverse engineering tool-chain: From bitstream to rtl code," *IEEE Access*, vol. 7, pp. 38 379–38 389, 2019.

[7] H. Wang, D. Forte, M. M. Tehranipoor, and Q. Shi, "Probing attacks on integrated circuits: Challenges and research opportunities," *IEEE Design & Test*, vol. 34, no. 5, pp. 63–71, 2017.

[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, H. Wang, N. Asadizanjani, M. M. Tehranipoor, and D. Forte, "A comprehensive analysis on vulnerability of active shields to tilted microprobing attacks," in *2018 Asian Hardware Oriented Security and Trust Symposium (AsianHOST)*, 2018, pp. 98–103.

[10] J.-M. Cioranesco, J.-L. Danger, T. Graba, S. Guilley, Y. Mathieu, D. Naccache, and X. T. Ngo, "Cryptographically secure shields," in *2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*. IEEE, 2014, pp. 25–31.

[11] 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 *2012 Eighth International Conference on Computational Intelligence and Security*. IEEE, 2012, pp. 530–533.

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

[13] 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.

[14] C. Helfmeier, D. Nedospasov, C. Tarnovsky, J. S. Krissler, C. Boit, and J.-P. Seifert, "Breaking and entering through the silicon," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, 2013, pp. 733–744.

[15] S. Bhunia and M. Tehranipoor, *Hardware security: a hands-on learning approach*. Morgan Kaufmann, 2018.

[16] 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.

[17] "AES core," [Online], https://opencores.org/projects/aes-128_pipelined_encryption, Accessed Nov. 19, 2022.

[18] "Simon Block Cipher Implementation," [Online], https://github.com/inmcm/Simon_Speck_Ciphers, Accessed Nov. 19, 2022.

[19] "Present Hardware Core," [Online], https://github.com/saiedhk/PresentCryptoEngine, Accessed Nov. 19, 2022.

[20] P. Kurup and T. Abbasi, *Logic synthesis using Synopsys®*. Springer Science & Business Media, 2012.

[21] I. Synopsys, "Compiler user guide," 2013.

[22] V. Naganathan, "A comparative analysis of parallel prefix adders in 32nm and 45nm static cmos technology," Ph.D. dissertation, 2015.