A Comprehensive Analysis on Vulnerability of Active Shields to Tilted Microprobing Attacks

Qihang Shi, Huanyu Wang, Navid Asadizanjani, Mark M. Tehranipoor, Domenic Forte
ECE Department, University of Florida, {qihang.shi, huanyuwang}@ufl.edu, {nasadi, tehranipoor, dforte}@ece.ufl.edu

***Abstract*—Microprobing attacks against integrated circuits used in security-critical systems have become a serious concern. With the help of advanced circuit editing technology, an attacker can remove layers of materials and expose wires carrying security critical information for probing. Active shields constitute the most widely used approach to deter microprobing attacks. However, a number of vulnerabilities have been found in existing active shield designs; in particular, their weakness to tilted bypass attacks has yet to be addressed. In this paper, we provide a comprehensive investigation on tilted bypass attacks with a mathematical model to investigate how best an attacker can exploit geometric weakness of shield designs in three dimensions, as well as shield design techniques informed with such observations. We also include a numerical analysis with realistic parameters to validate theoretical predictions.**

I. Introduction

Physical attacks are a growing concern for design of integrated circuits (ICs) used in security-critical applications. Physical attacks circumvent encryption by attacking their silicon implementations. Microprobing is one kind of invasive physical attack that directly probes signal wires in order to extract sensitive information [1]. Successful microprobing attacks have been reported on smartcards and microcontrollers in mobile devices [2], [3]. Plaintexts such as personal data, code format intellectual property (IP) or even encryption keys have been compromised [4].

Most security critical ICs are reinforced against microprobing attacks with active shield to detect a breach when a shield wire is cut, and zeroize sensitive information once detected. Several reports of attacks defeat active shields [3], [5]. Among discovered exploits, *bypass attack* exposes targeted physical wire with cutting-edge circuit editing tools so that active shields remain intact, constituting a most expedient, most preferred, and most difficult to protect against approach [3]. Further, it has recently been shown that milling at a tilted angle decreases the attack footprint thus making bypassing the shield even easier to execute [6]. To the best of the authors' knowledge, no active shield design has been proposed to counter this new threat to date, nor has any design claimed to be more resilient against normal bypass attacks.

In this paper, we make the following contributions:

- A mathematical model to analyze probing by shield bypass with focused ion beam (FIB) tilt and rotation.
- Conclusions drawn from the mathematical model to bolster the effectiveness of active shields.
- Demonstration of provided principles with numerical results.

The rest of this paper is organized as follows. Section II reviews related topics and prior contributions. Section III presents a mathematical model to calculate exposure of any wire to microprobing attack, considering all tilt and rotation angles. Section IV presents shield design principles to counter tilted bypass attacks and generic bypass attacks. In Section V, we present numeric simulation to validate theoretical modeling and proposed shield designs, evaluating their performance, and discuss implications of the results, before concluding the paper in Section VI.

II. Background

A. Technology Enabling Circuit Microprobing

Circuit microprobing refers to techniques that allow an attacker to directly observe partial or full sensitive information, collectively known as *assets* [7]. An *asset* can be any resource or values that could pique the interest of an attacker, e.g., plaintexts, encryption keys, firmware, configuration, or random numbers. Microprobing attacks are categorized as invasive attacks because they require depackaging to expose transistors and signal routing. Wires of asset-bearing nets and buses are likely buried under multiple passification, metal, and dielectric layers. On ICs fabricated with feature dimensions larger than 0.35μm, laser cutters can be used to remove these layers [1]. For technologies of lower dimensions, the most common tool is the focused ion beam (FIB) [8]. With the help of FIB, an attacker can mill at sub-micron or even nanometer level precision [9]. A measure of FIB capability, the *aspect ratio* is defined as the ratio between milled hole depth and diameter [10]. FIB instruments with higher aspect ratio can be expected to mill a hole of smaller diameter, thus leaving smaller impact on the IC.

B. Countermeasures against Microprobing Attacks

To protect against microprobing attacks, two categories of techniques exist: 1) detection-response based approaches, and 2) prevention based approaches.

Most existing techniques are designed to zeroize assets upon detection of probing attempts. This can be achieved either by detecting the actual activity of microprobing or activities essential for microprobing to work. The more widely studied

This research is supported by NSF (1717392) and SRC (TS-2769).
978-1-5386-7471-0/18/$31.00 ©2018 IEEE

and implemented approach is to detect hardware tampering by building a mesh of trigger wires to cover the design [11]–[15]. This is called an *active shield*, because the trigger wires are supposed to be constantly monitored in order to detect an attack, at least during boot process. A *digital* active shield sends digital random vectors through the trigger wires, and check whether received vectors are altered. A milling through the mesh would be reliably detected when it cuts off at least one of the trigger wires. An alternative [16] is to detect act of probing by monitoring change of capacitance, but this approach is susceptible to noise and false positives, has high overhead and can only protect a small subset of nets.

In addition to hardware based approaches, one cryptographical method called t-private circuits [17] modifies the security-critical circuit so that at least $t + 1$ probes are required by an attacker to extract one bit of information. Unfortunately, the overhead is proportional to quadratic to t, and it has been shown that such an approach might be jeopardized during CAD optimization process [18].

C. Microprobing Attack Techniques

The most common method to protect an IC from milling is the active shield, which places signal-carrying wires on top metal layers [11]–[15]. The expectation is that the milling will cut off at least one of these wires which can be detected by the shield. There are a few ways to invalidate or ineffectualize this mechanism, depending on construction of the shield[1]; Yet most of these techniques require some level of reverse engineering of the design, which takes time. On the other hand, as soon as FIB milling manages to reach the target wire without cutting off any shield wire, the shield is *bypassed* without requiring any amount of work by the attacker. Aside from shield layout and dimensions, an important FIB parameter influencing bypass success is *aspect ratio* (hitherto denoted as R_{FIB}). A higher R_{FIB} makes bypassing active shield easier. When milling is performed on modern nanoscale ICs, state-of-the-art FIB systems can reach an aspect ratio up to 8.3 [19]. Further, it has been shown that FIB milling can further reduce diameter of completely cut-off area by milling at an angle, so as to avoid unintentional cut-off of intervening wires unavoidable if milled perpendicular to the substrate [6]. It is also possible to circumvent the active shield through *back-side* photon emission techniques; however, photon emission-based techniques require repeated emission of photons, and may not be reliable to extract transient signals [20], making them more limited than bypass attacks. In summary, in this paper we focus on bypass attacks.

III. Mathematical Model of Exposure to Probing with Tilt and Rotation

We model FIB-based milling as shown in Figure 1, where colored bars represent metal wires on different routing layers, and the target wires attacker wants to reach may be buried beneath other wires in layers above them. Two gray cones shown in the figure represent cavities milled with FIB equipment, one milled top-down and one milled with tilt θ and rotation φ with regard to z- and x-axes, respectively. The milled cavity can then be deposited with conductor to facilitate electric connection between probes and target wires. If a shield wire is partially cut, dielectric can be deposited before conductor as insulation; such considerations can be easily included as a constant margin on top of the simplified conic model shown in the figure and used in the following analysis.

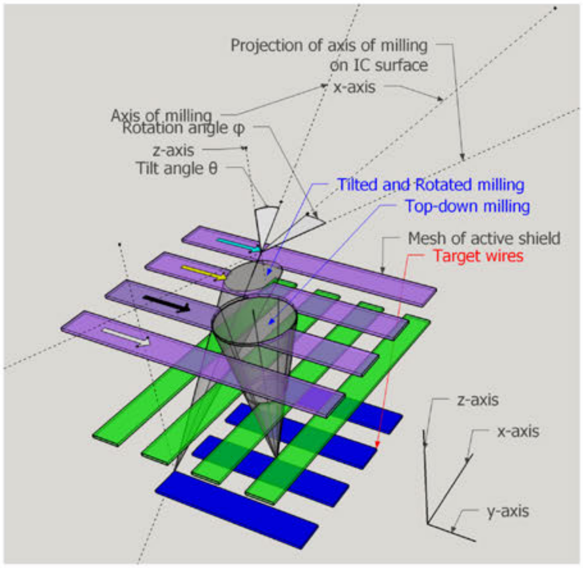


Fig. 1: Conic model of FIB-based milling in microprobing attacks.

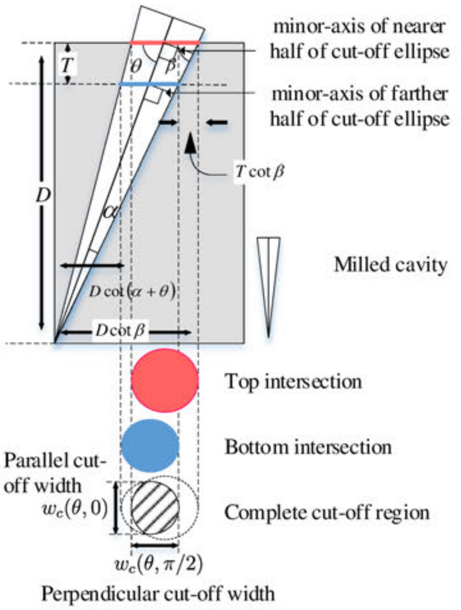


Fig. 2: Cut-off width when milling is tilted, in relation to direction of shield wires.

[1] e.g., recreating active shield signals, rerouting a copy of the same signal from the shield itself, etc [6].

TABLE I: Explanations on terminologies.

Term	Explanation
α	Half of opening angle of the milled cavity (modeled as a cone). $\tan\alpha := (2R_{\text{FIB}})^{-1}$
θ	Tilt of the milling, defined as angle between cone axis and its projection upon the surface of the IC.
φ	Rotation of the milling, defined as angle between projection of cone axis upon the surface of the IC and perpendicular line from the apex of the milled cone to the shield wire. A *parallel* tilted milling is one where $\varphi = \frac{1}{2}\pi$. A *perpendicular* tilted milling is one where $\varphi = 0$.
D	Depth of the milling, defined as sum of thickness of all layers between the top surface of the shield wire and the apex of the milled cone.
d	Diameter of the base of the milled cone.
R_{FIB}	Aspect ratio of FIB that milled the cone; $R_{\text{FIB}} := d/D$.
T	Thickness of the shield wire.
T_i	Thickness of i-th routing layer.
$w_c(\theta,\varphi)$	Cut-off width, defined as minimum width of wire on the shield layer parallel to the shield wires that can be completely cut open by the milled cone.
$T_{D,i}$	Thickness of dielectric layer between routing layer i and $i-1$.
w_i	Minimum width of i-th routing layer.
p_i	Routing pitch of i-th routing layer.

A. Tilted FIB Milling

The milled cavity will cut-off a section of material in shield layer, as shown in Figure 2. The question of whether milling will be detected depends on whether this section cuts off any shield wire, which depends on relative placement of shield wires, target wires, and apex of milled cavity, as well as width of the cut-off region viewed in the direction of shield wires (denoted as cut-off width $w_c(\theta,\varphi)$ in Figure 2). To simplify the problem for a generic conclusion, this study is focused on evaluating cut-off width and ignores the impact of relative placement issues. Terminology used in this investigation is provided in Table I.

Cut-off width in the case of top-down milling simply equals to diameter of intersection between cavity and bottom of the shield layer, i.e. $w_c(\pi/2,\varphi) = 2(D-T)\tan\alpha$. Tilted milling complicates this by introducing two degrees of freedom: tilt angle θ and rotation angle φ (shown in Figure 1). In this section, we deal with two corner cases of rotation angle φ: when it is perpendicular ($\varphi = 0$) or parallel ($\varphi = \pi/2$) to shield wires, as shown in Figure 2. It is easy to see tilting in the plane parallel to shield wires ($\varphi = \pi/2$) only makes the cut-off width $w_c(\theta,\pi/2)$ larger: $w_c(\theta,\pi/2)$ can be found by calculating the minor axis of the intersection between the cone and the bottom plane of the layer of the shield wires,

$$\begin{aligned} w_c(\theta,\pi/2) &= 2\text{sin}\theta(D-T)(\text{cot}(\theta-\alpha)-\text{cot}(\theta+\alpha)) \\ &= \frac{4(D-T)\text{tan}\alpha}{\text{sin}\theta - \text{tan}^2\alpha(\text{sin}\theta-\text{csc}\theta)} \end{aligned} \tag{1}$$

Which can be easily shown to be increasing as θ decreases. Therefore, tilting when $\varphi = \pi/2$ makes cut-off width $w_c(\theta,\pi/2)$ wider than top-down case. This makes shield wire cutting more likely and is undesirable for attacker.

This leaves the case of tilting in the plane perpendicular to shield wires, i.e., $\varphi = 0$. This case was studied in [6], which gives

$$w_c(\theta,0) = \frac{\sin 2\alpha}{\sin(\theta+\alpha)\sin(\theta-\alpha)}D - \begin{cases} T\cot(\theta-\alpha) & ,\ \theta\in[0,\frac{1}{2}\pi-\alpha] \\ T(\cot(\theta-\alpha)-\cot(\theta+\alpha)) & ,\ \theta\in[\frac{1}{2}\pi-\alpha,\frac{1}{2}\pi] \end{cases} \tag{2}$$

Calculating $\frac{\partial(w_c(\theta,0)/w_c(\pi/2,\varphi))}{\partial\theta} = 0$ shows a minimum $w_c(\theta,0)$ exists that is lower than $w_c(\pi/2,\varphi)$ [6].

B. Impact of Rotation upon Cut-off Width

The question remains whether any rotational angle $\varphi \in (0,\frac{1}{2}\pi)$ exists in between that makes probing attack more vulnerable than these two extremes. For this purpose, we use a planar model where both top and bottom intersections of the milled cavity and shield wire are projected to the top surface of the shield wire, as shown in Figure 3. As shown in the figure, we seek to study the largest cut-off width $w_{c,\varphi}$ when projection of targeted point of probing width is separated from that shield wire by a certain distance P. The bypass attack is considered unsuccessful when $w_{c,\varphi}$ becomes larger than min-width of shield wire w_i; therefore an increased $w_{c,\varphi}$ indicates less favorable rotation angle φ.

Intersection with top surface is represented with a red ellipse, while bottom intersection is represented with a blue one. The fact that both intersections are ellipses enables us to construct Cartesian axes so as to express w_c in terms of φ and P, as shown in Figure 4.

Cartesian axes in Figure 4 are constructed with its origin at the center of the top intersection ellipse, while its x and y axes follow the longer and shorter axes of the ellipse, respectively. These coordinates yield the following expression of both ellipses and edges of the shield wire as follows:

1) Top intersection: $b_1^2x^2 + a_1^2y^2 = a_1^2b_1^2$, where
   a) $a_1 = \frac{D}{2}(\cot(\theta-\alpha)-\cot(\theta+\alpha))$
   b) $b_1 = a_1\sin\theta$
2) Bottom intersection: $b_0^2(x-\Delta x)^2 + a_0^2y^2 = a_0^2b_0^2$, where
   a) $a_0 = \frac{D-T}{D}a_1$, $b_1 = \frac{D-T}{D}b_1$
   b) $\Delta x = T\cot\theta$
3) Edges of shield wires: $y = k(x-\Delta x)+c_0$ and $y = kx+c_1$
   a) $k = \cot\varphi$.
   b) $w_c(\theta,\varphi) = \sin\varphi(c_1 - c_0 + k\Delta x)$

Both nearer (red) and farther (blue) edges of a shield wire intersects top and bottom ellipses at one point only. The above equations simplifies into

$$\begin{aligned} w_c(\theta,\varphi) = \sin\varphi[&\frac{2D-T}{2}(\cot(\theta-\alpha) \\ &-\cot(\theta+\alpha))(\cot^2\varphi+\sin^2\theta)^{\frac{1}{2}} - T\cot\theta\cot\varphi] \end{aligned} \tag{3}$$

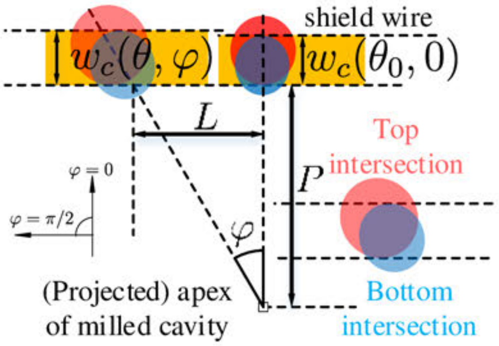


Fig. 3: Model formulation to study impact of rotational angle φ upon cut-off width.

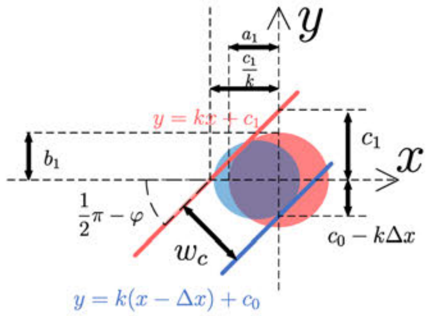


Fig. 4: Cartesian axes to find w as function of φ.

We can establish a relationship between φ and θ by utilizing the fact that the line segment between center of top ellipse and projection of target point of probing can be expressed using Figure 2 or Figure 3, i.e.

$$\begin{cases} \frac{c_1}{k} + P\sec\varphi = D\cot(\theta+\alpha) + a_1 \\ c_1 = \sqrt{b_1^2 + a_1^2 k^2} \\ k = \cot\varphi \end{cases}$$
$$\implies \cos\varphi = |\frac{2A}{-B - \sqrt{B^2 - 4AC}}| \tag{4}$$

where

$$A = P^2 - b_1^2$$
$$B = 2P(D\cot(\theta+\alpha) + a_1)$$
$$C = D\cot(\theta+\alpha) + a_1)^2 - a_1^2 + b_1^2$$

Equation 3 and Equation 4 together allow us to plot numeric solutions to address our initial question. A numeric analysis on this relationship is presented in Section V, which suggest that rotational angles $\varphi \in (0, \frac{\pi}{2})$ make for less effective bypass attacks than $\varphi = 0$, i.e. perpendicular to the shield wire.

IV. Design Principles to Deter Probing Attacks

We have shown angled probing attacks have the potential to make bypassing the shield easier. This begs the question whether any countermeasure exists. We find such remedy likely lies in multiple-layered shields, for the simple reason that a shield consisting of multiple layers of wire mesh defies basic assumptions used in analyzing bypass attacks against active shields so far.

A. Orthogonal multi-layered shield

An apparent design choice to counter such attacks is to construct an *orthogonal shield*, i.e., active shield comprised of at least two layers, wires in each layer in perpendicular direction from the other. Since tilting in perpendicular against one layer of mesh will be in parallel with another, this arrangement protects against the most vulnerable perpendicular direction. Further, through numerical simulations based on Equations 3 and 4 (shown in Section V), we have evidence that any rotational direction φ between fully perpendicular and parallel leads to more likelihood to completely cut off a shield wire.

This indicates that an orthogonal shield is not vulnerable to tilted microprobing attacks. Nevertheless, providing for random signals secure enough to defeat replay attack for an additional layer can be costly in terms of area overhead.

B. Staggered parallel multi-layered shield

Another apparent approach to address challenge of high aspect ratio (R_{FIB}) FIB equipment is to manipulate routing track origins of shield wires of each layer so that the distance between centers of two closest shield wires when viewed from a top-down angle is a fraction of that of largest component layer, as illustrated in Figure 5. Typically, design rules require wires to be placed at least one *pitch* away from another, where *pitch* is individually specified for each routing layer. By manipulating origins of routing tracks of shield layers, shield wires in one routing layer can be placed in the middle of two closest wires in another routing layer, when viewed from top-down direction. In the case of two layers, this can be done by giving either layer an offset equaling half of the routing pitch (assuming both layers has the same routing pitch); in the case of three layers, offsets can be calculated by assuming diameters of all three possible highest deterred R_{FIB} attacks (i.e., between wires on first and second layer, second and third layer, third and first layer) are the same; simple calculation yields offsets as

$$\begin{cases} \Delta x_2 = & \frac{1}{6}(-w_1 + 2p - (w_2 + (T_2 + T_{D,1})\tan\alpha) + \\ & 2(w_3 + \sum_{i=2}^{3}(T_i + T_{D,i-1})\tan\alpha)) \\ \Delta x_3 = & \frac{1}{6}(w_1 + 4p - 2(w_2 + (T_2 + T_{D,1})\tan\alpha) + \\ & (w_3 + \sum_{i=2}^{3}(T_i + T_{D,i-1})\tan\alpha)) \end{cases} \tag{5}$$

Maximum effective R_{FIB} the multi-layer staggered shield could protect against ($R_{\text{FIB,max}}$) improves if probing attack is believed to be only performed top-down. However, one disadvantage of this arrangement is that when probing attack is tilted, the multi-layer staggered shield is likely only as secure

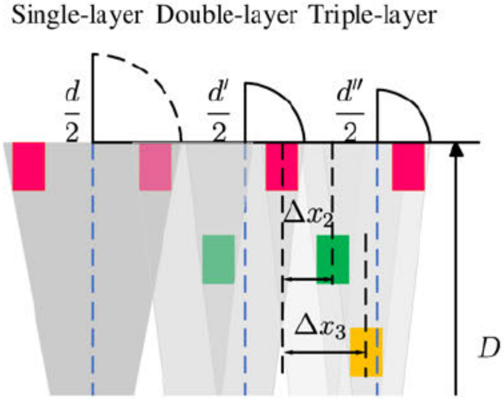


Fig. 5: When multiple layers are used for staggered parallel shield, the shield is made more secure against bypass attacks with higher R_{FIB} FIB equipments: diameter d shown in figure taken when R_{FIB} is highest that the shield is secure against; d is inversely proportional to aspect ratio $R_{\text{FIB,max}}$ used in milling the cavity.

as its most secure single layer.This observation is supported by results from numeric simulation, which are presented in Section V.

V. Numeric Results and Discussions

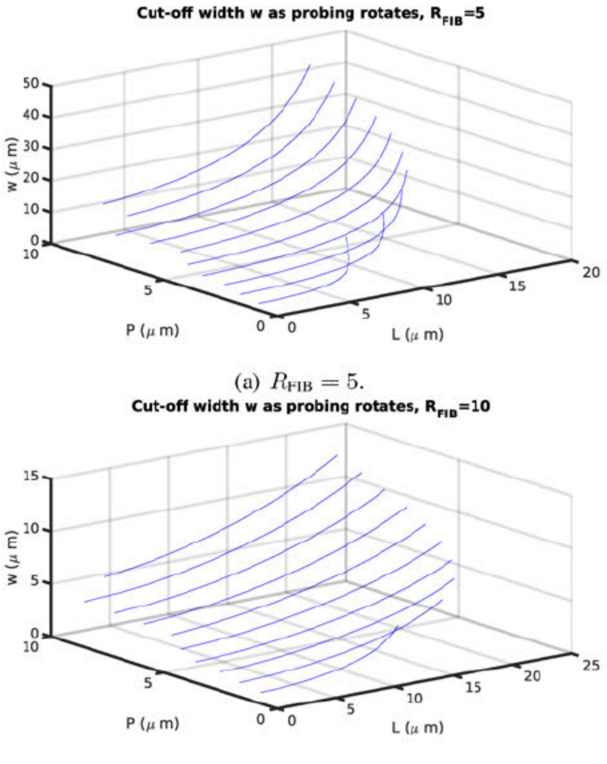
In this section, we present numeric simulation results to support and elaborate on theoretic conclusions made in Section IV. In both investigations, Synopsys' SAED90nm library was used to provide dimension data. Since calculations involved in our investigations are primarily based on back-end-of-line (BEOL) stack dimensions, results obtained should remain indicative of most other recent technologies since such dimensions will unlikely change dramatically.

A. Numeric Analysis on Rotational Angle upon Cut-off Width

In this simulation, data are calculated with Equation 3 and Equation 4. We plotted this relationship assuming target wires on M4 layer and shield wires on M8 layer for $R_{\text{FIB}} = 5$ and $R_{\text{FIB}} = 10$. P and L in Figure 6 are defined in Figure 3. Traces shown in each figure depict $w_c(\theta, \varphi)$ when P takes different values. Presented results shows a monotonic increase of cut-off width w as φ increases, i.e. rotating towards becoming parallel to shield wires. In all cases, best rotational direction (i.e. lowest w) for the attacker is $\varphi = 0$, i.e. perpendicular to the shield wire. This provides sufficiently reliable basis to consider non-perpendicular rotational directions inferior for the bypass attack.

B. Numeric Analysis on Impact of Tilt on Multi-layer Staggered Shields

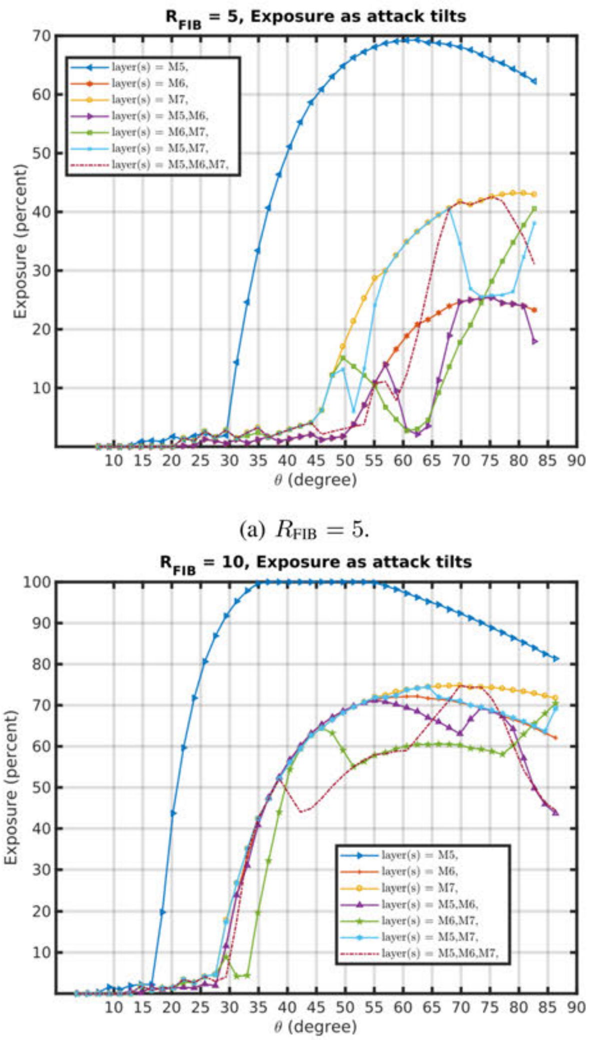
In this experiment, a number of multi-layer staggered shields are constructed as was described in Section IV-B. Layer M5, M6, and M7 are chosen for the purpose of including effect of different pitch sizes across member layers in the investigation is desirable, and in SAED90nm library pitch size in M7 is twice as wide as in M5 and M6. In cases of M6-M7 and M5-M7 shield, M5 and M6 layer are inserted without offset since they already are twice as dense as M7; Offsets of M5-M6-M7 shield are calculated with Equation 5. Results are presented in terms of exposed area, defined as area if axis of milling is placed in will result in complete cut-off of at least one shield wire. This is calculated using method described in [6] by making necessary modifications to account for tilted milling. Resulting exposure data are shown in Figure 7. M5-M6-M7 case performing worse than M6-M7 case is likely due to former being optimized for top-down milling, leaving larger weakness at certain angles than two layer design, as shown in Figure 5. Performance of M5 being much worse than M7 while M6 remains most desirable is as expected since in SAED90nm library M5 is much deeper than M7 while M7 has twice as wide routing pitch. Our earlier expectation that multi-layer staggered shield tends to behave as its best component layer when tilted is also corroborated as the result shows 2-layer and 3-layer shields are occasionally as bad as its best component layer but never worse than it. It is also interesting to see that at most vulnerable angle of the shields it is likely for multi-layer shield to be only as good as its best layer, since staggering cannot be designed for that angle and its complementary angle simultaneously. Finally, M6-M7 combination tends to outperform other 2-layer combinations, showing that layer dimensions' impact. To summarize, presented numeric results



(a) $R_{\text{FIB}} = 5$.

(b) $R_{\text{FIB}} = 10$.

Fig. 6: As milling axis rotates, cut-off width w increases. Traces represent cut-off width on shield wires at distance P from center of cavity.



(a) $R_{\text{FIB}} = 5$.

(b) $R_{\text{FIB}} = 10$.

Fig. 7: Numeric results on exposed percentage of various multi-layer staggered shield construction as probing attack tilts.

corroborates our expectation that multi-layer staggered shield is vulnerable to tilted bypass attacks, but might remain useful when tilted attack is prevented, e.g. when implemented in conjunction with orthogonal shield.

VI. Conclusion

Bypass attack is the greatest vulnerability of the most common countermeasure, which has been shown to be more powerful with tilted probing. In this paper, we have constructed mathematical models to characterize tilted microprobing attacks, evaluated possible design remedies and showed with numeric corroboration that orthogonal multi-layer shield is capable of preventing tilted microprobing attacks. Our investigation on staggered multi-layer shield showed that although vulnerable to tilted microprobing attacks, staggered two-layer shield can improve maximum FIB aspect ratio shield is effective against. We expect these findings to inform future active shield designs and shape design choices.

References

[1] S. Skorobogatov, "Physical attacks on tamper resistance: progress and lessons," in *Proc. of 2nd ARO Special Workshop on Hardware Assurance, Washington, DC*, 2011.

[2] C. Tarnovsky, "Tarnovsky deconstruct processor," youtube. [Online]. Available: https://www.youtube.com/watch?v=w7PT0nrK2BE

[3] V. Ray, "Freud applications of fib: Invasive fib attacks and countermeasures in hardware security devices," in *East-Coast Focused Ion Beam User Group Meeting*. Feburuary, 2009.

[4] R. Anderson, *Security engineering: A guide to building dependable distributed systems*. Wiley, 2001.

[5] C. Tarnovsky, "Security failures in secure devices," in *Black Hat Briefings*. Feburuary, 2008.

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

[7] "Building a secure system using trustzone technology," 2009. [Online]. Available: http://infocenter.arm.com/help/topic/com.arm.doc.prd29-genc-009492c/PRD29-GENC-009492C_trustzone_security_whitepaper.pdf

[8] S. E. Quadir, J. Chen, D. Forte, N. Asadizanjani, S. Shahbazmohamadi, L. Wang, J. Chandy, and M. Tehranipoor, "A survey on chip to system reverse engineering," *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, vol. 13, no. 1, p. 6, 2016.

[9] 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*, vol. 27, no. 4, pp. L18–L20, 2009.

[10] 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 *Proceedings of the 5th Singapore-MIT Alliance Annual Symposium*, 2005.

[11] P. Laackmann and H. Taddiken, "Apparatus for protecting an integrated circuit formed in a substrate and method for protecting the circuit against reverse engineering," Sep. 28 2004, uS Patent 6,798,234.

[12] 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 *Computational Intelligence and Security (CIS), 2012 Eighth International Conference on*. IEEE, 2012, pp. 530–533.

[13] A. Beit-Grogger and J. Riegebauer, "Integrated circuit having an active shield," Nov. 8 2005, uS Patent 6,962,294. [Online]. Available: https://www.google.com/patents/US6962294

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

[15] S. Briais, J.-M. Cioranesco, J.-L. Danger, S. Guilley, D. Naccache, and T. Porteboeuf, "Random active shield," in *Fault Diagnosis and Tolerance in Cryptography (FDTC), 2012 Workshop on*. IEEE, 2012, pp. 103–113.

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

[17] Y. Ishai, A. Sahai, and D. Wagner, "Private circuits: Securing hardware against probing attacks," in *Advances in Cryptology-CRYPTO 2003*. Springer, 2003, pp. 463–481.

[18] D. B. Roy, S. Bhasin, S. Guilley, J.-L. Danger, and D. Mukhopadhyay, "From theory to practice of private circuit: A cautionary note," in *Computer Design (ICCD), 2015 33rd IEEE International Conference on*. IEEE, 2015, pp. 296–303.

[19] H. Wu, D. Ferranti, and L. Stern, "Precise nanofabrication with multiple ion beams for advanced circuit edit," *Microelectronics Reliability*, vol. 54, no. 9, pp. 1779–1784, 2014.

[20] S. Tajik, H. Lohrke, J.-P. Seifert, and C. Boit, "On the power of optical contactless probing: Attacking bitstream encryption of fpgas," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '17. New York, NY, USA: ACM, 2017, pp. 1661–1674. [Online]. Available: http://doi.acm.org/10.1145/3133956.3134039