Contact-to-Silicide Probing Attacks on Integrated Circuits and Countermeasures

Ana Covic, Qihang Shi, Haoting Shen and Domenic Forte
ECE Department, University of Florida, (anaswim, qihang.shi)@ufl.edu, (htshen, dforte) @ece.ufl.edu

***Abstract*—Sensitive data contained and processed in integrated circuits (ICs), such as secret keys and encrypted firmware, can be extracted with focused ion beam (FIB) based probing attacks. Due to the unprotected structure on the backside of the die, the threat of backside probing attacks is particularly grim. In this study, we develop a quantitative model for backside probing attacks and apply it to three latest technology nodes 7, 10 and 14 nm with 3, 5, 8 and 10 FIB aspect ratios. The probed opening is modeled to have shape of conical frustum, which allows FIB beam diameter, in range of 10nm to 33.3nm, to produce the opening with diameter in range of 22nm to 57.3nm. We also propose a novel backside shield design structure with an estimated 16% area overhead that terminates the die operations as a result of probing to prevent malicious data extraction. Proposed backside countermeasure increases the complexity of the attack performed on protected die.**

***Index Terms*—FIB, micro-probing, security**

I. Introduction

The sensitive data stored on integrated circuits (ICs), in smart cards, smartphones, military, medical and financial systems, is now being targeted for extraction by physical attacks. Such attacks may be performed from either the frontside (upper metal) or the backside (silicon substrate) of the die by bypassing, rerouting, or disabling security modules such as verification and/or encryption blocks. Various countermeasures have been investigated, but they typically protect against the frontside attacks only while the backside is left exposed.

The backside probing attack [1] discussed in this paper requires sample preparation to obtain physical access to the chip, while maintaining partial or complete functionality for data extraction. Probing attack consists of multiple steps. First, the chip needs to be decapsulated, which can be accomplished by using chemicals, laser, plasma or mechanical polishing. Further die de-processing may also be done by mechanical polishing or using focused ion beam (FIB) [1]. Probing attacks require accessible spot size to be precise and accurate, meaning that the probe should not touch multiple nodes as it could short the circuit. Therefore, recent IC chips fabricated by advanced technology nodes require advanced FIB technology, such as helium ion microscope (HIM), which can deposit a sub-10nm interconnect or pad [2].

FIB utilizes strong and precise high current beam of ions for milling, material removal and deposition. FIB, although was initially developed for failure analysis, has been shown as a powerful tool for probing and circuit edit. FIB technology has been advancing at similar rate as transistor technologies representing serious threat to IC chips. Although expensive, nowadays more laboratories have purchased FIB systems for research and/or service. Meanwhile, renting from or collaboration with these laboratories makes it more affordable than ever to launch probing attacks on ICs.

Probing attacks can occur through the IC frontside (i.e., top metals) or backside (i.e., silicon substrate). Compared to frontside attack, the targets of backside probing are not limited to metal wires. According to [3], the most dangerous backside attack is contact-to-silicide probing, since silicide covers the entire unprotected active regions of transistor. Insulation is not needed when opening is milled for the contact-to-silicide (CtS) attack, because opening goes only through substrate and doped regions of substrate. Schottky contacting between Si and deposited metals ensures connection of these regions without significant current, so insulation layer in the opening is unnecessary [3]. In this way, the adversary can get access to the source/drain of *any single transistor*. Compared to contact-to-contact, or contact-to-metal probing attacks, silicide covers the whole area of the active regions of drain/source, which provides a significantly larger area than the area of the single contact for probing. This allows contact-to-silicide attack to require less precise milling than other methods.

Countermeasures against frontside probing attacks have been developed, such as active shields, t-private circuits, analog shields and sensors [4]. These methods provide protection of the IC, but most of them are not successful against backside attacks also having the costly implementation. Analog shields could measure changes in impedance caused by backside probing, but this method is not reliable as it is sensitive to environmental variations. Analog sensors also have reliability issue, as self-destructive mechanisms can be disabled by FIB probing. T-private circuits increase the complexity of any probing attack by requiring multiple simultaneous probes, but increasing the number of probes introduces non-linear costly area overhead [4]. Led by this motivation, quantification of threat and guidance for improvement of future standard cells and layouts are analyzed in this paper, with aim to improve the quality and reliability of backside probing defense measures. Our major contributions, are as follows:

- A quantitative model incorporating various FIB and technology node parameters in order to assess the susceptibility of modern designs to backside probing attacks.
- Analysis of backside probing attacks on FinFET transistors in 7nm, 10nm and 14nm technology nodes. Our conclusions can be extended to older technologies as well.

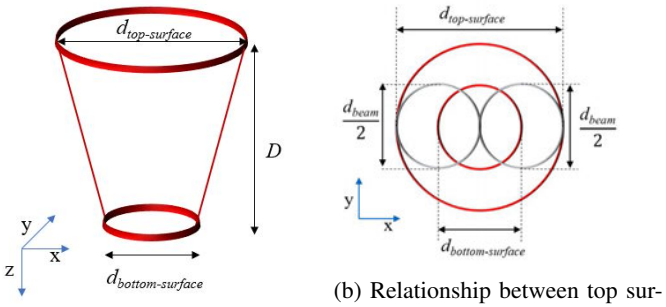
- A novel countermeasure that extends active shield technologies to the backside. Our evaluation of the pros and cons of this countermeasure reveals that it significantly increases the attack complexity.

The rest of the paper is organized as follows. In Section II, we provide our detailed attack model on single and multi-fin FinFETs. In Section III, we propose backside countermeasure, evaluate possible attacks and compare it to state-of-the-art countermeasures evaluating its effectiveness. Finally, we conclude in Section IV.

II. Attack Model

Most of existing work has covered attack models and countermeasures for the frontside of the IC [4]. However, in this paper, we are focused oback-n side attacks. Various physical probing attacks with FIB have been proposed on older technologies and the most efficient one has been contact-to-silicide (CtS) attack. Silicide is the material formed on the top of transistor drain and source terminals to form ohmic contacts between silicon and metals. This probing requires less precision compared to probing of the contact or metal line of the transistor because there are no metal interconnects present below the substrate to obstruct FIB milling and deposition.

Our attack model assumes sample preparation, which consists of backside die thinning by mechanical polishing and further material removal of the desired area with FIB to the thickness of 100nm. For the precise alignment, scanning electron microscope (SEM) on the FIB system must be able to see through the Si substrate and accurately observe at least the doping regions. Thus, considering the aspect ratio of the opening , we assume 100nm is the maximum thickness allowed for the precise alignment and milling of the opening with the respect to active region, where silicide is located. A milled opening has a conical frustum shape, as shown in Fig.1a. After milling, we model that the attacker will deposit metal in the opening. A nano probe will make contact to this metal in order to read data from the transistor.



(a) Conical frustum

(b) Relationship between top surface, beam and bottom surface diameters

Fig. 1: Geometry of milled opening

Note that since the backside is unprotected, virtually any transistor silicide can be probed without failure unless it results in a short circuit of two transistors. *In this paper, we assume that the attacker wants to probe adjacent active regions of two transistors* of 7nm, 10nm and 14nm technology nodes and for different probing specifications defined by aspect ratios: 3, 5, 8 and 10. Aspect ratio is the ratio between depth of the milled opening and diameter of the top surface of opening considering zero spot size. Adversary with larger aspect ratio poses a more dangerous threat than adversary with smaller aspect ratio. The reason for that is the ability to mill deeper opening with smaller diameter. Thus, the attack is modeled for range of available aspect ratios. Design rules [5] specify that the minimum width of active area and minimum spacing between two adjacent active areas are 4λ, where λ is a parameter defined by the technology node.

The three technology nodes analyzed in this paper are all three-dimensional FinFET, single fin and multi-fin nodes. Multi-fin structures are used for achieving greater current in a smaller area, as well as equal rise and fall times in CMOS. Variables used for modeling attacks on single and multi-fin FinFETS in this paper are defined in Table I.

TABLE I: Variables

Variable	Description
$d_{top\text{-}surface}$	The top surface diameter of opening
$d_{bottom\text{-}surface}$	The bottom surface diameter of opening
$d_{top\text{-}surface\text{-}maximum}$	The largest top surface diameter of opening that the milled opening can have such that deposition does not short adjacent target regions
D	Depth of the opening
d_{beam}	The top diameter of FIB beam
δ	Vertical distance between centers of openings in multi-fin FinFET attack

A. Attack on Single-fin FinFET

Fig. 2 illustrates our initial attack model and important parameters for a single fin device.

Length of the fin is defined by fabrication and process variation, but from [6], maximum fin length is 1λ. So, the width of targeted active region is 3λ, instead of 4λ. The pitch of the area under attack is 7λ, where the width of active region is 3λ, and the spacing is 4λ, as shown in Fig. 2. Since the conical frustum has top surface diameter larger than the bottom surface diameter, $d_{top\text{-}surface}$ has a size of the area under attack, 7λ. To avoid shortage between two openings that are created for probing different transistors, 10nm of additional distance is introduced between two openings as a safety margin. This is needed due to FIB stage or operator imprecision. In (1), we define

$$d_{top\text{-}surface} + 10nm = 7\lambda \quad (1)$$

Table II shows $d_{top\text{-}surface\text{-}maximum}$ for the three technology nodes calculated from (1). Diameter of the bottom surface opening at the active region is defined by technology node and the size of targeted active region. Maximum $d_{bottom\text{-}surface}$ is equal to the minimum size of active region, 3λ, to avoid connection of multiple source/drain/channel regions. Table III shows the bottom surface diameter of opening for all three technology nodes, where λ is from [7] – [9]

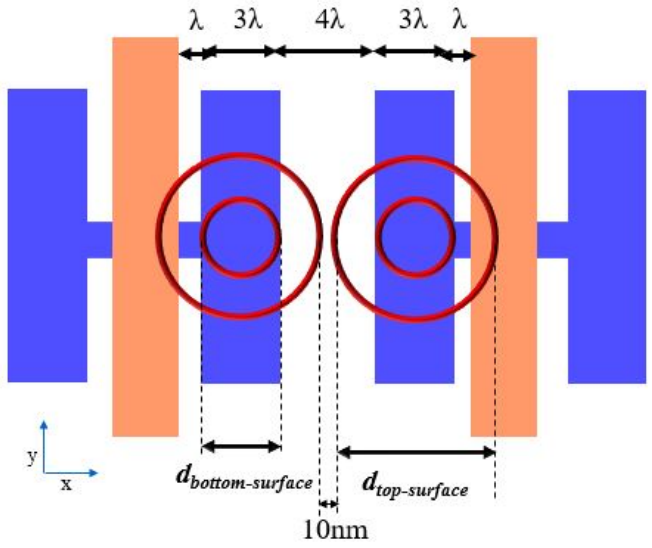


Fig. 2: Top down view for single-fin attack model where orange regions are polysilicon and blue regions are active doped regions.

TABLE II: Maximum top surface diameter

Technology Node [nm]	$\mathbf{d_{top\text{-}surface\text{-}maximum}}$ **[nm]**
14	46
10	32
7	18

The bottom surface of opening with $d_{bottom\text{-}surface}$ at the active region of transistor, is to be achieved by FIB. Beam is defined by the aspect ratio, ratio of $d_{top\text{-}surface}$ and D, from Fig. 1a. Since the shape of desired opening for this attack is conical frustum, bottom surface of the opening is achieved by dragging the beam in the circular area with already defined $d_{top\text{-}surface}$, constrained by (1). Beam specifications are the same, regardless of the value of $d_{top\text{-}surface}$. Considering zero spot size and D of 100nm, d_{beam} is shown in Table IV based on multiple aspect ratios.

From Fig. 1b, the relationship between $d_{top\text{-}surface}$, d_{beam} and $d_{bottom\text{-}surface}$ is defined as

TABLE III: Maximum bottom surface diameter

Technology Node [nm]	λ**[nm]**	$\mathbf{d_{bottom\text{-}surface}}$ **[nm]**
14	8	24
10	6	18
7	4	12

TABLE IV: Beam diameter

Aspect ratio	3	5	8	10
$\mathbf{d_{beam}}$ **[nm]**	33.3	20	12.5	10

$$d_{\text{top-surface}} = d_{\text{bottom-surface}} + d_{\text{beam}} \quad (2)$$

The calculated values of $d_{top\text{-}surface}$ for three technology nodes and multiple values of aspect ratio are shown in Table V. For the cases when $d_{top\text{-}surface}$ is greater than $d_{top\text{-}surface\text{-}maximum}$, distance between centers of openings cannot be parallel to the horizontal distance of 7λ, between two adjacent active regions, as shown in Fig. 2. Such alignment is not possible because it would make openings to overlap. This is the case for 14nm technology node for aspect ratio of 3; 10nm technology node for aspect ratios 3 and 5; and for all aspect ratios of 7nm technology node. In other words, those cases are not susceptible to attacks on adjacent transistors.

TABLE V: Top surface diameter of the opening

Technology node [nm]	**Aspect ratio**			
	3	5	8	10
	$\mathbf{d_{top\text{-}surface}}$**[nm]**			
14	57.3	44	36.5	34
10	51.3	38	30.5	28
7	45.3	32	23.5	22

B. Attack on Multi-fin FinFET

Fig. 3 illustrates our attack model and important parameters for a multi-fin device.

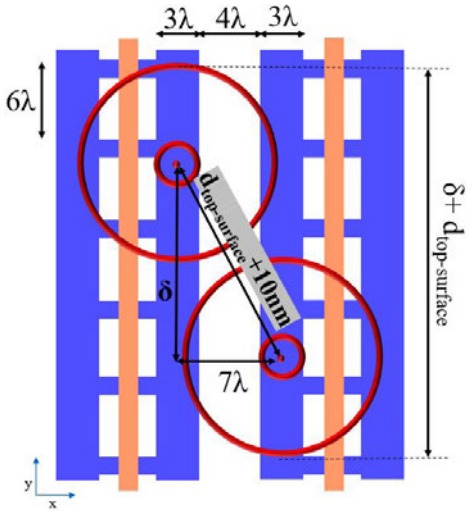


Fig. 3: Multi-fin attack model where orange regions are polysilicon and blue regions are active doped regions

Multi-fin FinFET structures are vulnerable to attacks with all aspect ratios because of the larger area available for probing. As shown in Fig. 3, multi-fin attack does not allow distance between centers of openings to be parallel with horizontal distance between active regions, so vertical distance δ needs to be found. Horizontal distance is known from design rules [6], while the distance between centers of openings is modeled to be $d_{top\text{-}surface}$ + 10nm. Distance between opening centers is hypotenuse of right triangle, with catheti being

horizontal distance of and δ. To find the δ, Pythagorean Theorem is used. Maximum horizontal distance is equal to $d_{\text{top-surface-maximum}}$, 7λ; the fin pitch [6] is 6λ, as shown in Fig. 3. To calculate number of fins needed for all three technology nodes to be vulnerable, (3) is used.

$$Fin_{\text{number}} = \frac{\delta + d_{\text{top-surface}}}{6\lambda} \tag{3}$$

δ + $d_{\text{top-surface}}$ is the total vertical distance two openings occupy and 6λ is the fin pitch. Table VI shows the number of fins needed for adjacent transistors to be vulnerable for four different aspect ratios in all three technology nodes.

For the single-fin FinFET instances in Table VI, the probeable area of active region area is 100% with top surface diameters confined in Table V. This means that alignment of the openings is not limited, but the size of top surface diameter is limited to avoid overlapping. However, for the multi-fin cases from Table VI, probeable area of a single transistor is defined by (4).

$$Area_{\text{probable}} = (W - \frac{\delta + d_{\text{top-surface}}}{2}) * 3\lambda \tag{4}$$

The width of the active region of transistor is 3λ, and the length of the transistor is W. Vertical probeable length of active region is the total length W, reduced by half of δ + $d_{\text{top-surface}}$, total vertical distance occupied by top surface of openings. Since the total area of the active region is W*3λ, the probeable active region area with the respect to the complete area of a single active region, is defined in (5).

$$\frac{Area_{\text{probeable}}}{Area_{\text{total}}} = \frac{3}{4} * (1 - \frac{\delta + d_{\text{top-surface}}}{2W}) \tag{5}$$

TABLE VI: Number of fins

Technology node [nm]	**Aspect ratio**			
	3	5	8	10
	Number of fins			
14	2	1	1	1
10	3	2	1	1
7	4	3	2	2

Considering 1μm long FinFET, the worst case probable area is 71%, for the $d_{\text{top-surface}}$ of 57.3nm and aspect ratio of 3, while the best case scenario for $d_{\text{top-surface}}$ of 22nm and aspect ratio of 10 is 74%.

III. Proposed countermeasure

To protect against the attacks modeled in Section II, we propose the backside metal shield. Existing work investigated frontside metal shield connected to the shield located at the lower metal layer which is identical to the top layer metal shield [3]. If any part of the shield is removed, the chip responds by self-destruction of critical data. A similar idea is developed for the backside metal shield. However, while the conventional frontside shield can be integrated as upper metal layers of an IC, additional fabrication steps are needed on the backside of the wafer in our case. First, metal traces would be deposited at the backside of the substrate. The traces must be connected to the inner logic located at the frontside of the IC consisting of pattern generator and comparator. As the strategy used for the frontside shield, the backside shield also carries signals. Cross-check of logic values can be performed to test if any traces are changed by the probing attack. In addition to monitoring logic values, another probing detection method, inspired by the analog shields and detectors [4], is monitoring the range of impedance and time constant. If significant mismatch to predefined range of impedance and time constant is detected, alarm signal is sent to recognize the attack. However, range of analog parameters needs to be carefully predefined because of the process variations that take place in chip manufacturing phase. Combination of multiple probing detection methods makes this countermeasure more secure and reliable.

To let the backside shield carry the signal, it needs to be connected to the frontside by through silicon vias (TSVs). Nowadays, TSVs are widely used for 2.5/3D IC packages and vertical stacking of multiple ICs. The most limiting properties of the TSVs for designing backside metal shield are the density and the pitch of TSVs. From various reported dimensions, following dimensions are chosen to work the best with our application, as shown in Table VII [10].

TABLE VII: TSV property

Property	**Size [μm]**
Width	10
Pitch	25
Length (wafer thickness)	200

Taking Intels Skylake scalable-performance SP as an example. The 10-core low-core-count LCC die has an area of 322mm^2 [11], allowing 720 TSVs along one side of the die of 18mm, and thus 518 thousand TSVs on the back in total. Considering the width of TSVs, the area overhead from the TSVs in this die would be 16%. With 518 thousand TSVs, metal shield consists of metal traces connecting these TSVs. Increasing the number of metal traces, rerouting of the shield encounters a greater challenge. Additional metal layer secured at the back of the die is the only layer overhead. Compared to any other countermeasure [4], this approach requires identical number or less additional layers added to design.

A. Attack Steps Against backside Metal Shield

Following the method used by the backside probing attack on unprotected die from Section II, modifications are required to perform the attack on shielded die because of the existence of the shield. Considering that the backside of the die would now be covered with metal traces of the pitch of 25μm and width of 10μm, as defined in Table VII, adversary would now have to perform more complex sample preparation consisting of metal trace removal and TSVs removal in addition to silicon removal. Sample preparation consists of several steps.

The first step consists of removal of metal traces, TSVs and silicon, as shown in Fig. 4b. If the metal traces are removed using etching technique, not only metal traces would be removed, but also metal TSVs, which are connected to metal traces. So, time to remove metal traces and TSVs would be incorporated into one step and it would depend on etching rate of both metals. This technique leaves less material to be mechanically polished. However, if etching technique is omitted, metal traces, TSVs, and surrounding silicon would all be mechanically polished together. Polishing time, in this case, would be affected by polishing rate of different materials: two metals and silicon.

This attack requires the die to be polished to the thickness of 20µm because removed backside shield must be recreated. To reroute the shield, 20µm of thickness allows metal traces to be deposited lithographically. Lithography allows for automated simultaneous deposition of all metal traces, while FIB metal deposition requires operator to create individual traces one at the time. So, the second step is new and consists of rebuilding of the metal traces back on the die by lithography to prevent the logic and/or impedance mismatch between inner and outer shield. Once the die is thinned to 20µm, the height of TSVs is decreased, as shown in Fig. 4b, so the resistance is decreased accordingly. To increase the resistance to the original value, width and pitch of new lithographically deposited metal traces must be significantly different. There are two approaches in determining new dimensions of metal traces: (1) The length of metal traces to be kept the same as before, since the density of TSVs is constant. So, the width of traces must decrease, as the resistance is proportional to the length and inversely proportional to the cross-section area of the trace; (2) The width of the metal traces to be kept the same as before thinning of the die, but the length of the traces increases, by rerouting techniques.

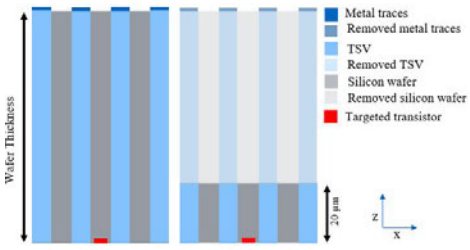


Fig. 4: (a) Cross-section of implemented backside shield where the top of figure is bottom of the IC
(b) Thinning to 20µm thickness

In both approaches, changing the dimensions of the metal traces results in change of capacitance between neighboring traces. In the first approach, decreasing the width of metal traces results in pitch increase, which consequentially increases capacitance. The second approach also affects capacitance. Rerouting can introduce increase in distance between traces, which can neutralize the effect of increased cross-section. However, rerouting can introduce parallel capacitance between metal traces that was not significant before rerouting, resulting in increased capacitance overall.

Thus, it is challenging to lithographically pattern new metal traces because there is a trade-off between keeping resistance and capacitance the same as before. To keep resistance as before, new trace must increase the length of the trace, or decrease the width and thickness of trace. After sample preparation, capacitance decreases as well, so to increase the value of new capacitance, length, width or thickness of metal trace must increase. While length is required for both parameters to be increased, change in area (thickness and width) affects resistance and capacitance differently.

If the second step is accomplished successfully, the third step consists of FIB thinning, which was not present in the attack from Section II, as shown in Fig. 5b. Because the attack on unprotected die requires circular area of diameter of the size of at least 22nm and at most 57.3nm and the thickness of 100nm, FIB thinning to the thickness of 100nm is needed through the opening of area of 100µm by 100µm to provide enough space for FIB thinning. Thickness from step 2, is defined as 20µm instead of 100nm to allow lithographic metal trace deposition. Since the TSV density is less than 100µm, partial TSV removal and additional rerouting is needed to compensate for TSV and metal trace removal. This also makes this attack challenging.

Finally, last step of sample preparation is the same as in the attack from Section II, i.e., FIB milling of die in shape of conical frustum to the thickness of 100nm followed by metal contact deposition, as shown in Fig. 6b.

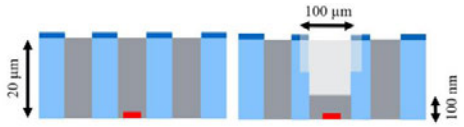


Fig. 5: Legend and orientation are the same as in Fig.4
(a) Result of Step 2 metal deposition
(b) Step 3 of sample preparation of die: 100µm opening and FIB thinning to 100nm thickness

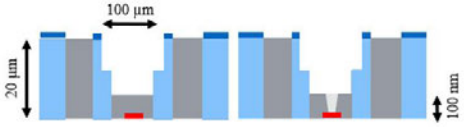


Fig. 6: Legend and orientation are the same as in Fig.4
(a) Result of Step 3 FIB opening and thinning to 100nm
(b) Attack performed from Section II

B. Countermeasure evaluation and comparison to other methods

Countermeasure from Section III consists of backside metal shield implemented using TSVs to connect the shield to logic located on the front side. To evaluate effectiveness of the countermeasure, possible attack was introduced in Section

III-A. The time to perform the attack on unprotected die, without considering package removal, consists of times from following steps:

$$t_{\text{No-protection}} = t_{\text{Si-removal}} + t_{\text{FIB-thinning}} + t_{\text{Conical-frustum-opening}} + \\ + t_{\text{Metal-deposition}} \tag{6}$$

However, once countermeasure is implemented, assuming that Step 2 from Section III is successfully performed, the time to perform the attack is significantly increased by:

$$\Delta t = t_{\text{Trace-removal}} + t_{\text{TSV-removal}} + t_{\text{FIB-opening}} + t_{\text{Re-routing}} + t_{\text{Lithography}} \tag{7}$$

Recreation of the metal shield is very demanding because of the need of cleanroom to perform lithography. The time and effort required to rebuild the metal shield will deter an attack at reasonable cost.

As discussed in Section III, area overhead for implementing backside shield, is 16%, because the changes of original die design are minimal through introduction of TSVs. Compared to the area overhead of different countermeasures, such as active mesh, analog shields and t-private circuits [4], area overhead produced from our design is significantly smaller. Method protecting frontside of the die, t-private circuits, consists of additional four AND logic gates and four XOR logic gates for every set of circuit in the original design. This method is effective, but it is very expensive [4]. Implementation of analog shields and sensors, as a method is very effective as well, and its area overhead is smaller than the one of t-private circuits, but it is not reliable because of the effect of process variations on analog parameters [4].

None of the methods discussed in [4] protect against backside attacks successfully. While analog shield, specifically probe attempt detector PAD [12] represents possible countermeasure against photon emission attack, scaling technology makes it ineffective. However, countermeasure introduced in Section III is not only effective against electrical probing attacks, but also against photon emission attacks. Photon emission is natural phenomena which occurs during transistor switching activity. In this attack, attackers passively monitor the activity of transistor, making photon emission hard to detect. However, with introduction of optical probing, active monitoring is done using laser to induce the light to transistor which gets reflected and captured by detector. For both, passive and active photon emission optical probing attacks, monitored transistors need to be exposed and openings need to be milled because latest FinFET technologies are fabricated on heavily doped silicon wafer, which does not allow infrared light to pass through silicon. Since our backside shield countermeasure does not allow successful transistor exposure, it is also effective against both electrical and optical probing attacks.

IV. Conclusion

In this paper we proposed two contact-to-silicide attack models from the backside of the die. Our results confirm that this attack is powerful against various technology nodes. Even newest technology FINFET nodes, such as 14nm, 10nm and 7nm are vulnerable because of the lack of backside countermeasures.

Since the current technologies do not have backside protection implemented, we also proposed the backside metal shield as the countermeasure for the backside of the die against our attack model. Compared to frontside countermeasures [13], this countermeasure requires minimal design changes by introduction of through silicon vias (TSVs). To detect the attack from the backside, probing detection methods would be based on detecting impedance, time constant and/or logic mismatches.

Further work needs to be done on developing probing detection methods and incorporating logic mismatch detection with analog properties mismatch detection. Reliability of the countermeasure needs to be quantitatively evaluated by balancing the fault-alarm with the respect of lack of alarm from the shield. Evaluation and implementation of the metal shield on the standard logic cells needs to be performed. Cell design and placement can be optimized to minimize probable area. Nevertheless, this paper represents an excellent initial step towards protection against a dangerous backside probing attack.

References

[1] Swarup Bhunia, Mark Tehranipoor, Hardware Security, Morgan Kaufman Publishers, 2019, pp. 250

[2] Zeiss Orion NanoFab, Zeiss, Product Information Version 2.0, Available: https://applications.zeiss.com/C125792900358A3F/0/0F2465540E1880F3C1257A7200336AEC/$FILE/EN_42_011_015_ORION_NanoFab_2_0.pdf

[3] R. Schlangen, P. Sadewater, U. Kerst, C. Boit, Contact to Contacts or Silicide by use of backside FIB Circuit Edit allowing to approach every Active Circuit Node, Microelectronics Reliability 46 (2006) 14981503

[4] H. Wang, D. Forte, M. M. Tehranipoor and Q. Shi, "Probing Attacks on Integrated Circuits: Challenges and Research Opportunities," in IEEE Design and Test, vol. 34, no. 5, pp. 63-71, Oct. 2017.

[5] Wang, Huanyu et al. A Physical Design Flow against frontside Probing Attacks by Internal Shielding. TECHCON 2018 (2018)

[6] Design rules: Microwind Lite 3.8

[7] Etienne Sicard. Introducing 7-nm FinFET Technology in Microwind, Microwind, Available: https://hal.archives-ouvertes.fr/hal-01558775/document

[8] Etienne Sicard. Introducing 10-nm FinFET Technology in Microwind, Microwind, Available: https://hal.archives-ouvertes.fr/hal-01551695/document

[9] Etienne Sicard. Introducing 14-nm FinFET Technology in Microwind, Microwind, Available: https://hal.archives-ouvertes.fr/hal-01541171/document

[10] A. Yu, J.H. Lau, S.W. Ho., et all. Fabrication of High Aspect Ratio TSV and Assembly with Fine-Pitch Low-Cost Solder Microbump for Si Interposer Technology with High-Density Interconnects, IEEE Transactions on components, packaging and manufacuting technology, Vol. 1., No. 9., September 2011

[11] Ian Cutress, The Intel Skylake-X Review: Core i9 7900X, i7 7820X and i7 7800X Tested, June 19, 2017, Available: https://www.anandtech.com/show/11550/the-intel-skylakex-review-core-i9-7900x-i7-7820x-and-i7-7800x-tested/6

[12] S. Manich, M. S. Wamser and G. Sigl, "Detection of probing attempts in secure ICs," 2012 IEEE International Symposium on Hardware-Oriented Security and Trust, San Francisco, CA, 2012, pp. 134-139.

[13] Q. Shi, H. Wang, N. Asadizanjani, M. M. Tehranipoor and D. Forte, "A Comprehensive Analysis on Vulnerability of Active Shields to Tilted Microprobing Attacks," 2018 Asian Hardware Oriented Security and Trust Symposium (AsianHOST), Hong Kong, 2018, pp. 98-103.