HAL
open science

Post-layout Security Evaluation Methodology Against Probing Attacks

Sofiane Takarabt, Sylvain Guilley, Youssef Souissi, Laurent Sauvage, Yves Mathieu

To cite this version:

Sofiane Takarabt, Sylvain Guilley, Youssef Souissi, Laurent Sauvage, Yves Mathieu. Post-layout Security Evaluation Methodology Against Probing Attacks. Nguyen-Son Vo; Van-Phuc Hoang; Quoc-Tuan Vien. Industrial Networks and Intelligent Systems. 7th EAI International Conference, INISCOM 2021, Hanoi, Vietnam, April 22-23, 2021, Proceedings, 379, Springer International Publishing, pp.465-482, 2021, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 978-3-030-77423-3. 10.1007/978-3-030-77424-0_37 . hal-03365004

HAL Id: hal-03365004

https://telecom-paris.hal.science/hal-03365004v1

Submitted on 11 Nov 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Post-Layout Security Evaluation Methodology Against Probing Attacks

Sofiane Takarabt[1,2], Sylvain Guilley[1,2], Youssef Souissi[1], Laurent Sauvage[2], and Yves Mathieu[2]

[1]Secure-IC S.A.S., 35 510 Cesson-Sévigné, France
[2]Télécom Paris, Institut Polytechnique de Paris, 91 120 Palaiseau, France

Abstract. Probing attack is considered to be one of the most powerful attack used to break the security and extract confidential information from an embedded system. This attack requires different bespoke equipment's and expertise. However, for the moment, there is no methodology to evaluate theoretically the security level of a design or circuit against this threat. It can be only realized by a real evaluation of a certified evaluation laboratory. For the design house, this evaluation can be expensive in term of time and money. In this paper, we introduce an innovative methodology that can be applied to evaluate the probing attack on any design at simulation level. Our method helps to extract the sensitive signals of a design, emulate different Focused Ions Beam technologies used for probing attacks, and evaluate the accessibility level of each signal. It can be used to evaluate precisely any probing attack on the target design at simulation level, hence reducing the cost and time to market of the design. This methodology can be applied for both ASIC and FPGA technology. A use-case on an AES-128 shows the efficiency of our methodology. It also helps to evaluate the efficiency of the active shield used as a countermeasure against probing attack.

Keywords: Probing attack · FIB · AES · Active shield · Exposed area.

1 Introduction

Nowadays, embedded systems are omnipresent in our daily life and contain more sensitive and confidential information. Because of this trend, many physical attacks are developed in order to break and extract sensitive information from these systems. The best known attacks are Side-Channel Attack (SCA), fault injection and probing attacks [10, 3]. The latter is the most powerful one. Using a Focused Ion Beam (FIB) [1] station allowing to access the internal signals of the device at the micro-metric or even nano-metric scale, this attack removes the measurement noise and properly retrieves the target information, such as secret keys or encrypted data. The attacker may target buses to read the memory content, or combinatorial signals to read an intermediate sensitive values. There are two major countermeasures used to protect against this type of attack (or attacker model). The first is based on masking scheme, where the attacker needs

to combine d wires to retrieve the secret [8] (known as d-probing model). The principle is to share the secret into several parts, so the attacker must probe more signals to be able to reconstruct the secret, which makes the attack more difficult. The second is based on active shield [4]. It is integrated into the chip itself on metal layers. The goal is to detect any physical intrusion by activating an alarm, when a shield wire is cut. However, this approach is a race between the precision of the FIB (or performance) and the characteristics of the used shield. The most important parameters for the latter are; the wire width and the spacing. The denser it is, the more efficient is the shield to detect intrusions.

The FIB performance depends on several parameters. From an attacker perspective, it is the resolution of the spot that is decisive. It depends on the technology of the FIB, the voltage and current limits. With the size and the shape of the spot, we can model the holes as a cone [1], and hence the ratio of the FIB. It is the ratio between the diameter and the depth of the hole. Several experiments have shown that for holes with a diameter higher than 100 nm, a ratio of 10 can be achieved. For diameters lesser than 100 nm, the ratio decreases to 1, and even at lower values [5]. This decrease is due to the fact that when the diameter is small, it becomes difficult for the extracted particles from the surface to come out, and it would be more difficult to increase the depth without increasing the diameter [5]. To enhance the ratio, Helium ion (He^+) beam can be used instead of Gallium ion beam (Ga^+) [18].

Despite the advanced technology used in the new generation of devices, probing attacks remain a serious threat, using a high resolution and a high aspect ratio FIB. To ensure an acceptable security level, a rigorous evaluation of the device is fundamental. For the moment there is no effective methods for evaluating probing attack. To be very effective, we must place ourselves within the framework of the best attacker having a very broad knowledge of the target device.

For this reason we propose an advanced methodology for evaluating a circuit at pre-silicon level, based on its post-layout description and by combining SCA primitives and geometric notions to deal with the circuit layout. This is validated on a real use-case involving an Advanced Encryption Standard (AES) IP protected with an active shield. In the following we presents in detail our approach, and contributions.

1.1 Contribution

In this paper, we give an end-to-end methodology to evaluate a circuit against front-side FIB probing attacks. Based on a full pre-silicon model of the circuit, we give an automated evaluation of sensitive signal identification, location and complexity access given a FIB configuration. Our main contributions are:

- Automatic identification of sensitive signals
- Improved method for exposed area detection [17]
- An adapted metric for evaluating the security in term of exposed area

The sensitive signal identification is based on Normalized Inter-Class Variance (NICV) SCA metric [2], that we apply to each signal individually, using the critical parameters of the implementation. Only a few knowledge of the target IP is required, which allows testing third-party IPs, since the layout file description (Library Exchange Format (LEF) and Design Exchange Format (DEF) files) are provided. For exposed area search, our approach is fully bottom-up and supports angled holes (which is not supported in [17]). It delimits the attack zones according to the presence of wires at each metal layer, thus it makes possible to track all the possible attack paths, and to determine the contribution of the shield on a given implementation. Besides, no interaction is needed with the routing tool and it is fully autonomous. This allows a quick evaluation of custom countermeasures without re-running the whole routing process. We demonstrate our approach on a real implementation of an AES protected with one shield, and we evaluate the different ways that may improve the security of the device.

1.2 Outline

The paper is organized as follows. In section 2, we start by giving some related and previous work about probing model and probing attack. In section 3, we describe the different step of our methodology about sensitive signal identification, location and evaluation against probing attacks. In section 4, we give some results on protected implementation using a shield, and we discuss how the security can be improved by inserting new (virtual) shield.

2 Related work

2.1 Probing model

In probing model, the attacker is allowed to probe d signals [8]. It is said to be secure at order d if no information about the secret can be learned up to d probes. If we consider a powerful attacker who can record a given signal of the circuit, the number of needed measurements to recover the key depends on the function that computes this value [6].

For example, if we probe the value of the *AddRoundKey* output, we can recover only one bit of the secret key. The attacker needs to probe each bit to recover the whole key (which is very complex and time consuming). The best way to minimize the number of measurements is to probe a non-linear function [6]. In the case of AES or Data Encryption Standard (DES), we probe the Substitution Box (S-Box) output (or the input if we target the last round) [15].

2.2 FIB for probing attack

To achieve a real probing attack, a FIB workstation is required. The attacker need to follow three main steps:

- Reverse engineering: The goal is to reconstruct the target circuit or gain knowledge about the structure of the design. Thus, identify the vulnerable signals or area for probing attacks [11]. It is based on a chemical process to properly decapsulate the chip, and a microscope imaging to reconstruct each layer. This process is performed on a sacrificial chip.
- Probing pad creating: When the design is reversed, the attacker creates connections with the sensitive signals on the target chip, located thanks to the previous step.
- Extract secret: The attacker record the value of the sensitive signals and compare with an hypothetical value involving the secret data [21].

The complexity of the probing attack depends on many parameters. Mainly, the step of reverse engineering is the most complex one. The attacker should identify each block and the vulnerable signals of the implementation [19]. This process is highly dependent on the performance of the workstation. The performance of a FIB is determined by the following parameters:

- Ion Beam: It depends on the voltage V, the current I and the aperture of the Ion column. The voltage varies generally from hundreds to few thousands volts (1 kV to 30 kV), and the current varies from few pico to few nano amperes (1 pA to 50 nA).
- Electron Beam: used for imaging.

Those two parameters determine the resolution and the performance of the FIB station [18, 22]. For example at 30 kV and 1 pA, the resolution of the ion beam, or the spot size may reach 7 nm. The distribution of the ions follow a Gaussian Probability Density Function (PDF) [9]. It is the main factor involved in the milling process to access sensitive signals [12]. In [1], the authors gives mathematical model for the ion beam profile and different equations to estimate the diameter, the depth and the dwell time. It is also important to mention that the smaller the diameter, the lower the sputtering yield. This can be explained by the fact that among the sputtered particles, some are redeposited on the substrate, which leads to a lower hole ratio [23].

The ling step can be enhanced to achieve higher aspect ratio as presented in [13], by activating the Electron Beam (EB) to reduce the Coulomb interaction, and fix to a very low current for ions. In [7], the authors show a different technique to achieve high aspect ratio and sub-micro diameter holes. By fixing the dwell time to 0.1 ms and the current at 48 pA they achieved an absolute depth of 1.8 μm with a relative diameter less than 300 nm, which gives a ratio of six ($R_{FIB} = \frac{depth}{diameter} = 6$).

In [17, 20], the authors described a methodology allowing to analyze a hardware implementation protected by an active shield against probing attack. They showed on a protected implementation with an active shield, the optimal ratio necessary to bypass the shield, or conversely, deduce the ratio for which the shield remains effective.

3 Methodology of FIB for probing

As described in the previous section, FIB probing is an advanced, complex and extremely expensive attack. Therefore, there are just few entities that can realize a FIB testing on their circuits. For this reason, we propose a new methodology to simulate the FIB attack at an early stage of the design life cycle. With this methodology, the designer can simulate and correct all vulnerabilities that can be exploited by the attacker using a FIB. The new methodology is composed of the following steps that we detail in the sequel:

1. Sensitive signals identification
2. Sensitive signals location
3. Exposed signals

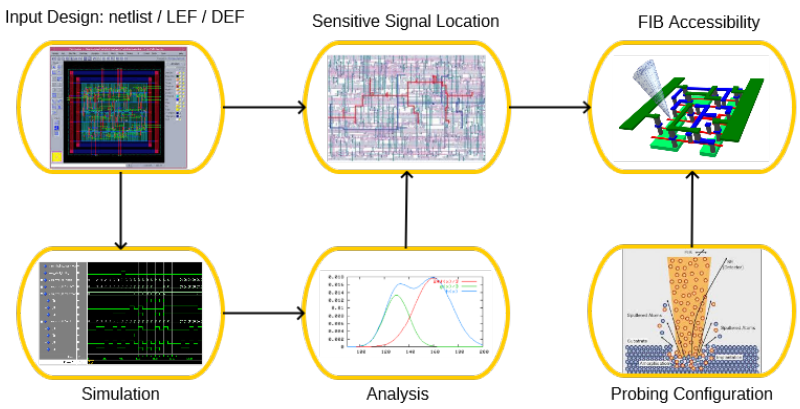


Fig. 1: Global workflow for probing evaluation threats

The global workflow of our approach is presented in fig. 1. In term of FIB attack, we can address three main types; by-passe attack, re-routing attack and disable shield attack.

When an implementation is protected by a shield, the easiest way for an attacker is to avoid cutting its wires, which is the first attack (by-passe attack). The last two attacks require more effort on the attacker side. They require more investigation for the reverse engineering step, and the routing of certain wires. This increase the attack time and its complexity. In the following, we address only the by-passe attack, which do not require editing the circuit.

3.1 Sensitive signals identification

The FIB allows probing and monitoring the internal signals of the circuit during its operation. With the retrieved data, the attacker can recover the sensitive

information hidden inside the circuit. The question is which signal the attacker needs to probe. In a complex circuit, with thousands of internal signals, he can not probe them all. For this purpose, the first step of our methodology consists in creating a method to select a group of sensitive signals that could be interesting for a FIB attack. The workflow of our method is the following:

- Tag the critical parameters
- Create the testbench
- Launch the logic simulation
- Create the simulated traces
- Analysis

The first step of our method consist in tagging the critical parameters. In this step, the designer needs to define all critical parameters that he want to protect against the FIB attack. For example, they could be the value of the secret key, plaintext or masks of cryptographic IPs.

Once the critical parameters are selected, they will be used as the input for the second step: Creating the appropriated testbench. In this testbench, we will create a test process which varies these values. It will be used to evaluate the propagation of these values into the design.

The third steps consists in launching the simulation of the new testbench using a digital simulator. During the simulation, all internal signals states are stored and used for the evaluation. In the fourth step, we use the simulation results to generate the activities traces of each signal. Once the simulated traces of each signal are generated, we can launch the last step; analysis. For this purpose, we use the NICV as a metric for the evaluation. This metric allows detecting the dependency of each simulated signal with the sensitive parameters which are defined above by the designer. The NICV is given by:

$$NICV(X,Y) = \frac{\mathbb{V}[Y|X]}{\mathbb{V}[Y]} \tag{1}$$

This metric is applied for each internal signal and each sensitive parameter. At the end, we will obtain the NICV coefficient of each signal for each time sample. Then, we can apply a threshold to select the signals where the NICV is greater than this selected threshold. It means that these signals are correlated with the sensitive values that the designer wants to protect. Hence, by probing these signals, an attacker can retrieve these sensitive values. At the end, a list of sensitive signals for each sensitive value is obtained .

3.2 Sensitive signal location

Once the sensitive signals are identified, we need to know if these signals are accessible. First, we need to identify the physical location of these signals in the layout. It is done using a layout parser. This parser is able to analyze all kind of layout (ASIC or FPGA design) and extract the location of each physical segment of the signals. It will allow identifying how many segment a specific signal (or

net) has, on which metal they are located and their corresponding coordinates. The procedure of this parser is the following:

1. Take the layout file as input
2. Find the information related to the technology (number of metal layers, wires width, Vias etc.)
3. Parse the name of all wires used by the devices (including the power wires Vdd and Gnd)
4. For each wire, retrieve the following information:
   - The different segments
   - The metal layer related to each segment
   - Different Vias of the layer
   - The metal layers related to each Via

At the end of the parsing step, we get the whole information of each wire. All these information will be stored in a database. Then, a customized program is used to select the desired signal and show all these information. Note that, this parser can be applied for both ASIC and FPGA layouts. It gives the information of both sensitive and non-sensitive wires (signals). The information of non-sensitive wires is also important. It will help us to determine the real sensitive areas for probing attack. More details about the sensitive areas will be presented in the next section.

3.3 FIB probing model

A FIB is composed of different components that allow scanning and milling specimens. An electronic microscopy is used to scan the surface of the sample, and an ion beam for milling and lamellae preparation. In the case of milling, a flow of ions are emitted with specific current **I** $(5nA; 30nA)$), accelerated at a specific voltage U $(5kV; 30kV)$, and focused into a point of the sample. The ions hit the surface of the target and weakens the focused zone and tear atoms from the sample. The depth and the diameter of the left hole depends on the Dwell time (fixed time at single point), the beam current and the voltage. Another factor which depends on the sputtered yield is the incidence angle to the surface. Experiments shows that the maximum yield is reached when the angle is between 65° and 85°. The spot size of the beam is obviously the most important parameters which defines the FIB resolution. The best knows resolution is about 5 nm [18].

The purpose of probing attack is to be able to access to some sensitive signals of the circuits. To access these signals, we need to identify an appropriate area, that optimizes the milling step. This can be defined as the dimension of the cone that we must make to achieve that, and decide if a such cone is feasible with a given FIB.

3.4 FIB access methodology

In the circuit layout, we have different layers that contains the targeted signal. For a given signal at position $X = (x, y, z)$ (or a list of positions of wires), we try to access this signal without damaging the circuit (or with minimal damage). We describe our method applied to a wire, which can be seen as a list of positions at different layers. The principle idea of this method is a bottom-up process, which is based on two principle steps:

- Projection: The wire will be projected recursively to the layers above.
- Delimitation: This step consists in eliminating the region that is crossed with other wires, or select the one that has the less number of wires (minimal damage).

We start from the wire position, and give the surface from where it can be accessed. Note that in this method, we assume that all wires have either 0° or 90° with respect to the X axis.

Algorithm 1: Projection and delimitation process

```
Input: Design: (LEF, DEF files) , Signal target: S
Output: Accessibility paths
1  Segments ← shape(S)
2  for segment ∈ Segments do                    // For each segment in Segments
3      current_layer ← get_layer_index(segment)
4      layer_above ← current_layer + 1
5      height ← Design.get_distance_between_layers(current_layer, layer_above)
6      rectangle ← first_projection(segment, height)                // Projection
7      wires_at_layer_above ← Design.get_wires_at_layer(layer_above)
8      sub_rectangles = rectangles.split(wires_at_layer_above)
        // Delimitation
9      new_sub_rectangles = empty_list()
10     for r ∈ sub_rectangles do
11         current_layer ← layer_above
12         layer_above ← current_layer + 1
13         height ←
             Design.get_distance_between_layers(current_layer, layer_above)
14         r.update_projection_angles(segment)
15         r.project_up(height)                                         // Projection
16         wires_at_layer_above ← Design.get_wires_at_layer(layer_above)
             new_sub_rectangles.add(r.split(wires_at_layer_above))
17     sub_rectangles = new_sub_rectangles
18     while layer_above < top_layer do
19         goto step 9
20 return sub_rectangles
```

In algorithm 1, we give the projection and delimitation steps that give us the list of all surfaces allowing to access any sensitive wire.

Projection A wire can be seen as a list of positions in a given layer. Here, we describe the whole process for one segment of the wire (for the whole wire, we apply the same method for each segment). The normal projection of the wire gives its image at the top layer, and by varying the projection angle θ from $[0, \theta_{max}]$ along x and y axes from the normal angle, we get a rectangle image which represents the surface from where the targeted wire can be reached from the layer above. If the segment is determined by two positions (x_0, y_0) and (x_0, y_1) (here we suppose that is vertical), then the boundaries of the rectangle can be computed as follows:

$$r = z \times \tan(\theta_{max})$$
$$R = \{(x_0 - r, y_0 - r), (x_0 - r, y_0 + r), (x_0 + r, y_1 + r), (x_0 + r, y_1 + r)\}$$

where z is the distance between metal layers. It depends on the level of the metal layer and the used technology.

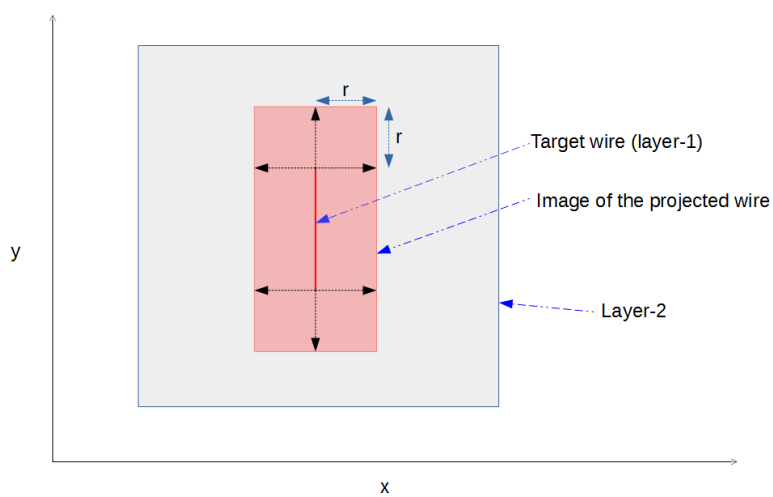


Fig. 2: First projection of a sensitive wire to the top layer.

The whole area allows accessing the target wire by different angled holes. Figure 2 shows the projection phase of a wire located at layer $M1$. The image of the projection gives a rectangle at layer $M2$. We consider that, from any point from this rectangle, the sensitive signal can be accessed by the FIB.

The rectangle may be crossed with some signals located at layer $M2$. Thus, it should be divided into smaller sub-rectangles. This is the second step of our method, and will be detailed in the next section.

Delimitation The purpose of the delimitation step is to check if the projected rectangle is crossed by some wires in the layer above. For each wire, we need to split and delimit the area to form other sub-rectangles, thus we obtain a new list of independent areas. Once the delimitation is done as illustrated in fig. 2, and the list of rectangles are determined, we can project them again to the layer above, and so on, to reach the surface of the layout. In this step, we can eliminate the region where the diameter of the hole exceeds the size of the area (we cannot mill through this area without completely cutting a wire).

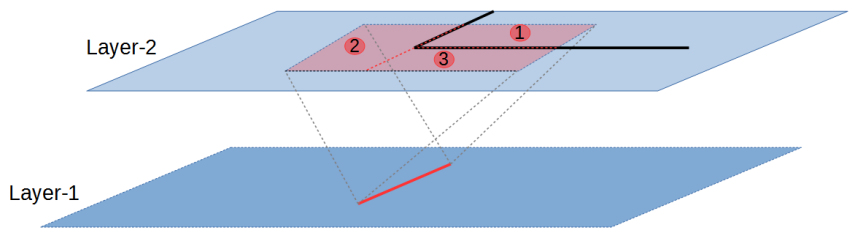


Fig. 3: The projected area is crossed by one wire. It will be divided into small rectangles.

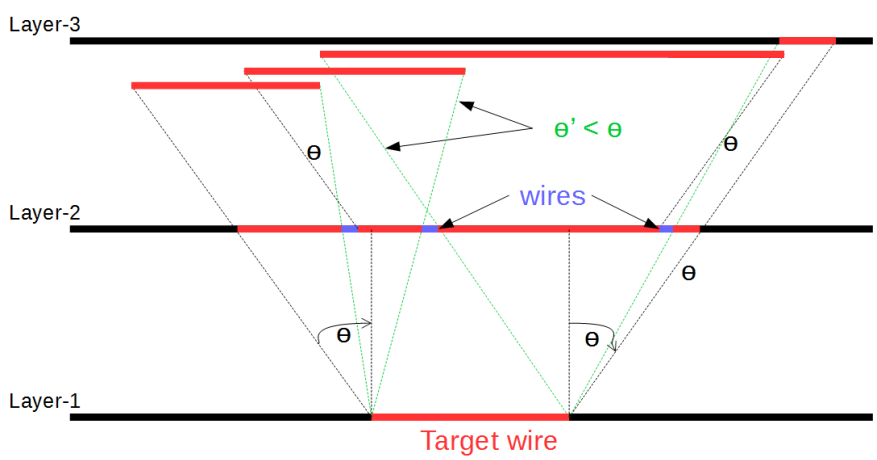


Fig. 4: Cross-section of projected sensitive wire to the top layers: The projection angle θ is adapted following each situation.

The projection angle has to be determined by the limits of the targeted wire, and the maximum realisable angle. We illustrate in fig. 4 the process of the pro-

jection of each area. Each rectangle becomes independent, and the accessibility of the signal should be determined by the projection path. In fact, many rectangles can be projected to some surface to make a bigger area, but this should not be considered as a contiguous one. The angles of projection for each sub-rectangle should take into a account its location. The angles of projection also depend on their location. For each rectangle, this angle is determined by either its maximal value ($\theta_{max} = \theta^*$), or the extremities of the targeted wire and the rectangle location, as illustrated in fig. 4 in green. Therefore, each area has its own projection angle computed after its creation.

FIB model Once the phase of projection and delimitation are done, one needs to see how much is difficult to access the sensitive wire. This basically depends on two parameters; the surface of the access path and the performance of the FIB. Obviously, the larger the surface is, the easier the access is. So as a priority, we will sort all the available access paths according to their surfaces. It allows us to find the optimal set-up to access the sensitive wire. Once this phase is completed, we can estimate the setting of the FIB as well as the complexity of milling (or milling time).

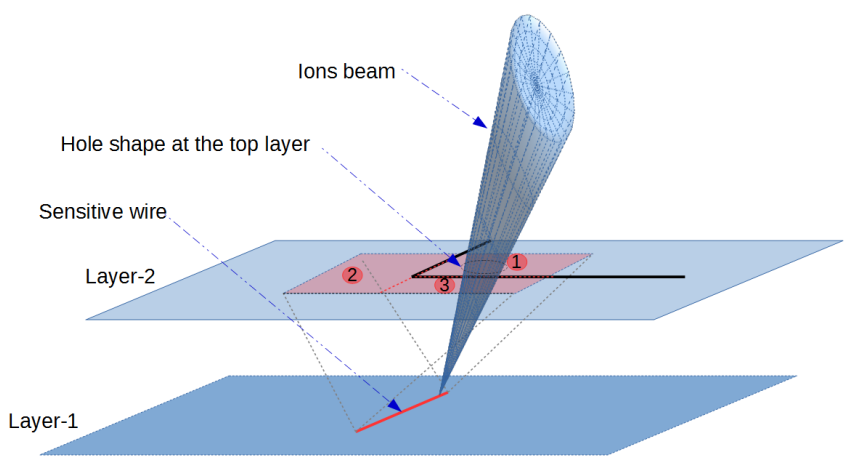


Fig. 5: Illustration of the FIB model for milling.

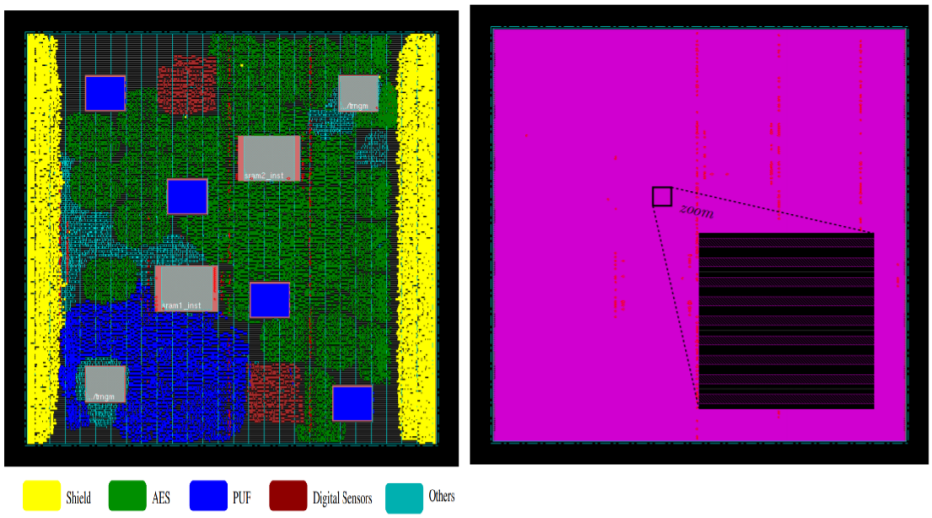
Depending on the best found surface, we can determine the shape and the volume of the optimal cone that allows to access the sensitive wire, and thus fix the voltage and the current of the ions beam. With those information we can estimate the time needed to make the hole.

4 Study-case on AES

To demonstrate the reliability of our methodology on a concrete case. We apply our method to evaluate an ASIC circuit, implementing an AES protected with an active shield.

4.1 Target IP

The circuit is composed of different IPs including AES, a Physical Unclonable Function (PUF), Digital sensors and also an active shield used to protect the circuit against probing attacks.



(a) (b)

Fig. 6: Circuit used for the evaluation: (a) Logic part of different IPs, (b) Shield mesh located at top-most metal layer [4].

An overview of this design is presented in fig. 6. As explained in [14], it is composed of 8 IPs, particularly, an active shield, an AES, a PUF and two digital sensors. The active shield (described in [4]) is composed of three parts:

- ALICE (transmitter), which embeds a SIMON block cipher to generate 128 random bits.
- BOB (receiver), which also embeds a SIMON block cipher.
- Shield mesh (Figure 6 (b), which is composed of n lines on the last metal layer. It is used as a communication channel between ALICE and BOB, and achieves the anti-tamper protection of the integrated circuit located below it, with a 128 bits comparator.

This design uses the CMOS 65 nm technology from STMicroelectronics. The core size is 560 $\mu m \times 560$ μm. The shield mesh is composed of 640 parallel lines with 0.4 μm width and 0.4 μm spacing.

4.2 Sensitive signal location

To identify the sensitive signals, we run a leakage detection analysis with the NICV as described in section 3.1, using the intermediate value computed by the S-Box. There are 9448 signals (wires) at all in the AES block (without counting logic gates). After the analysis, we have only 256 sensitive signals, which correspond to the output of the S-Box, and the input of *MixColumns*, as detailed in table 1. The result of parsing is shown in fig. 7, where the signals around the circuit are plotted with the right positions from the DEF file.

Table 1: Result of parsing and sensitive signal identification.

Block	#Signals	#Sensitive signals
AES	9448	256
S-Box	6511	128
MixColumns	268	128

It is therefore those signals that are vulnerable against a probing attack. We note that the *ShiftRow* block is not present in the design, as it is just a wiring of the S-Box output into the input of *MixColumns*.

4.3 FIB-probing evaluation

We have selected the output of the S-Box. This signal is routed over layers $M3$, $M4$ and $M5$. To compare the FIB attack with an implementation without shield, we consider only the metals at levels lower than 6. For the performance of the FIB, we have fixed the ratio to 5 ($R_{FIB} = 5$). The criticality of a probing attack can be measured by the number of exposed areas, their surfaces and the angle to the target wire. The larger the angle is (compared to the normal angle), the greater the relative hole depth becomes. Thus, more time will be needed to complete the hole.

To heuristically estimate the difficulty of the FIB attack, we have defined a metric taking the different parameters into account, namely the surface of each exposed area and its relative depth. The bigger the area is, the easier the attack is. Moreover, the bigger the angle (or the depth) is, the more the attack is difficult. Hence, this heuristic I can be calculated as follows:

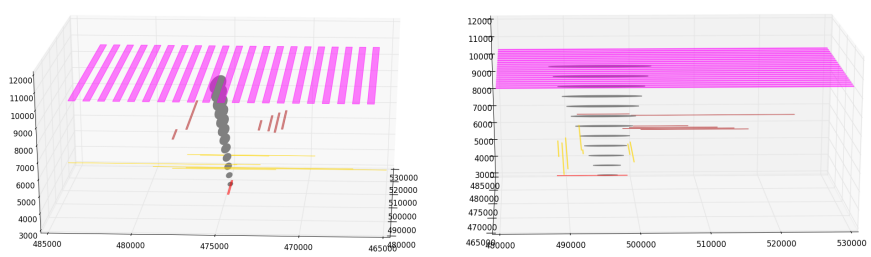
$$\begin{aligned} I_i &= \frac{R_i}{D_i} \\ I &= max_{I_i}\{I_i\} \end{aligned} \tag{2}$$

where R_i are the exposed rectangles surfaces, and D_i is the relative depth from R_i to the sensitive signal. This latter is computed from the center of the rectangle. The larger I is, the easier the probing attack is.

Table 2: Results for different angles. For each angle we show the number of exposed areas and the value of I (μm) (eq. (2)).

Implementation \ θ_{max}	$\frac{\pi}{3}$	$\frac{\pi}{4}$	$\frac{\pi}{6}$
w/t shield	143 (23.784)	39 (21.632)	16 (13.543)
w shield (M7)	525 (2.101)	142 (1.643)	61 (1.635)

We reported in table 2, the number of exposed area for different realisable angles. These angles can be chosen by the evaluator relatively to the capacity of the FIB station. The targeted segment of the sensitive signal is the one at level $M3$. We can see that the number of exposed areas is higher at $M7$, because each exposed area at $M6$ will further be divided at $M7$ according to the shield wires, but the surfaces are smaller. The indicator I is significantly lower when considering $M7$ (as expected). This shows that the attack becomes difficult at $M7$, but still feasible with the chosen ratio in this case ($R_{FIB} = 5$). The exposed areas that do not verify the FIB ratio are ignored. Furthermore, for bigger angles the indicator is bigger, because more susceptible (larger) areas can be found, with a relative low depth.



(a) Front side sagittal section.

(b) Left side sagittal section

Fig. 7: Best area to mill. The sensitive signal is presented at layer $M3$. The path of the hole is presented as small (gray) ellipses.

For a signal taking the output of the S-Box, we illustrate in fig. 7 the best exposed area for the attacker to mill. Interestingly, at this position, there is no much signals at layer $M6$. This allows us to get larger exposed areas when running algo-

rithm 1. As we can see, the hole could have an ellipsis shape ($0.800\mu m \times 12.8\mu m$). As there is no wire at layer $M6$, the hole can be extended further (if needed) along the shield wire direction and thus, allow making a deeper hole. As we can see in this evaluation, the shield did not provide significant protection. We note an improvement in the difficulty of the attack in the case where no shield is added, but the attack remains feasible and it is only the depth of the hole which increases, without making its realization impossible with the chosen ratio.

4.4 Security improvements

To see possible improvements, we can imagine adding a second layer of shield ($M8$). We considers two ways for that:

1. A second parallel shield, but with an *offset* relatively to $M7$.
2. A second *orthogonal* shield with respect to $M7$.

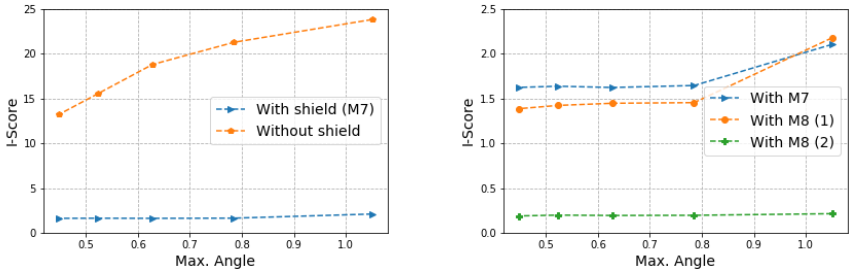
We then calculate the score I to find the best area in both cases. We find that in case (1), there is a very negligible (or even no) improvement. We always get rectangles with a very large length, around $15.8\mu m$ and a width of 0.800 μm. The latter is limited by the characteristics of the shield (wire width and spacing). The second solution offers more protections. Surfaces with a very large width at $M7$ level are forced to be divided when projected to $M8$. All holes that can be milled from $M8$ must be restricted to a diameter less than 800 μm at $M7$. By limiting the diameter, the depth that could be reached is restricted.

Table 3: Evaluation with a second shield $M8$. For each angle we show the value of $I(\mu m)$ (eq. (2)).

M8 \ θ_{max}	$\frac{\pi}{3}$	$\frac{\pi}{4}$	$\frac{\pi}{6}$
Parallel with offset (1)	2.174	1.452	1.421
Orthogonal (2)	0.214	0.196	0.198

As expected, we can deduce from the value reported in table 3, that a second shield with an orthogonal orientation relatively to $M7$ is more efficient. Besides, with the same chosen ratio ($R_{FIB} = 5$), the signal shown in fig. 7 cannot be accessed. As the highest diameter that we can achieve at layer $M7$ is less than 0.8 μm, the ratio of the FIB should be higher than 9 to be able to access that signal.

In fig. 8, we show the improvement of the security level estimated by eq.(2) when there is no shield, after the insertion of two parallel shields and then, after the insertion of two orthogonal shields. The results show that the security level increases more significantly with two orthogonal shields.



(a) With and without shield. (b) With parallel and orthogonal shields.

Fig. 8: I score with different shield configurations.

With this procedure, we can determine the available ways to secure a given implementation against probing attacks. For example, manual re-routing of excessively exposed signals to lower levels makes these attacks more difficult as demonstrated in the last test, but still, we can also move other signals (not necessarily sensitive ones) in empty areas above the sensitive signals, which force the size of the exposed areas to be reduced.

5 Conclusion

In this paper we have presented an end-to-end methodology, allowing to evaluate a hardware implementation against a probing attack. The selection of sensitive signals is performed automatically, with minimal configuration (random or fixed input). We have shown an example of an attack on an implementation protected by an active shield, considering the parameters of a typical FIB. This later can be adapted to model a more powerful attacker, being able to make smaller holes at higher depth as shown in the state-of-the-art with different techniques. By analyzing the possible angles of attack identified exhaustively, the designer can choose to modify the routing in the most optimal way according to the performance of a given FIB, such as re-routing over lower metal layers, moving some signals to empty areas, or inserting a second layer of shield. Besides, our framework is autonomous, and no interaction is required with the routing tool, thus he designer can test some countermeasures and re-routing without launching the full routing process, and estimate the security gain more in advance.

Acknowledgments

This work has been funded in part by the bilateral French-German “APRIORI” project (MESRI-BMBF call). The tool presented in this paper is implemented in Secure-IC Virtualyzr product [16]. Virtualyzr is an electronic design automation (EDA) software tool dedicated to pre-silicon security evaluation.

Bibliography

[1] Mohammad Yeakub Ali, Wayne Hung, and Fu Yongqi. A review of focused ion beam sputtering. *International journal of precision engineering and manufacturing*, 11(1):157–170, 2010.

[2] Shivam Bhasin, Jean-Luc Danger, Sylvain Guilley, and Zakaria Najm. Nicv: normalized inter-class variance for detection of side-channel leakage. In *Electromagnetic Compatibility, Tokyo (EMC'14/Tokyo), 2014 International Symposium on*, pages 310–313. IEEE, 2014.

[3] Eric Brier, Christophe Clavier, and Francis Olivier. Correlation power analysis with a leakage model. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 16–29. Springer, 2004.

[4] Jean-Michel Cioranesco, Jean-Luc Danger, Tarik Graba, Sylvain Guilley, Yves Mathieu, David Naccache, and Xuan Thuy Ngo. Cryptographically secure shields. In *2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, pages 25–31. IEEE, 2014.

[5] Yongqi Fu and Kok Ann Bryan Ngoi. Investigation of aspect ratio of hole drilling from micro to nanoscale via focused ion beam fine milling. 2005.

[6] Helena Handschuh, Pascal Paillier, and Jacques Stern. Probing attacks on tamper-resistant devices. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 303–315. Springer, 1999.

[7] Wico CL Hopman, Feridun Ay, Wenbin Hu, Vishwas J Gadgil, Laurens Kuipers, Markus Pollnau, and René M de Ridder. Focused ion beam scan routine, dwell time and dose optimizations for submicrometre period planar photonic crystal components and stamps in silicon. *Nanotechnology*, 18(19):195305, 2007.

[8] Yuval Ishai, Amit Sahai, and David Wagner. Private circuits: Securing hardware against probing attacks. In *Annual International Cryptology Conference*, pages 463–481. Springer, 2003.

[9] Fatin Syazana Jamaludin, Mohd Faizul Mohd Sabri, and Suhana Mohd Said. Controlling parameters of focused ion beam (fib) on high aspect ratio micro holes milling. *Microsystem technologies*, 19(12):1873–1888, 2013.

[10] Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings*, pages 388–397, 1999.

[11] Oliver Kömmerling and Markus G Kuhn. Design principles for tamper-resistant smartcard processors. *Smartcard*, 99:9–20, 1999.

[12] Hong-Wei Li, Dae-Joon Kang, MG Blamire, and Wilhelm TS Huck. Focused ion beam fabrication of silicon print masters. *Nanotechnology*, 14(2):220, 2003.

[13] Hu Luo, HaiLong Wang, YiMin Cui, and RongMing Wang. Focused ion beam built-up on scanning electron microscopy with increased milling pre-

cision. *Science China Physics, Mechanics and Astronomy*, 55(4):625–630, 2012.

[14] Xuan Thuy Ngo, Jean-Luc Danger, Sylvain Guilley, Tarik Graba, Yves Mathieu, Zakaria Najm, and Shivam Bhasin. Cryptographically Secure Shield for Security IPs Protection. *IEEE Trans. Computers*, 66(2):354–360, 2017.

[15] Jörn-Marc Schmidt and Chong Hee Kim. A probing attack on aes. In *International Workshop on Information Security Applications*, pages 256–265. Springer, 2008.

[16] Secure-IC. VIRTUALYZR tool (VTZ). `https://www.secure-ic.com/solutions/virtualyzr/` and `https://cadforassurance.org/tools/design-for-trust/virtualyzr/`, Accessed online on March 4th, 2021.

[17] Qihang Shi, Navid Asadizanjani, Domenic Forte, and Mark 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)*, pages 155–160. IEEE, 2016.

[18] Vadim Sidorkin, Emile van Veldhoven, Emile van der Drift, Paul Alkemade, Huub Salemink, and Diederik Maas. Sub-10-nm nanolithography with a scanning helium beam. *Journal of Vacuum Science & Technology B: Microelectronics and Nanometer Structures Processing, Measurement, and Phenomena*, 27(4):L18–L20, 2009.

[19] Sergei Skorobogatov. Physical attacks on tamper resistance: progress and lessons. In *Proc. of 2nd ARO Special Workshop on Hardware Assurance, Washington, DC*, 2011.

[20] Huanyu Wang, Qihang Shi, Domenic Forte, and Mark M Tehranipoor. Probing assessment framework and evaluation of antiprobing solutions. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 27(6):1239–1252, 2019.

[21] Lingxiao Wei, Jie Zhang, Feng Yuan, Yannan Liu, Junfeng Fan, and Qiang Xu. Vulnerability analysis for crypto devices against probing attack. In *The 20th Asia and South Pacific Design Automation Conference*, pages 827–832. IEEE, 2015.

[22] H Wu, LA Stern, D Xia, D Ferranti, B Thompson, KL Klein, CM Gonzalez, and PD Rack. Focused helium ion beam deposited low resistivity cobalt metal lines with 10 nm resolution: implications for advanced circuit editing. *Journal of Materials Science: Materials in Electronics*, 25(2):587–595, 2014.

[23] Jack Zhou and Guoliang Yang. Focused ion-beam based nanohole modeling, simulation, fabrication, and application. *Journal of manufacturing science and engineering*, 132(1), 2010.