Hidden in Plain Sight: A Detailed Investigation of Selectively Increasing Local Density to Camouflage and Robustify Against Optical Probing Attacks

Sajjad Parvin[ш], Chandan Kumar Jha[ш], Sallar Ahmadi-Pour[ш], Frank Sill Torres[‡], and Rolf Drechsler[ш,†]
[ш] Institute of Computer Science, University of Bremen, Germany
[†] Cyber-Physical Systems, DFKI GmbH, Germany
[‡] Institute for the Protection of Maritime Infrastructures, German Aerospace Center, Germany
{parvin, chajha, sallar, drechsler}@uni-bremen.de, frank.silltorres@dlr.de

***Abstract*—Modern chips have been demonstrated to be vulnerable to malicious Side-Channel Analysis (SCA) attacks that put Intellectual Property (IP) at risk. These SCA attacks and their countermeasures have been well-studied in literature. However, in recent years a non-invasive and laser-based SCA attack through the backside of chips, namely Optical Probing Attack (OPA), has emerged. OPA is effective in retrieving the chip's IP by reading out the transistors' terminal voltage. Some countermeasures to mitigate OPA have been proposed in the literature. However, these methods are too expensive to implement as they require a significant change in the fabrication process. These existing methods require a whole redesign of logic cells layout, characterization, synthesis, and place and route techniques which can be quite challenging.**

In this work, we investigate the effect of increasing the density around an important logic cell in the design, that needs to be secured against OPA. Our methodology requires only the standard cell library gates and can be easily integrated into the ASIC design flow. We found that increasing the local density of cells around an important logic cell can lead to a larger reflection. This can significantly help to camouflage the secure cell against OPA, as the reflection from the secure cell and the neighboring cells can be hard to differentiate. We show that this methodology can prove to be an effective countermeasure against OPA by performing detailed experiments of density versus reflection using nand and inverter cells. We exhaustively evaluated thousands of placement strategies with varying densities to show its efficacy against OPA.

***Keywords*—Optical Probing, Security, Local Density, Place and Route, PnR.**

I. Introduction

With the increasing use of embedded systems and the Internet of Things, security has become a crucial aspect in electronic systems. Many software-based solutions have been proposed to secure the information of electronic systems [1]. However, the software-based solutions can be easily bypassed by a malicious attacker if the hardware is not secure [2]. It has been shown in the literature, that a malicious attacker can exploit the hardware vulnerabilities using *Side-Channel Analysis* (SCA) such as differential power analysis [3], electromagnetic attacks [4], etc., to steal the *Intellectual Property* (IP) of an electronic system [2]. Moreover, laser-assisted SCA has been proposed to probe the voltages of devices in a design [5], [6].

Acknowlegment: The work described in this paper has been supported by the Deutsche Forschungsgemeinschaft (DFG – German Research Foundation) under the priority programme SPP 2253–439918011 in project DR 287/38-1.

In recent years, it has been demonstrated that laser-assisted SCA, namely *Optical Probing Attack* (OPA) can be utilized by an adversary to retrieve the information processed on a chip [7], [8].

Several countermeasures have been proposed in the literature to prevent attacks that try to retrieve information from a chip. Some of these countermeasures require a significant change in the fabrication process of chips to use novel materials and structures like nanopyramids, or coating the backside of the chip with special materials [9]–[11]. These types of modifications in the chip fabrication design can be costly, and not attractive for chip design houses and fabrication facilities. Furthermore, there exist sensor-based methods countermeasures that can detect the OPA [11], [12] on a chip with a high confidence. However, sensor based countermeasures are susceptible to be bypassed by an adversary, to then perform OPA on a chip to retrieve IP of the chip.

In addition to the aforementioned countermeasures, [13] investigated the use various logic styles and layout designs to decrease the possibility of probing a region of the design in order to hinder an adversary from probing the IP. A change in the layout design and logic style of a design introduces an inherent, and cost effective security measures to design a secure circuit which comply with the use of conventional CMOS technology process design kit. However, a change in the logic styles, or layout design, requires a great amount of effort. This means that design engineers need to redesign the gate library from scratch (layout design, and characterization). In addition, there might be a case that designers might require to come up with an optimized synthesis technique for that specific secure gate library, i.e. differential gate library [13].

In this work, we investigated the effect of a change in the local density around a logic cell that must be secured against OPA. We show how a design-house can utilize our approach while using standard CMOS gate library and constraint the place and route tool, in order to increase the density around a target cell that process important information. Thus, increasing the light interference caused by surrounding gates to camouflage the target cell's light reflection. In this work, we present an extensive investigation on the effect of light reflection of a design under optical probing when varying the local density around the targeted cell. The contribution of this work can be summarized as follows:

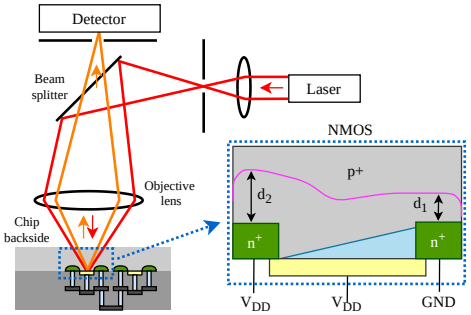
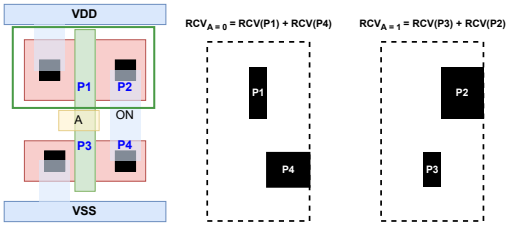


Fig. 1: Illustration of an optical probing setup when the laser is focused on an NMOS biased in saturation region.



(a) (b) (c)

Fig. 2: (a) standard CMOS INV logic cell's layout, INV logic cell layout's geometry contributing to the reflection of light when the applied input is (b) logic "0", (c) logic "1".

- We present a detailed study of the effect of local density to make the design more robust against OPA.
- We investigate the effects of protecting the targeted cell by surrounding them using inverters and NAND cells.
- We propose a methodology to incorporate the findings into the design flow to robustify our designs against OPA.

II. Contactless Optical Probing

In this section, we explain the necessary background and formulation for *Optical Probing* (OP) to be used for the rest of the paper.

A. Methodology and Setup

OP capabilities are usually embedded into a *Laser Scanning Microscopes* (LSMs), in which a focused laser beam is scanned using galvanometric mirrors or statically pointed at a single point on a chip. At the same time, a detector collects the reflected light. Since silicon is transparent to light in the *Near-InfraRed* (NIR) spectrum, probing an *Integrated Circuit* (IC) through its backside is possible without thinning or preparation of the chip. As shown in Fig. 1, the laser light focused on a region of the die area of the IC passes the bulk silicon and travels through the active areas of transistors. A portion of the incident light is reflected (e.g. when the incident light hits the first metal layer). It then travels back through the silicon into the microscope lens. Afterward, the beam splitter directs the reflected light to an optical detector, which converts its intensity into voltage.

B. Optical Probing for Data Extraction

As voltage differences applied to a transistor can be detected using OP, data stored or processed on an IC can be extracted as well. The probing technique where the laser is parked at a certain location of the chip is called *Electro-Optical Probing* (EOP)[1]. Using EOP, sensitive data processed by the IC can be extracted [7], [8]. Due to having a weak modulation of the reflected optical beam, the chip needs to be run in a loop, and the captured signal needs to be integrated to achieve a decent *Signal-to-Noise Ratio* (SNR).

[1]In the case of using a coherent light source, EOP is typically called *Laser Voltage Probing* (LVP), and EOFM is called *Laser Voltage Imaging* (LVI).

In order to localize the paths carrying periodic signals on the chip, the laser can be scanned over the chip while feeding the detector's output into a narrow-width bandpass filter set to the frequency of interest. Consequently, a gray-scale encoded image of the scanned area is obtained where bright spots indicate areas with switching activity. This technique is called *Electro-Optical Frequency Mapping* (EOFM)[1]. By injecting a periodic pattern into the data processed by the device, all potential locations on the chip that may carry data of interest can be identified using EOFM and later probed using EOP [7], [8], [14].

Since the device has to be operated in a loop for this approach, single-trace measurements, i.e., where the data of interest is only present once on the chip, are impossible. An extension to EOFM, called *Laser Logic State Imaging* (LLSI), allows such single-trace measurements by modulating the power supply of the device during operation and conducting EOFM. In this way, the charge carrier density of transistors is modulated, and transistors in the on- and off-states can be distinguished. Therefore, LLSI allows the extraction of data from on-chip memories, such as flip-flops and SRAM cells [15], [16] and the detection of malicious modifications on FPGAs [17].

C. Optical Resolution and Technology Size

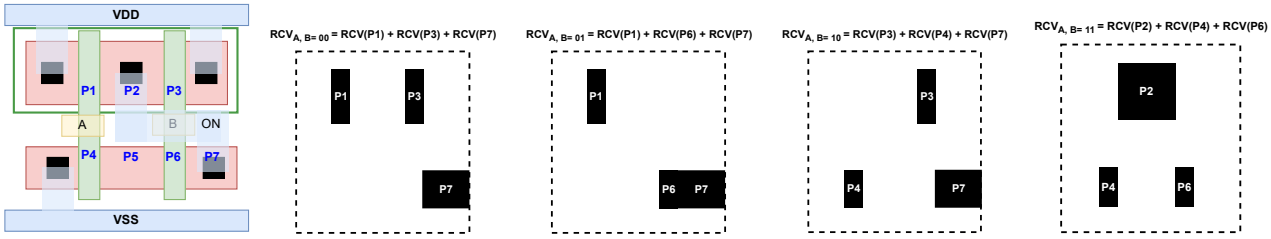
Even though there are different ways to define the spatial resolution R of optical probing, the most common definition is defined in the form of Fourier optics and Abbe's criterion [18] as $R = 0.5\lambda/NA$ where λ is the wavelength of the light and NA is the *Numerical Aperture* of the microscope system. The parameter R can be understood as the minimum distance between resolvable two-point sources [18]. The intensity of the laser spot can be described as Gaussian distribution [18] with

$$p(r) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{\frac{-(r)^2}{2\sigma^2}} \quad (1)$$

where r is the distance from the center of the beam and σ is the standard deviation which can be calculated as $\sigma = 0.37\lambda/NA$ for a confocal microscope [18].

D. Reflection Caliber Value *(RCV)*

In [13], a simple-to-use model is proposed for the reflection of a transistor under OP. This model, called RCV,



(a) (b) (c) (d) (e)

Fig. 3: (a) standard CMOS NAND2 logic cell's layout, NAND2 logic cell layout's geometrical modeling when the applied input is (b) logic "00", (c) logic "01", (d) logic "10", (e) logic "11"

approximates the reflected light from a transistor's active region as a linear function of the applied voltage to the transistor's terminals (V), amplification constant of transistor K ($K_{PMOS} = 1.3K_{NMOS}$), transistor's fabrication related parameter (β), the power of incident laser light (P_L), and the area of transistor's active region. The RCV value can be expressed as follow:

$$RCV = V \times K \times \beta \times P_L \int_0^{2\pi} \int_0^{r_{spot}} p(r) \times A(r,\theta)\, dr d\theta, \quad (2)$$

where $p(r)$ and $A(r,\theta)$ are the laser's power Gaussian distribution and the area of the active region under the laser spot in polar coordinates, respectively. Furthermore, (2) can be expanded to be applicable for a *Field Effect Transistor* (FET) which has Drain (D), Gate (G), and Source (S) regions. The RCV of a single transistor is the sum of all the active regions of a transistor (R) light under OP, which is shown below:

$$RCV_{FET} = \sum_{\forall R \in FET\{D,S,G\}} RCV_R. \quad (3)$$

Since, in real designs, we have standard logic gates, we can expand the RCV equation furthermore to simulate probing a logic gate cell. The RCV of a logic gate cell is the sum of RCV_{FET} for all the transistors (t) in a logic gate cell. RCV_{Cell} is represented as follows:

$$RCV_{Cell} = \sum_{\forall t \in Cell} RCV_{FET_t}. \quad (4)$$

III. Methodology

In this section, we discuss the approach utilized to study the effectiveness of selectively increasing local density to robustify against optical probing attacks. Increasing the density around secure cells can lead to increased interference from the reflections of the light sensed by the OPA frameworks. Hence, this will help to camouflage the secure cell and greatly hinder the process of identifying information in relation to the secure cells. In order to achieve this, we developed a methodology to study the effects of density against OPA.

The standard cell library consists of a number of gates and it is impractical to exhaustively evaluate all possible combinations of the gates. Hence, we investigate the subset of universal gates namely nand (NAND) and inverter (INV) for evaluation in this work. Our method can easily be extended and is also applicable to any other gates in the standard cell library. We investigated three different case studies to evaluate and assess our methodology.

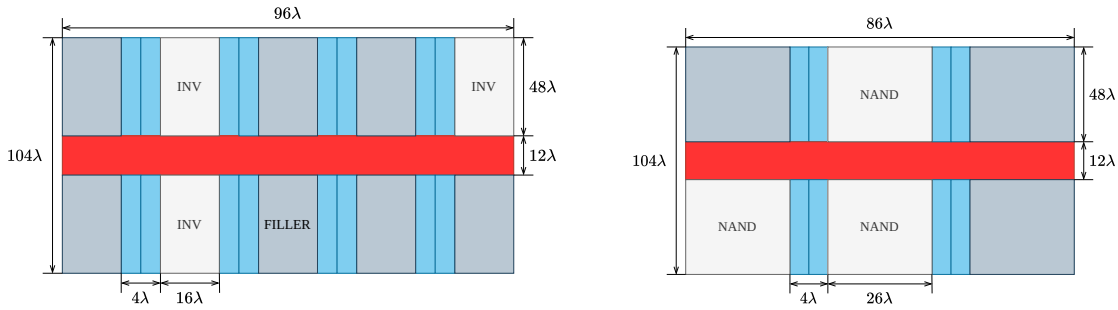
- INV: This captures the case when the secure cell is an inverter (simple gate) and the camouflage is also done using inverters (simple gate).
- NAND: This captures the case where the secure cell is a nand (complex gate) and the camouflage is also done using nand (complex gate).
- A combination of INV and NAND: This captures three scenarios. First, the case where the secure cell is simple and is camouflaged by complex gates. Second, the case where the secure cell is complex and is camouflaged by the complex gate. Lastly, it also captures the combination of both.

A. Generating Geometrical Model

According to Section II, the laser light is modulated due to the presence of an electrical field. To perform OP in simulation, we need to model the region of each transistor in the design that has a voltage difference at its terminal with respect to the transistor's bulk voltage ($|\Delta V| > 0$). For each modeled active region of the transistor, we assign a respective RCV value to it, as shown in equation 2. To elaborate the geometrical modeling of logic cells to perform OP in simulation, consider the INV logic cell shown in Fig. 2 (a). Upon applying different values to the input of the INV logic cell, a different region of the logic cell has $|\Delta V| > 0$. For an INV logic cell, we have 4 different regions, namely, P1 to P4. When the logic value "0" is applied to the INV logic cell's input, regions P1 and P4 have $|\Delta V| > 0$, as shown in Fig. 2 (b). In the case of applying logic "1" to the input of INV logic cell, then the region P2 and P3 will have $|\Delta V| > 0$, as shown in Fig. 2 (c). Similarly we generated the same geometrical modeling for the NAND cell for the four possible input combinations. Geometrical modeling for a NAND2 cell when the applied input are "AB = 00", "AB = 01", "AB = 10", "AB = 11" are shown in Fig. 3 (a), Fig. 3 (b), Fig. 3 (c), and Fig. 3 (d), respectively.

B. Generating Placement and Input Stimulus

To study the impact of the density using INV and NAND cells as camouflage cells, we created a floor plan. The floor



(a) (b)

Fig. 4: Floorplan and Placement (a) INV Cells, (b) NAND cells

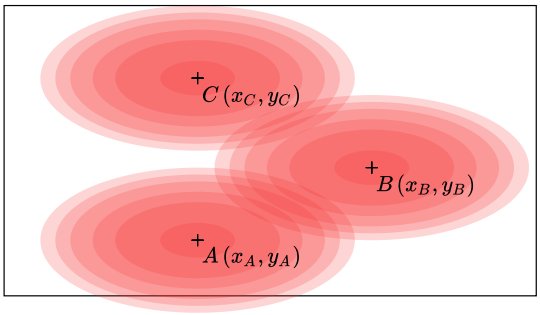


Fig. 5: Three different Laser Positions (not to scale)

plan can be used to place 10 INV cells and 6 NAND cells as shown in Fig. 4a and Fig. 4b respectively. We divided the floor plans into different number of cells to keep the areas similar for both experiments.

1) INV Cells: Every location in the floor plan can be filled with one of three possible cells: i) It can be filled with an INV when the applied input is logic state "1", or ii) when the applied input is logic state "0", or iii) filler cell. The filler cell does not contribute to the reflection. Hence, the higher the number of filler cells lesser is the density, and vice versa. There are 10 possible locations and each location has three possible options as shown. Thus, we have $3^{10} = 59,049$ possible combinations of different placements. This exhaustively covers all the input patterns and filler combinations. We generated the geometric models for all the possible placements and then grouped them according to their density. For example, the designs which have no filler cells have 100% density and the designs that have one filler cell have 90% density. Hence, we have placements from 10% density to 100% density in steps of 10%.

2) NAND Cells: Every location in the floor plan can be filled with either of five possible cells: i) It can be filled with a NAND when the applied input is logic state "00", ii) when the applied input is logic state "01", iii) when the applied input is logic state "10", iv) when the applied input is logic state "11", and finally v) filler cell. There are 6 possible locations and each of the cells can be filled with these five possible options. Hence, the total number of combinations will be $5^6 = 15,625$. We generated the geometric models of all the possible different placements and grouped them according to their density. For example, the designs which have only no filler cells have 100% density and the designs that have one filler cell have 83% density. Hence, we have placements from 16.6% density to 100% density in steps of 16.6%.

3) NAND and INV cells: To further investigate the impact of the simple vs complex cells, we performed another study. We fixed the density at 100% and changed the ratio of NAND to INV cells. We kept the number of locations to 6. The number of possible combinations for each location is six, i.e. INV cell having input "1" or "0", and the NAND cell having input "00", "01","10", and "11". Hence, the total number of combinations, in this case, will be $6^6 = 46,656$. We grouped the geometric models according to the ratio of the NAND and INV. Since the dimension of INV cells is smaller than NAND, we match the dimensions by placing a filler next to the INV cells.

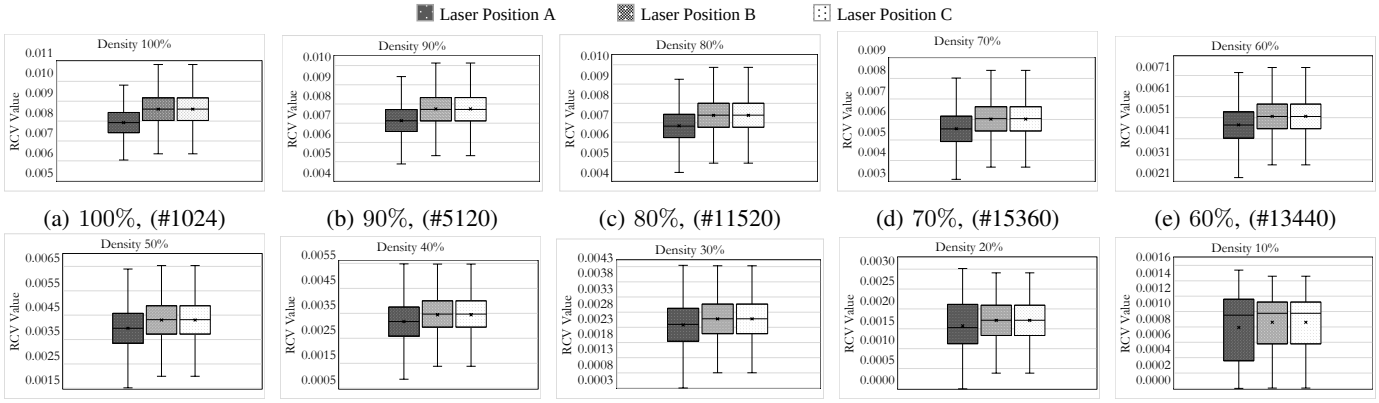
C. Performing OPA in Simulation

In order to perform OPA in simulation, we used the equation 2 as discussed in Section II. For the ease and simplicity, we took the values for the K and β which are fabrication parameters as constant. However, for $K_{PMOS} = 1.3K_{NMOS}$ in our study. For the laser power, we used the value 1, and for the laser spread function, we utilized a Guassian distribution. Next, we parked the laser on 3 different region of a design as shown in Fig. 5, and read out the RCV value of that specific region of the design.

IV. Experimental Results

In this section, we discuss the experimental results obtained using our methodology. We performed the experiments for INV, NAND, and a combination of NAND and INV. We observed the reflection values from three different locations as depicted in Fig. 5. We utilized the box plots to show the obtained RCV values.

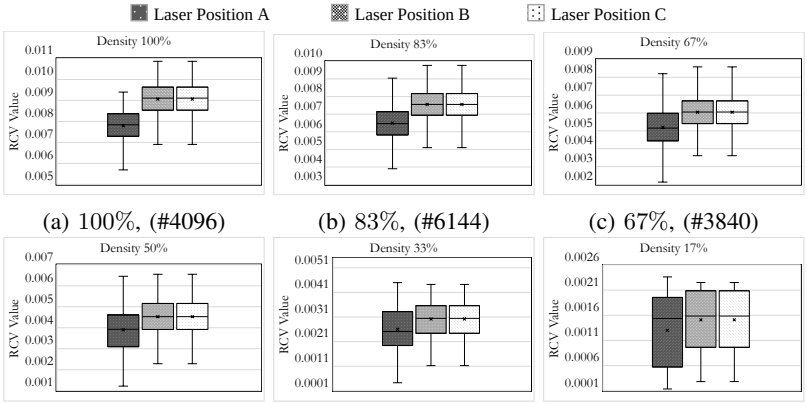
1) INV Cells: In Fig. 6, we show the RCV values as the density is reduced from 100% to 10%. We see that the RCV values are reducing with the reduction of density for INV. The RCV values of the three different locations are also very close to each other. On average, as we reduce the density from 100%



(a) 100%, (#1024) (b) 90%, (#5120) (c) 80%, (#11520) (d) 70%, (#15360) (e) 60%, (#13440)

(f) 50%, (#8064) (g) 40%, (#3360) (h) 30%, (#960) (i) 20%, (#180) (j) 10%, (#20)

Fig. 6: RCV values for varying density of INV (# Number of designs)



(a) 100%, (#4096) (b) 83%, (#6144) (c) 67%, (#3840)

(d) 50%, (#1280) (e) 33%, (#240) (f) 17%, (#24)

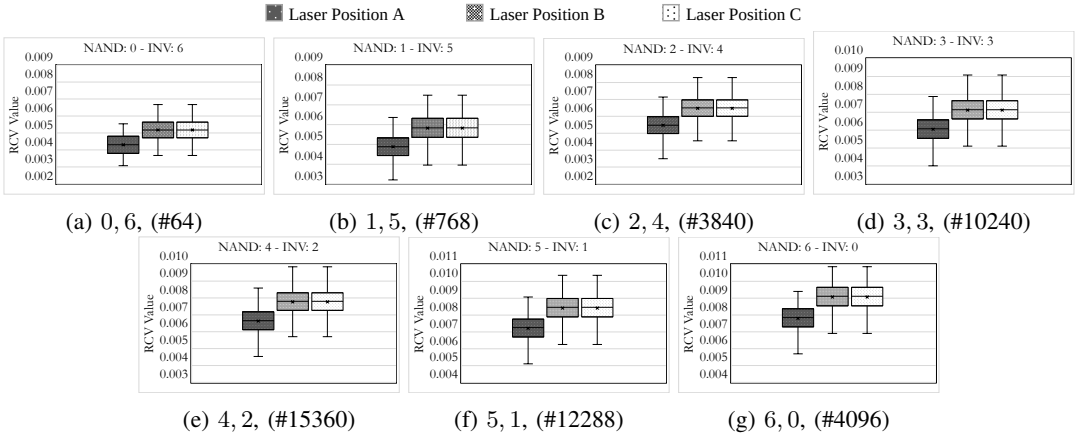
Fig. 7: RCV values for varying density of NAND (# Number of designs)

to 10%, the RCV value changes from 0.008 to 0.0008. Since we want to camouflage the secure circuit, the RCV value has to be as high as possible. Hence, the higher value is desired, but this comes with the additional cost of area and power. Thus, the designer can tailor the design density of the camouflage circuit depending on the constraints. At lower densities, we also observe that the RCV values vary largely with respect to the design placement and the input values, hence at lower densities to achieve better camouflage the placement and the input needs to be selected for achieving high RCV.

2) NAND Cells: In Fig. 7, we show the RCV values as the density is reduced from 100% to 17%. The granularity of placement is coarser as the NAND cells are larger as compared to the INV, and we wanted to keep a similar area for our study. We see that similarly to INV, the RCV values are reducing with the reduction of density for NAND. The RCV values of the three different locations are also very close to each other. On average, as we reduce the density from 100% to 17%, the RCV value changes from 0.009 to 0.0015. The RCV value of the NAND cells is slightly higher than the INV cells for a similar density. Hence, it is better at camouflaging as compared to the INV cells. For example, for a 100% density, INV gives an RCV value of 0.0083, while NAND gives an RCV value of 0.0086. Therefore, the designer can use complex gates for camouflaging instead of simple gates. However, complex gates will come with an additional cost in terms of power consumption and also increase the routing complexity. In any case for a secure cell, the designer chooses to trade off between the required amount of robustness required versus cost. We also observe a higher variation in the RCV values for lower densities, similar to INV cells.

3) NAND and INV Cells: In Fig. 8, we show the RCV values for NAND and INV at 100% density. We performed this experiment to highlight the difference when using INV vs NAND cells for camouflaging. As we increase the ratio of NAND cells to INV cells while keeping the density to be at 100%, we observe an increase in the RCV. For the case where we have 0 NAND cells and 6 INV cells, we see that the RCV value is 0.004. However, in the case where we have 6 NAND cells and 0 INV cells, the RCV value is 0.008, which is twice that of the INV cells. This clearly demonstrates that complex gates are far better at camouflaging as compared to simple gates.

Overall we made the following key observations from our



(a) $0, 6$, (#64) (b) $1, 5$, (#768) (c) $2, 4$, (#3840) (d) $3, 3$, (#10240)

(e) $4, 2$, (#15360) (f) $5, 1$, (#12288) (g) $6, 0$, (#4096)

Fig. 8: RCV values for varying density of (NAND, INV) set with 100% Density (# Number of designs)

study.

- The higher the density, the better the camouflage, as the RCV value is higher.
- Complex gates are better at camouflaging as compared to simple gates.
- For lower densities the variation in RCV is much larger, hence the cell placement and the inputs need to be examined more thoroughly.

V. Ease of Integration and Overheads

Our proposed methodology can be integrated into the ASIC design flow in a number of ways. One of the methods can be to design a black box having a high density of NAND/INV cells and place it around the cell we want to secure against OPA. We can also identify localized regions in the layout and place high-density cells around them to robustify these cells against OPA. Since this process of increasing robustness against OPA is along the lines of the typical ASIC design flow, it can also be added as a command to the industry standard tools.

Our proposed methods require placing high-density cells around the secure cell, which can be driven using inputs that are not on the critical path. Hence, the proposed methodology has no performance overheads. Since these high-density cells are placed only around secure cells, the area and power overhead will depend on the number of cells that needs to be secured. We will explore this in the future.

VI. Conclusion and Future Work

In this work, we investigated the effects of increasing the local density around a logic cell that must be secured as a novel countermeasure against OPA. We showed through an extensive study that increasing the density around the secure cell, that is desirable to an adversary, leads to an increase in the reflection. This additional reflection from the denser region hinders the attack and helps camouflage the secure cell. As of our future work, we will investigate our study with more logic cells, and integrated our solution in a large scale design to evaluate our methods performance, security measures.

References

[1] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*. CRC press, 2018.

[2] X. Lou, T. Zhang, J. Jiang, and Y. Zhang, "A survey of microarchitectural side-channel vulnerabilities, attacks, and defenses in cryptography," *ACM Computing Surveys (CSUR)*, vol. 54, no. 6, pp. 1–37, 2021.

[3] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology—CRYPTO'99: 19th Annual International Cryptology Conference Santa Barbara, California, USA, August 15–19, 1999 Proceedings 19*. Springer, 1999, pp. 388–397.

[4] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi, "The em side-channel (s)," in *CHES*, vol. 2. Springer, 2002, pp. 29–45.

[5] U. Kindereit, G. Woods, J. Tian, U. Kerst, R. Leihkauf, and C. Boit, "Quantitative investigation of laser beam modulation in electrically active devices as used in laser voltage probing," *IEEE TDMR*, 2007.

[6] U. Kindereit, "Investigation of laser-beam modulations induced by the operation of electronic devices," Doctoral Thesis, Technische Universität Berlin, Fakultät IV - Elektrotechnik und Informatik, 2009.

[7] H. Lohrke, S. Tajik, C. Boit, and J.-P. Seifert, "No place to hide: Contactless probing of secret data on fpgas," in *CHES*, 2016.

[8] S. Tajik, H. Lohrke, J.-P. Seifert, and C. Boit, "On the power of optical contactless probing: Attacking bitstream encryption of fpgas," 2017.

[9] H. Shen, N. Asadizanjani, M. Tehranipoor, and D. Forte, "Nanopyramid: An Optical Scrambler Against Backside Probing Attacks," 2018.

[10] E. Amini et al., "Assessment of a Chip Backside Protection," *Journal of Hardware and Systems Security*, 2018.

[11] E. Amini and et al., "Special session: Physical attacks through the chip backside: Threats, challenges, and opportunities," in *VTS*, 2021.

[12] T. Farheen, S. Roy, S. Tajik, and D. Forte, "A twofold clock and voltage-based detection method for laser logic state imaging attack," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 31, no. 1, pp. 65–78, 2023.

[13] S. Parvin and et al, "Toward optical probing resistant circuits: A comparison of logic styles and circuit design techniques," in *ASP-DAC*, 2022.

[14] M. T. Rahman, S. Tajik, M. S. Rahman, M. Tehranipoor, and N. Asadizanjani, "The key is left under the mat: On the inappropriate security assumption of logic locking schemes," 2020.

[15] T. Krachenfels, F. Ganji, A. Moradi, S. Tajik, and J.-P. Seifert, "Real-world snapshots vs. theory: Questioning the t-probing security model," in *IEEE SP*, 2021.

[16] T. Krachenfels, T. Kiyan, S. Tajik, and J.-P. Seifert, "Automatic extraction of secrets from the transistor jungle using laser-assisted side-channel attacks," in *USENIX*, 2021.

[17] T. Krachenfels, J. Seifert, and S. Tajik, "Trojan awakener: Detecting dormant malicious hardware using laser logic state imaging," *CoRR*, 2021.

[18] V. Ravikumar, G. Lim, J. Chin, K. Pey, and J. Yang, "Understanding spatial resolution of laser voltage imaging," *Microelectronics Reliability*, 2018.