FELOPi: A Framework for Simulation and Evaluation of Post-Layout File Against Optical Probing

Sajjad Parvin[ψ], Mehran Goli[ψ,‡] Frank Sill Torres[†], and Rolf Drechsler[ψ,‡]

[ψ] Institute of Computer Science, University of Bremen, Germany
[†] Institute for the Protection of Maritime Infrastructures, German Aerospace Center, Germany
[‡] Cyber-Physical Systems, DFKI GmbH, Germany
{parvin, mehran, drechsler}@uni-bremen.de, frank.silltorres@dlr.de

Abstract— Optical Probing (OP) has been shown to be capable of retrieving intellectual property of the chips. However, to design a robust circuit against OP, the chip must be designed, fabricated, and optically probed in an experimental setup to determine the OP robustness of the design which is time consuming. To mitigate the aforementioned problems, we propose a simulation framework, namely FELOPi, which takes the layout file format of a design as an input and then performs OP on it. FELOPi can help designers to design robust circuits toward OP attacks before fabricating the chip. Hence, utilizing FELOPi results in tremendous time and cost reduction.

I. Introduction

Designing a 100% secure and invulnerable *Integrated Circuit (IC)* is almost impractical as it requires rigorous testing, which results in an increase in the cost and time to market of the end product. Therefore, for mission-critical application ICs there is the need for a tool to evaluate the design security robustness against various attacks, i.e. side-channel attacks. Designers are aware of how to design against some well-known attacks which are well studied in the literature, such as differential power attack by designing a circuit using differential logic gates [1] or introducing randomness to the processed data by silicon [2]. However, for newer and lesser known types of security attacks, countermeasures are barely studied. For example, Lohrke et al. [3] showed that by performing optical probing through the backside of silicon, an adversary can retrieve secret data on chips. Several countermeasures have been proposed to prevent *Optical Probing (OP)* attack, such as [4–6].

As a cost-effective and fast approach to designing a robust chip against OP, we propose FELOPi, a framework for the simulation and evaluation of post-layout files against optical probing. FELOPi can perform OP in simulation using the GDS-II file of the design. This allows designers to evaluate their design against OP before sending it for fabrication, which cuts a huge amount of cost and time for the design house. As a result, in the design phase, designers can have a better understanding of the robustness of a design against OP.

II. Preliminaries

A. Methodology and Setup

OP is a technique where a focused laser beam is scanned using galvanometric mirrors or statically pointed at a single point of a chip while a detector collects the reflected light. Since silicon is transparent to light in the *Near-InfraRed (NIR)* spectrum, OPing an 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 IC passes the bulk silicon and travel through the active areas of transistors. A portion of incident light is reflected back, for instance, when the incident light hits the first metal layer, then it 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. The reflected light experiences a change in the index of absorption and refraction as it passes through a transistors due to the existence of an electrical field [7].

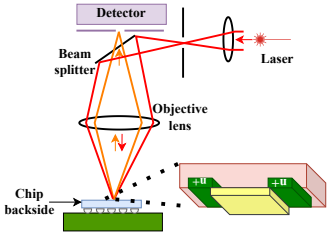


Fig. 1. Illustration of an optical probing setup.

There exists several OP scanning methods: *Electro-Optical Probing (EOP)*, *Electro-Optical Frequency Mapping (EOFM)*, and *Laser Logic State Imaging (LLSI)*. In EOP, a laser light is parked on a certain spot of a chip, and reads out the voltage at that spot [3]. In EOFM, an area of chip is scanned by moving the laser light across the chip. EOFM is used to localize the regions carrying signals with a specific frequency of operation [8]. And LLSI is an extension of EOFM where the laser scans an specific region of the chip, while the power supply is modulated with a small sinusoidal signal e.g. ($100mV$, $100kHz$) [9]. The purpose of LLSI is to read out the static state of each device in the design.

B. Reflection Caliber Value (RCV)

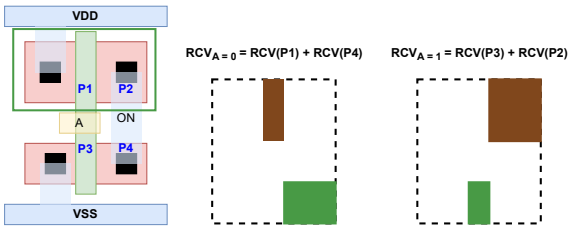
In [5], a simple to use model is proposed for the reflection calculation of a transistor under OP. This model, which is called, RCV approximate the reflected light from a transistor's active region as a linear function of applied voltage to the transistor's terminals (V), amplification constant of the transistor K ($K_{PMOS} = 1.3K_{NMOS}$), transistor's fabrication related parameter β, power of incident laser light P_L, and the area of transistor's active region. The RCV value can be expressed as follow:

$$RCV = V \times K \times \beta \times P_L \int_0^{2\pi} \int_0^{r_{spot}} p(r) \times A(r,\theta)\, dr d\theta, \quad (1)$$

where $p(r)$ and $A(r,\theta)$ are laser's power Gaussian distribution, and area of active region under laser spot in polar coordinate, respectively.

III. Modeling Gates Layout's Active Regions

To perform OP on a cell layout, we need to model the active regions' geometry. By applying different input values to a logic cell, different regions of a logic cell's layout contribute to the reflection of light under OP. This means, those regions of each transistor in the logic gate that has $|\Delta V| > 0$ with respect to the body voltage, can modulate the incident light [7]. Consider the NOT cell in Fig. 2 (a), if we exclude the diffusion regions connected to VDD and VSS due to having the $\Delta V = 0$ for those diffusion regions with respect to the body voltage (NMOS, and PMOS body terminals are connected to VSS, and VDD, respectively), we have four different regions that modulate the incident light (regions P1, P2, P3, and P4). By applying input logic "0", the regions P1 and P4 contribute to the reflection of light, as shown in Fig. 2 (b). Applying input logic "1" results in regions P2 and P3 to contribute to the reflection of light, as shown in Fig. 2(c). This is due to having $|\Delta V| > 0$ on these regions based on the applied input value with respect to their bulk voltage. Moreover, we created a pattern-based geometry of each logic gate from all the cells in our



(a) (b) (c)

Fig. 2. (a) standard CMOS NOT gate's layout, (b) NOT gate layout's geometry contributing to the reflection of light when the applied input is logic "0", (c) NOT gate layout's geometry contributing to the reflection of light when the applied input is logic "1".

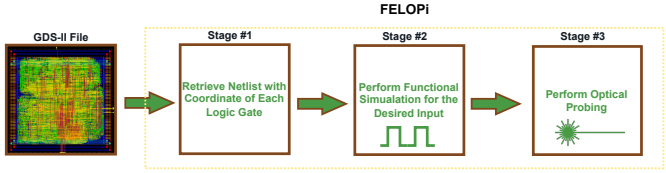


Fig. 3. FELOPi's work flow.

design, similar to what is shown for the NOT gate in Fig. 2. We created a geometry-based library based on the applied input values for standard CMOS NOT, NAND2, NOR2, XOR2, NAND3, NOR3, XOR3, and FF gate.

IV. FELOPi Framework

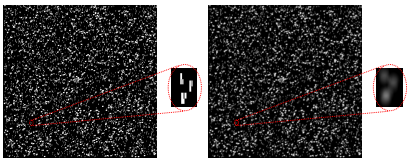
The working process of "FELOPi" is demonstrated in Fig. 3. The FELOPi takes the GDS-II file of the design as an input, as it contains information about each transistor and its corresponding wiring in a design. The voltage present at the diffusion regions (drain, source, and gate of transistors) determines the strength of the electrical field. According to the Equation (1), the voltage present at each terminal of the transistor is proportional to the strength of the reflected light from a device (the electric field present in each junction modulates the incident light). After feeding the GDS-II file to FELOPi, we need to retrieve the coordinate of each mapped gate in the netlist from the GDS-II file. There exist tools that can perform such an operation, i.e., the Calibre tool from Mentor Graphics.

After retrieving the location of each logic cell from the GDS-II file, we perform a functional simulation on the netlist. The purpose of the functional simulation is to obtain the state of each logic gate in the GDS-II file based on the applied input. FELOPi has a logical computation engine developed in C++ where a user can apply any input value to the netlist and retrieve the state of each logic gate in the design. It must be noted for functional simulation, we use Verilog netlist, as performing post-layout simulation on the GDS-II file takes a long time due to extracting all the parasitic capacitance and resistance in the design.

After determining the state of each logic gate in the design, FELOPi replaces each logic gate with its corresponding geometry model, as explained in Section III. Then, we can whether park the laser on a spot in a specific coordinate of the chip to read the reflection value from that specific region of the design (EOP analysis) or scan the entire region of the design using the laser (convolution between laser distribution function and layout of the design) to create an activity map of the design (EOFM, and LLSI analysis). For an example, the activity map of a design under OP is shown in Fig. 4.

V. Discussion and Integration

FELOPi is a powerful tool that can be integrated in the work flow of both designers and security test engineers. FELOPi enables its user to develop robust circuit against OP, and explore



(a) (b)

Fig. 4. (a) GDS-II file after passing through stage 1 and stage 2 of FELOPi, (b) scanning all the logic gates in the design.

vulnerabilities of a design in simulation with no cost. Moreover, by providing correct logic gates' model designed in various transistor technologies such as FinFET, FD-SOI, RFET, etc, FELOPi can be useful to develop OP secure circuits in these technologies. Furthermore, OP is a time consuming process in an experimental setup, and FELOPi reduces the probing time to few seconds by performing the OP in simulation (using state of the art GPU/CPU). Moreover, in [10], it is shown that OP can be used to detect hardware trojans inserted in the design during the fabrication stage by comparing the OP analysis of unmodified chip's layout, and OP analysis of the fabricated chip. Consequently, FELOPi can be used to expose hardware trojans in the designs as well.

VI. Conclusion and Future Work

In this work, we proposed the first framework called "FELOPi" to evaluate the security robustness of a layout against OP. FELOPi takes the GDS-II file as an input and, based on the applied input values to the circuit, computes the region of transistors in each cell gate that contributes to the reflection of light. Hence, it empowers engineers to perform EOP, EOFM, and LLSI on the circuit to probe the processed signal on a chip's layout file. FELOPi's purpose is to help designers and security engineers to evaluate circuits against OP on a large scale. As of our future work, we will load a more detailed response model of transistors and logic gates into FELOPi from our taped-out chip. Hence, FELOPi will be the first simulator developed for large-scale designs that perform OP analysis based on real technology (a commercial 28nm technology).

Acknowledgement: 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.

References

[1] A. Moradi, M. T. M. Shalmani, and M. Salmasizadeh, "Dual-rail transition logic: A logic style for counteracting power analysis attacks," *CEE*, 2009.

[2] S. Chen, W. Ge, J. Yang, B. Liu, and J. Yang, "A power analysis attack countermeasure based on random execution," *TrustCom/BigDataSE*, 2018.

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

[4] M. T. Rahman, N. F. Dipu, D. Mehta, S. Tajik, M. Tehranipoor, and N. Asadizanjani, "Concealing-gate: Optical contactless probing resilient design," *JETC*, 2021.

[5] S. Parvin, T. Krachenfels, S. Tajik, J.-P. Seifert, F. Sill Torres, and R. Drechsler, "Toward optical probing resistant circuits: A comparison of logic styles and circuit design techniques," *ASP-DAC*, 2022.

[6] E. Amini et al., "Assessment of a Chip Backside Protection," *JHSS*, 2018.

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

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

[9] B. Niu, G. M. E. Khoo, Y.-C. S. Chen, F. Chapman, D. Bockelman, and T. Tong, "Laser Logic State Imaging (LLSI)," *ISTFA*, 2014.

[10] S. Parvin, M. Goli, F. Sill Torres, and R. Drechsler, "Trojan-D2: Post-layout design and detection of stealthy hardware trojans - a RISC-V case study," *ASP-DAC*, 2023.