Lo-RISK: Design of a Low Optical Leakage and High Performance RISC-V Core

Sajjad Parvin[ψ], Sallar Ahmadi-Pour[ψ], Chandan Kumar Jha[ψ], Frank Sill Torres[‡], and Rolf Drechsler[ψ,†]
[ψ] 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, sallar, chajha, drechsler}@uni-bremen.de, frank.silltorres@dlr.de

***Abstract*—Optical Probing Attacks (OPA) have been shown as an effective solution to bypass several known protection schemes of integrated circuits and to read out sensitive information, like security keys or *Intellectual Property* (IP). As a countermeasure, we propose a methodology for designing high-performance OPA-hardened digital circuits.**

Several existing solutions for OPA-hardened designs require changes in the fabrication process, resulting in a higher cost. Other approaches suffer from notable performance reductions and require significant changes in the employed gate libraries. In this work, we alleviate these limitations and propose a methodology to design high-performance OPA-hardened circuits. We achieve this by using a two-step methodology. First, we design a high-performance, and *Low optical Leakage Dual-Rail Logic* (LoL-DRL) gate library based on a standard CMOS gate library. That means, no complete redesign of the layout is required, unlike comparable approaches. Second, we propose a lightweight synthesis technique to synthesize OPA-hardened circuits from conventional circuits. Furthermore, we applied our methodology on a RISC-V core to design the first OPA-hardened RISC-V core named *Lo-RISK*. Our method ensures a negligible performance penalty, however at notable costs in terms of area and power.

***Keywords*—Optical Probing, RISC-V, ASIC, Security**

I. Introduction

With the increasing amount of security flaws uncovered and attack methods proposed, engineers are often challenged to find new ways to secure their designs and prevent the exposure of sensitive data. For example, attacking methods like Meltdown [1] and Spectre [2] exploit critical vulnerabilities of modern processors and are able to reveal the protected information during operation. Other schemes are based on *Side-Channel Analysis* (SCA), such as EM attacks, differential power attacks, etc. However, the industry standard technologies are not developed, keeping security as a priority. This can make a design vulnerable, which can be exploited by the attackers, e.g. via backdoors. In recent years, the *Optical Probing Attack* (OPA) has been shown as an effective method, to probe chips for sensitive and seemingly secure information using contactless probing through the backside of modern integrated circuits [3]. Data on areas of the chip containing sensitive information can be mapped out, and the *Intellectual Property* (IP) can be revealed. As a countermeasure, various methods have been proposed [4], [5] to harden circuits against such attacks. These methods often come with trade-offs that make them infeasible for industrial applications. For example, some methods lead to significantly higher costs due to modifications required in the fabrication process. Other approaches require tailored layouts, leading to significant performance reduction, i.e. near-threshold computing [5]. In this work, we mitigate both of these issues and propose an industry-compatible CMOS gate library that is OPA-hardened called *Low optical Leakage-Dual Rail Logic* (LoL-DRL). As our solution complies with the standard CMOS production process, the downsides of already investigated methods are avoided. Furthermore, we employ our approach for turning an open-source available RISC-V processor robust against OPA with minimal change in the ASIC-design flow. RISC-V [6] is a free and open source *Instruction Set Architecture* (ISA) that has gained attention from both the academic and the industrial community.

The contribution of this work can be summarized as follows:

- Proposing the OPA-hardened gate library *LoL-DRL*, based on standard CMOS gate library. This OPA-hardened library does not require layout redesign from scratch. However, the constraint for OPA-hardening can be obtained by juxtaposing two complementary standard CMOS gate layouts from the library.
- Comparison of the information leakage in case of *Optical Probing* (OP) of the standard CMOS gate library against the proposed *LoL-DRL* gate library.
- Application of the proposed OPA-hardened gate library for the RISC-V processor *Lo-RISK*.

The rest of this paper is organized as follows. Section II discusses the preliminary and background of OP and gives a brief overview of RISC-V. Section III introduces the OPA-robust gate library as well as the ASIC flow. Section IV presents obtained results, and Section V concludes this work.

II. Preliminaries

In this section, we provide the necessary information on the fundamentals of OP (Section II-A), background on the mathematical model of OP (Section II-B) and finally a brief overview of RISC-V (Section II-C).

A. Fundamentals of Optical Probing

The basic principle of OP is shown in Fig. 1. The setup shows a focused laser beam that is positioned at the backside of a chip with a wavelength around 1100 to 1300 nm. This is due to the transparency of silicon to the *Near-InfraRed* (NIR) light. Based on the voltage present on each transistor's terminal in that area of the chip, the laser light is modulated

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.

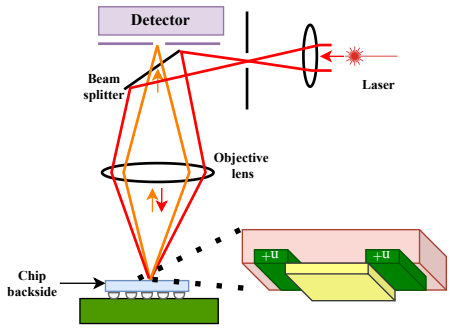


Fig. 1: Optical probing setup

due to the strength of the electrical field in the junctions of the transistor [7]. The modulation of incident light means a change in the absorption and refraction index of reflected light in comparison to the incident light. Hence, the reflected light is collected with a detector, and the present voltage can be identified at the transistor terminal based on the change in the absorption and refraction index of the incident light [7].

Since differences in the voltage applied to a transistor can be detected using OP, this can be used to extract data processed or stored on the *Integrated Circuit* (IC). The technique where the laser is statically pointed at one location of the chip is called *Electro-Optical Probing* (EOP). Using EOP, sensitive data processed by the IC can be extracted [3]. Due to the weak modulation of the optical beam, the chip has to be operated in a loop while integrating the captured signal to achieve a sufficient *Signal-to-Noise Ratio* (SNR).

To localize periodical signals on the chip, the laser can be scanned over the device while feeding the detector's output into a narrow-width bandpass filter set to the frequency of interest. The measurement results in a gray-scale encoded image of the scanned area, where bright spots indicate areas with switching activity. The corresponding technique is called *Electro-Optical Frequency Mapping* (EOFM). 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 located using EOFM and later probed using EOP [3]. An extension to EOFM, called *Laser Logic State Imaging* (LLSI), allows even the extraction of static logic states by modulating the power supply of the device [8], [9].

B. Modeling Optical Probing

Although there are different ways of defining the spatial resolution R, the commonly used formulation for OP is defined in Fourier optics and by Abbe's criterion [10] as $R = 0.5\lambda/NA$ where λ is the wavelength of the light and NA is the Numerical Aperture of the microscope system. R can be seen as the minimum distance between resolvable two-point sources [10]. The intensity of the laser spot can be modeled as a Gaussian distribution [10] with

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

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 [10].

According to its definition, the optical resolution can be improved by either reducing λ or increasing the NA. The opaqueness of silicon for a reduced λ below 1100 nm puts challenges on sample preparation. For further information on visible light probing, we refer to [11]. On the other hand, the theoretical maximum NA achievable by a classical microscope lens, i.e., through air, is 1. However, existing high-end lenses achieve an NA of only around 0.75, resulting in a maximum possible resolution between 733 nm and 866 nm for a λ of 1100 nm and 1300 nm, respectively. A *Solid Immersion Lens* (SIL) can increase the NA up to around 3.5, increasing the resolution to around 200 nm, allowing *Failure Analysis* (FA) of single transistors down to 10 nm technologies [12].

In [5], a lightweight model is proposed for the reflection of a transistor under OP. This model, which is called, *Reflection Caliber Value* (RCV), 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), power of incident laser light (P_L), and the area of transistor's active region. The RCV value can be expressed as follow:

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

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.

C. RISC-V

The RISC-V ISA is a royalty-free, modular, and open-source instruction set that has recently received a lot of attention. Around a basic set of mandatory instructions covering arithmetic operations, control transfer instructions as well as load and store instructions, the ISA can be augmented with instruction set extensions. Such extensions can add further instructions like multiplication and division, support for compressed instructions, and more. Furthermore, the RISC-V ISA specification defines *Control and Status Registers* (CSRs) to further extend the processor's features with interrupts, user modes, and more. Part of the success of RISC-V as an ISA can be observed in the amount of available open-source projects supporting the instruction set. For more comprehensive information around the RISC-V ISA refer to the ISA specification Volume 1 [6] for details around the instruction set and the modular extensions as well as Volume 2 [13] on the privileged architecture covering CSRs and additional features.

In this work, we utilize the RISC-V processor from the open source MicroRV32 platform [14] to make it OPA-hardened. The multi-cycle processor is configured to feature the base instruction set together with the extensions for multiplication and division and CSRs.

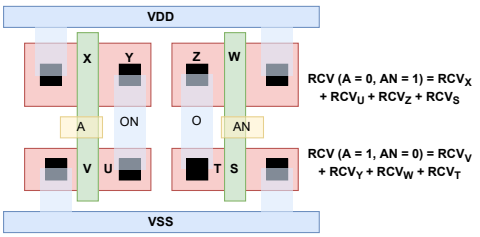


Fig. 2: DRL based CMOS INVERTER

III. ASIC FLOW, AND OPA LEAKAGE ANALYSIS

OPA has been used successfully to breach the security of a chip and hijack its confidential information [3]. However, there are some countermeasures proposed in the literature to prevent OPA on chips containing secure information. These methods require a change in the fabrication process of transistors [4] or require active chip monitoring, which can be bypassed [3]. Furthermore, these methods are not compatible nor feasible for standard industrial processes. Hence, we need to find an answer to the question: *How to prevent OPA using industry-standard technology and at the layout level*?

It is shown in [5], that the differential logic style based gates are more robust against OPA as compared to the standard CMOS based gates.

A. Low optical Leakage Dual-Rail Logic Based CMOS Gates

LoL-DRL gates are created using CMOS gates with a constraint of juxtaposing two complementary gates from a CMOS standard gate library which are driven with complementary input values. Such an example for a LoL-DRL inverter is shown in Fig. 2. In principle, differential gates have less optical information leakage [5]. This is due to the limited optical resolution of the optical probing setup, and the compact layout design style of differential logic gates, i.e. LoL-DRL. Hence, an adversary with OPA capability, when probing a LoL-DRL based circuit, cannot identify which region of a logic gate has logic value "0" or logic value "1". In other words, by constraining the regions carrying complementary signals in the layout of each LoL-DRL cell, it becomes indistinguishable for an adversary with OPA capabilities to probe. Hence LoL-DRL based designs are OPA-hardened.

To compare the optical leakage of gates from the standard CMOS gate library with the LoL-DRL gate library, we performed OPA via simulation, based on the model discussed in Section II. We apply various input values to each gate and park the laser beam on the *Pull-Up Network* (PUN), *Pull-Down Network* (PDN), and in a region to cover both PDN and PUN (EOP analysis). Upon applying various input values to the gate's layout, different regions of the logic gate's layout have $|\Delta V| > 0$ with respect to the bulk voltage. Regions with $|\Delta V| > 0$ contribute to the reflection of light which means in that specific region of the logic gate, there exists an electric field capable of modulating incident light. Hence, we model the geometry of the regions of the gate's layout with $|\Delta V| > 0$ and assign RCV value to it, to perform OPA in simulation. As

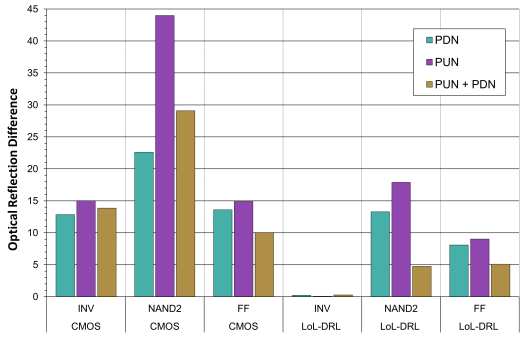


Fig. 3: Optical leakage analysis of standard CMOS and differential CMOS gate library

an example consider the layout of the LoL-DRL inverter gate shown in Fig. 2. Based on applying different logic input values, different regions of the transistors contribute to the reflection of light.

Next, we determine the difference between the largest and the smallest optical reflection value among all input combinations applied to the logic gate. This value defines the leakage for a logic gate upon applying various input combinations, as discussed in [5]. Fig. 3 depicts the results of our analysis using a wavelength of 1300 nm and NA of 3.5. It can be concluded that our LoL-DRL gate library shows less leakage in comparison to the standard CMOS gate library. We used the logic gates with minimum feature size from the standard gate library for OP simulation. It is sufficient to perform this analysis for INVERTER, NAND2, and Flip-Flop as they are minimally functionally complete set and can be used to implement any boolean function.

B. ASIC Flow

The Lo-RISK framework is shown in Fig. 4. For the ASIC flow of the Lo-RISK core, we created a library that consists of LoL-DRL based INVERTER, NAND2, NAND3, XOR2, XOR3, and a FF. To use this library in the ASIC flow, we need to characterize these gates to obtain a timing library and prepare the gates' ".lef" file for the place and route within *Cadence Innovus*. We performed the characterization, using the *Cadence Liberate*. Since we created the LoL-DRL gate library based on the standard CMOS gate library, we used the load and transition values from the ".lib" file of the standard CMOS gate library for characterization.

Next, we synthesized the RISC-V core from the MicroRV32 platform using a standard CMOS gate library. For the synthesis, we used INVERTER, NAND2, NAND3, XOR2, XOR3, and FF to be used by the *Cadence Genus*. Also, the LoL-DRL version of the designs was also created. We then used a script to convert the synthesized RISC-V core using the standard CMOS gate library to an OPA-hardened RISC-V core. This script replaces each standard gate in the synthesized netlist with its OPA-hardened LoL-DRL based CMOS gate. By performing a conversion on the RISC-V netlist synthesized using standard CMOS gate library, we achieve OPA-hardened RISC-V core, namely, Lo-RISK. As the next step, we need to

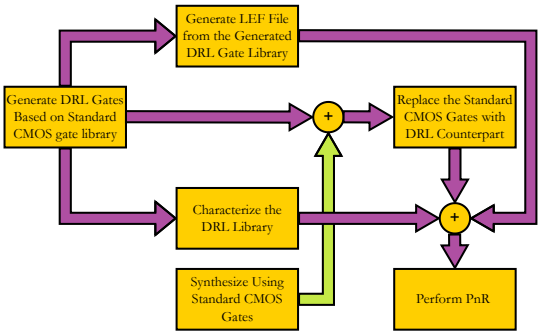


Fig. 4: ASIC flow of Lo-RISK

TABLE I: Post Synthesis performance comparison between standard RISC-V and Lo-RISK

Specification	Standard RISC-V	Lo-RISK
Power (µW)	0.725	1.482
Area (μm^2)	12208	24417
Frequency (MHz)	158	156
#Gates	24208	48416

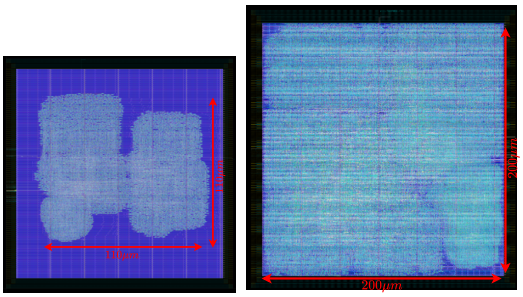
import the Lo-RISK netlist to the *Cadence Innovus* to perform place and route. *Cadence Innovus* takes the timing library namely,".lib" file, generated in the characterization stage, and ".lef" file of the each gate in our LoL-DRL gate library which is generated using *Cadence Abstract*, as inputs. The ".lib" and ".lef" files are used for timing analysis, place, and route.

IV. Results and Discussion

As previously mentioned, we evaluate the performance of the proposed OPA-hardening technique on the core of the open-source MicroRV32 platform [14]. The core uses the 32-bit base instruction set together with the M-extension for multiplication, division, and Zicsr-extension for CSRs. We used *Cadence Genus* to perform synthesis, and place and route using a commercial 28nm node technology. The post-synthesis performance results are shown in Table I. It can be deduced from Table I that the power, area, and gate count of the Lo-RISK is twice as much of the standard RISC-V core. This is due to using LoL-DRL-based CMOS gates which basically each gate in the OPA-hardened library is a compound of two standard gates constrained to be juxtaposed in the layout. However, Lo-RISK has a similar operating frequency as compared to the RISC-V designed using a standard CMOS gate library as shown in Table I. Fig. 5 depicts the layout of the RISC-V and Lo-RISK obtained using *Cadence Innovus*. By comparing Fig. 5 (a), Fig. 5 (b), and the results in Table I, we can conclude that for a secure design, there is a trade-off between area, power consumption, and security. However, for a high-performance secure design doubling the area, and power consumption are acceptable.

V. Conclusion

In this paper, we proposed the design flow for the first OPA-hardened RISC-V core. To our knowledge, this is the first complete work that explores starting from the library design to the place and route of a large OPA-hardened circuit.



(a) (b)

Fig. 5: (a) standard RISC-V layout, (b) Lo-RISK layout

We show how engineers can utilize the standard CMOS gate library, namely LoL-DRL, to design a secure circuit against OPA at the expense of doubling the area, and power, while keeping the frequency of operation the same as conventional circuits built based on standard gate library. Moreover, by using our approach to design an OPA-hardened circuit, the designers can use the standard gate library without much effort in redesigning new gate libraries or designing gates with novel layouts or using OPA-hardened transistor technology (novel material and structure) that is expensive, and unknown to the industry. By this, we proposed an industry-friendly ASIC flow to design OPA-hardened circuits.

References

[1] M. Lipp *et al.*, "Meltdown: Reading Kernel Memory from User Space," *Commun. ACM*, vol. 63, no. 6, p. 46–56, may 2020.
[2] P. Kocher *et al.*, "Spectre Attacks: Exploiting Speculative Execution," *IEEE Symposium on Security and Privacy (SP)*, pp. 1–19, 2019.
[3] S. Tajik, H. Lohrke, J.-P. Seifert, and C. Boit, "On the Power of Optical Contactless Probing: Attacking Bitstream Encryption of FPGAs," *ACM SIGSAC Conf. on Comp. and Commu. Security*, p. 1661–1674, 2017.
[4] H. Shen, N. Asadizanjani, M. Tehranipoor, and D. Forte, "Nanopyramid: An Optical Scrambler Against Backside Probing Attacks," *ISTFA*, pp. 280–289, 2018.
[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*, pp. 429–435, 2022.
[6] A. Waterman and K. Asanović, Eds., *The RISC-V Instruction Set Manual; Volume I: Unprivileged ISA*, 2019.
[7] 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 Trans. on Device and Materials Rel.*, vol. 7, no. 1, pp. 19–30, 2007.
[8] B. Niu *et al.*, "Laser Logic State Imaging (LLSI)," *ISTFA 2014*, pp. 65–72, 2014.
[9] T. Krachenfels, F. Ganji, A. Moradi, S. Tajik, and J.-P. Seifert, "Real-World Snapshots vs. Theory: Questioning the t-Probing Security Model," *IEEE SP*, pp. 1955–1971, 2021.
[10] V. K. Ravikumar, G. Lim, J. M. Chin, K. L. Pey, and J. K. Yang, "Understanding spatial resolution of laser voltage imaging," *Microelectronics Reliability*, vol. 88, pp. 255–261, 2018.
[11] C. Boit *et al.*, "Contactless visible light probing for nanoscale ics through 10 um bulk silicon," *NANOTS*, 2015.
[12] M. von Haartman *et al.*, "Optical Fault Isolation and Nanoprobing Techniques for the 10 nm Technology Node and Beyond," *ISTFA*, 2015.
[13] A. Waterman and K. Asanović, Eds., *The RISC-V Instruction Set Manual; Volume II: Privileged Architecture*, 2019.
[14] S. Ahmadi-Pour, V. Herdt, and R. Drechsler, "The MicroRV32 Framework: An Accessible and Configurable Open Source RISC-V Cross-Level Platform for Education and Research," *J. of Sys. Architecture*, vol. 133, p. 102757, 2022.