Toward Optical Probing Resistant Circuits: A Comparison of Logic Styles and Circuit Design Techniques

Sajjad Parvin*, Thilo Krachenfels†, Shahin Tajik‡, Jean-Pierre Seifert†§,
Frank Sill Torres¶, and Rolf Drechsler*‖

* Institute of Computer Science, University of Bremen, Germany
† Chair of Security in Telecommunications, Technische Universität Berlin, Germany
‡ Department of Electrical and Computer Engineering, Worcester Polytechnique Institute, USA
§ Fraunhofer SIT, Germany
¶ Institute for the Protection of Maritime Infrastructures, German Aerospace Center, Germany
‖ Cyber-Physical Systems, DFKI GmbH, Germany

Abstract— Laser-assisted side-channel analysis techniques, such as optical probing (OP), have been shown to pose a severe threat to secure hardware. While several countermeasures have been proposed in the literature, they can either be bypassed by an attacker or require a modification in the transistor's fabrication process, which is costly and complex. In this work, firstly, we propose a formulation for the caliber of reflected light from OP. Secondly, we propose circuit design techniques and logic styles to alleviate OP attacks based on our formulation. Finally, we compare several logic families and circuit design techniques in terms of performance and OP security merits. In this regard, we perform simulations to compare the optical beam interaction between the different logic gates. By utilizing our proposed circuit design techniques and dual-rail logic (DRL), the signal-to-noise ratio (SNR) of the reflected light from OP is reduced significantly.

I. Introduction

Sophisticated failure analysis (FA) techniques, such as optical probing (OP), enable the observation of on-chip signals in a contactless manner with high resolution through the chip backside. In the case of OP, the incident laser light is modulated by the different voltages on the chip, which is then fed into a detector. This advanced technique can also be misused as an attack tool. It has been demonstrated that OP attacks can bypass conventional countermeasures and extract confidential information, e.g., secret keys and intellectual property, from integrated circuits (ICs) [1–5]. The predominant use of flip-chip packages, where the chip backside is exposed to the attacker, facilitates the application of OP.

Several countermeasures have been proposed in the literature to combat OP attacks. They can be classified into three categories; 1) attack detection sensors, 2) modification of the IC fabrication process, and 3) circuit-level countermeasures. In [2], an OP detection sensor based on ring oscillators (ROs) is proposed. The idea is to detect the injected heat of the laser beam, which causes changes in the ROs' operating frequencies. However, there are two problems associated with sensor-based countermeasures; a) active monitoring, which results in high power consumption, b) limited spatial resolution, and c) unguarded sensors' control unit, potentially allowing an adversary to disable the detection mechanism. Another approach would be to coat the backside of the chip with an active opaque layer [6], which requires modifying the manufacturing process. On the other hand, an example for the modification of the fabrication process is proposed in [7], where a Nanopyramid structure is added to the transistors to scramble the laser light. Although it might be effective, this approach is costly and highly complex for implementation.

In contrast to previous techniques, circuit-level countermeasures attacks can be more secure and fabrication-friendly because each logic block will be designed to provide robustness against OP attacks inherently. For instance, in [8], a circuit design technique is proposed where a CMOS gate is placed between two other redundant CMOS gates, called concealing gates. These concealing gates hide information of the core gate by producing OP signals based on the input values. However, due to the layout design and distance between the core CMOS gate and concealing gates, deep learning algorithms might be applicable for extracting information from concealing gates [4]. A more thorough approach would be the design of a logic gate that can provide concealment inherently. An example of such a logic family is dual-rail logic (DRL). DRL uses both the input and its complemented version to perform a logical operation and produce the output and its complement. This feature allows designers to cramp transistors carrying signals and their complements. Thus, in each switching state, the reflected light's intensity of a logic gate stays similar.

Our contribution. This work investigates various logic styles and circuit design techniques in terms of performance and robustness against OP attacks. In this regard, we first define the interaction of a single transistor with the optical probe and then expand the formulation on a logic gate. Subsequently, we realize logic gates in different logic styles and model their interaction with the laser beam. We show that considering a DRL, among various solutions, can significantly reduce the signal-to-noise ratio (SNR) of the logic gate under the optical probe. Besides investigating different logic styles, we propose other circuit techniques such as supply voltage reduction and

Contact addresses: {parvin,drechsler}@uni-bremen.de, {tkrachenfels, jpseifert}@sect.tu-berlin.de, stajik@wpi.edu, frank.silltorres@dlr.de

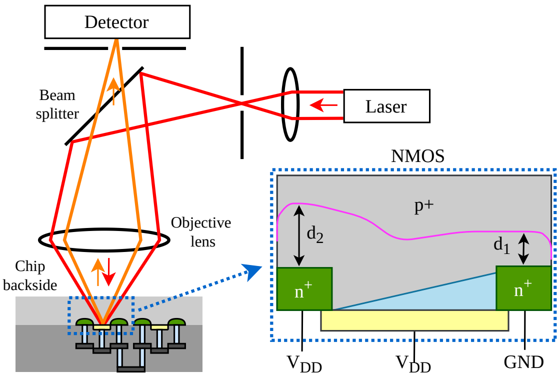

Fig. 1. Schematic of an optical probing setup and an NMOS biased in the saturation region.

limiting the output swing to reduce the reflected light's SNR.

II. Contactless Optical Probing

A. Methodology and Setup

OP capabilities are typically incorporated into a laser scanning microscope (LSM), where a focused laser beam is scanned using galvanometric mirrors or statically pointed at a single point of the device while a detector measures the reflected light, see Fig. 1. As silicon is transparent to light in the near-infrared (NIR) spectrum, imaging an IC through its backside is possible without thinning the material. As illustrated in Fig. 1, the laser light focused on the IC passes the bulk silicon and traverses the active area. A part of the light is reflected, for instance, at the first metal layers and then travels back through the silicon into the microscope lens. The beam splitter then forwards the reflected light to an optical detector, where its intensity is measured and converted into a voltage.

B. Origin of the Signal

For OP with wavelengths around 1300 nm, the main effects of laser beam interaction with the device are absorption and refraction due to free carriers, whereas the number of free carriers depends on the voltage present at the device [9, 10]. The influence of the number of free carriers for wavelength λ on the absorption coefficient α and the index of refraction n can be calculated as follows [9]:

$$\Delta\alpha = \frac{\lambda^2 q^3}{4\pi^2 c_0^3 \epsilon_0 n_0}\left[\frac{\Delta N_e}{m_e^2 \mu_e} + \frac{\Delta N_h}{m_h^2 \mu_h}\right] \tag{1}$$

$$\Delta n = -\frac{\lambda^2 q^2}{8\pi^2 c_0^2 \epsilon_0 n_0}\left[\frac{\Delta N_e}{m_e} + \frac{\Delta N_h}{m_h}\right] \tag{2}$$

where n_0 is the index of refraction of un-doped silicon, q is the electron charge, ϵ_0 is the permittivity of free space, c_0 is the speed of light in vacuum, μ is the mobility, m is the effective mass, and ΔN are the changes in charge carrier density. The indices h and e stand for holes and electrons, respectively. If the voltage applied to the semiconductor interface is changed, the charge carrier density N, i.e., the number of free carriers in the signal path, will change. The maximum amplitude of ΔN is highly dependent on the doping concentration [10]. The authors of [10] have shown that, next to the well doping concentration, also the diffusion doping impacts $\Delta\alpha$ and Δn.

C. Optical Probing for Data Extraction

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 IC. The technique where the laser is statically pointed at one location of the chip is called electro-optical probing (EOP)[1]. Using EOP, sensitive data processed by the IC can be extracted [1, 2]. 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 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)[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 located using EOFM and later probed using EOP [1–3]. 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 [4, 5, 11].

D. Optical Resolution and Technology Size

Although there are different ways of defining the spatial resolution R, the commonly used formulation for optical probing is defined in Fourier optics and by Abbe's criterion [8, 12] 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 [12]. The intensity of the laser spot can be described as Gaussian distribution [12] with

$$p(r) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{\frac{-(r)^2}{2\sigma^2}} \tag{3}$$

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 [12].

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. Interested readers are referred to the topic of visible light probing [13]. 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 FA of single transistors down to 10 nm technologies [14].

[1] When using a coherent light source, EOP is typically called laser voltage probing (LVP), and EOFM is called laser voltage imaging (LVI).

III. Optical Probing Formulation

A. Single transistor

As explained in Section II, OP works based on the modulation of incident light upon transistors. A change in reflected light majorly stems from a change in carrier concentration in a transistor based on the applied voltage. The reflected light intensity (E) from a die area under a laser spot can be written as $\sum_{-r_{spot}}^{r_{spot}} E_r$, where r_{spot} and E_r denote radius of the laser spot, and the intensity of all reflected photons, respectively. The reflected light's intensity has various components. Each component stems from a different region of a transistor. The source of these reflected lights can be either static or dynamic. We are interested in the dynamic (modulated) component of the reflected light. The modulated portion of the reflected light is caused by an applied voltage to the transistor's terminals. This applied voltage reflects the data processed by the device and is of interest for the attacker. In [15], it is shown that the probed voltage from a transistor's terminal has approximately a linear relationship with the applied voltage. Hence, we can formulate the reflection caliber value (RCV) of a transistor's active region as follows:

$$RCV = V \times K \times \beta \times P_L \int_0^{2\pi} \int_0^{r_{spot}} p(r) \times A(r, \theta)\, dr d\theta \quad (4)$$

Parameter $A(r, \theta)$ in equation 4 denotes the area of each active region of the transistor in polar coordinates, where r is the radius and θ is the angle. $p(r)$ represents the laser's spread function (see equation 3). V denotes the present voltage at a region of the transistor. P_L denotes the magnitude of laser power. Parameter K is a fabrication-related constant. This is due to the fact, that the gate region and source/drain region have some overlap regions. These overlap regions can cause an interference between modulated signals generated by the drain and gate regions. At these overlapping areas, there are modulated signals that are racing with each other and the resultant signal can cause a positive or negative amplification signal [15]. Moreover, K also includes 180° phase shift of photons due to reflection off the metal contacts. The value of K_p for PMOS is larger than the value K_n for NMOS ($1.3K_n < |K_p| < 1.5K_n$). K_p and K_n have a negative and positive sign, respectively [15].

The β index is a function of the space charge region's (SCR's) depth (d_{SCR}), the doping concentration (N), the mobility (μ), and the structure of the device (ST). β is different for each region of the transistor. As shown in Fig. 1, if a transistor is biased in saturation region, the SCR's depth around source is much smaller compared to the drain region. Basically, β describes the traverse path of photons through different regions of the transistors. Moreover, β depends on the structure of the transistor as well; for FD-SOI transistors, the laser power (P_L) must be low to extract fathomable results due to existence of a buried oxide layer in the beam's path [16].

Building on the definition of the RCV for a single active region, we can define it for an entire transistor as follows:

$$RCV_{FET} = RCV_D + RCV_S + RCV_G + e^{-N} \times RCV_{Bulk} \quad (5)$$

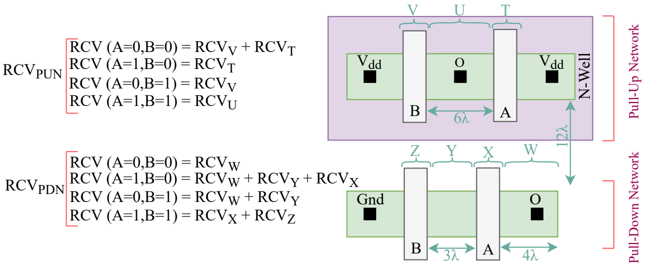

Fig. 2. Input dependency of reflected light of a CMOS NAND2 under OP analysis. V, U, T, Z, Y, X, W denote transistor regions contributing to light reflection based on the applied input values; A and B are inputs of the gate; λ is a design rule parameter equal to the half of the minimum drawn transistor channel length [17].

In equation 5, N is the well doping concentration and D, S, G, and $Bulk$ denote drain, source, gate, and bulk of the transistor, respectively. The last term in equation 5 shows that the contribution of the bulk voltage to the intensity of the reflected light is much higher in lightly-doped transistors [15].

B. Expanded formulation on a logic gate

Previously, we formulated the RCV of a single transistor and have shown that different regions of the transistor contribute to its RCV. Since a logic gate consists of multiple transistors, the gate's RCV is influenced by several transistors, depending on the applied input values. In other words, different combinations of the gate's input values cause different regions of the transistors to contribute to the reflected light. Consequently, the RCV of a logic gate can be written as follows:

$$RCV_{Log.Gate} = \sum_{\forall t \in Log.Gate} \sum_{i \in \{D,S,G,Bulk\}} RCV_{ti} \quad (6)$$

In equation 6, RCV_{ti} is the RCV of contributing regions i of a transistor t under the applied input values. As shown in Fig. 2, equation 6 is applied to a CMOS NAND2 gate when the laser is centered on the pull-down network (PDN) and centered on the pull-up network (PUN) and is only covering one region at a time. It can be seen that based on different applied input values, the $\text{RCV}_{\text{Log.Gate}}$ changes. Hence, to hide information from OP, a circuit must be designed as such to have a constant $\text{RCV}_{\text{Log.Gate}}$ regardless of the applied input values.

IV. Circuit Design Techniques Against Optical Probing Attacks

From equations 4 and 5, it can be inferred that two fundamental approaches can be taken to perturb OP attacks; 1) manipulating the transistors' fabrication parameters, and 2) utilizing circuit design techniques. In this paper, however, we will only focus on circuit design techniques.

A. Differential Logic Styles

When wiring transistors to implement a circuit, three different wirings are possible: 1) NMOS or PMOS transistor is controlled by an input signal (i.e., pseudo NMOS Inverter shown in Fig. 3(a)); 2) both NMOS and PMOS transistors (complementary transistors) are controlled by a single input signal, e.g., a CMOS Inverter as shown in Fig. 3(b)); 3) having complementary transistors controlled by complementary input signals, e.g., a CMOS differential Inverter gate as shown in Fig. 3(c)). The latter two transistors' wirings are sufficient to decrease the SNR of the reflected light upon OP. In principle, placing complementary transistors that are controlled by the same signal can be utilized to reduce the SNR of the reflected light ($K_p \sim -K_n$). However, due to strict layout design rules, complementary transistors can not be juxtaposed. Furthermore, the resulting light modulation amplitudes for NMOS and PMOS transistors are different ($|K_p| = 1.3|K_n|$). Hence, reflection cancellation due to complementary transistors can not be incorporated as a robust countermeasure against OP. Consequently, the best possible wiring to reduce the SNR of the reflected signal is to have both complementary transistors and complementary input signals. This wiring is the equivalence ofDRL-style gates. DRL utilize both signal and its complement for performing logical operation to produce output and output complement values [18]. This feature of DRL can be used to obfuscate information leakage from OP.

In DRL, the diffusion region of the NMOS or PMOS transistors in their respective wells can be juxtaposed. As a result, due to the limited resolution of FA tools, it becomes harder for an attacker to distinguish which transistor is carrying the information. In other words, upon each input switching, the amount of injected free carriers in transistors stays constant, regardless of the input values. This can be seen by expanding equation 6 on a DRL gate. As a result, in theory, the reflection and refraction indices do not change. As an example, consider a DCVSPG NAND2-AND2 gate as shown in Fig. 4. This gate uses both signals and their complement in the PDN. This means that the layout of the PDN can be designed as such that regions carrying complementary signals are juxtaposed.

Evaluation of the DRL family against OP. To evaluate how well DRL hides information from the adversary, we propose a metric called *complementary active regions differentiability (CARD)*. CARD is defined as a ratio between the distance of the edge of two modulated regions driven by complementary signals in an n-/p-well (W_c) to the optical resolution (R):

$$CARD = \frac{W_c}{R} \tag{7}$$

CARD demonstrates the complexity of OP analysis. If this value is greater than "1", it is easy for the adversary to distinguish active regions of each transistors. We compared a DRL NAND2-AND2 which is shown in Fig. 4 with a NAND2 concealed with two Inverter gates from [8] in Table I. Our differential gate shows a superior information obfuscation capability (more than 5× of the concealing-gate technique). In Table I, CARD$_{\text{min}}$ and CARD$_{\text{max}}$ stand for CARD value with minimum and maximum distance ($W_{c_{min}}$ and $W_{c_{max}}$ are shown in Fig. 4) between adjacent modulated areas which are driven by complementary signals, respectively.

TABLE I
CARD VALUE COMPARISON OF NAND2 GATE CONCEALED WITH TWO INVERTERS AND DIFFERENTIAL NAND2-AND2 DCVSPG LOGIC GATE UNDER A LASER WITH A RESOLUTION OF R = 865 NM.

Technology Node (nm)	CARD$_{\text{min}}$ [8]	CARD$_{\text{min}}$ ours	CARD$_{\text{max}}$ [8]	CARD$_{\text{max}}$ ours
90	0.780	0.208	1.561	0.312
45	0.390	0.104	0.780	0.156
32	0.277	0.074	0.555	0.111
22	0.191	0.051	0.382	0.076

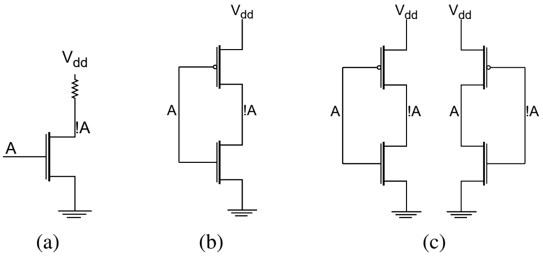

Fig. 3. Three possible wirings of transistors to perform any logical operation.

B. Careful layout design

A careful layout design can help the circuit to have less parasitic capacitances and lower power consumption. According to the equation 4, by minimizing the area of diffusion regions, the RCV can be reduced as well. According to design rules [17], merging diffusion areas results in $\frac{1}{4}A_{orig} \leq A_{merged} \leq \frac{1}{2}A_{orig}$. Based on equation 4, by merging diffusion areas the overall area is reduced, and RCV consequently decreases. Thus, the SNR of the reflected signal is compromised. Moreover, having a balanced layout[2] for differential trees of DRL logic in terms of complementary diffusion areas is necessary. This helps reducing the SNR of the reflection.

C. Supply voltage reduction

Supply voltage reduction results in power consumption reduction at the cost of a higher delay. Lowering the supply voltage results in transistors entering near-threshold voltage (NTV) or subtheshold voltage (STV) regions. According to equations 1 and 2, the lower the applied voltage is, the lower the reflected light's amplitude becomes. Hence, extracting information from a circuit will become harder due to the reduction of the reflected light's SNR. However, measures must be taken not to let an adversary increase the supply voltage at her will.

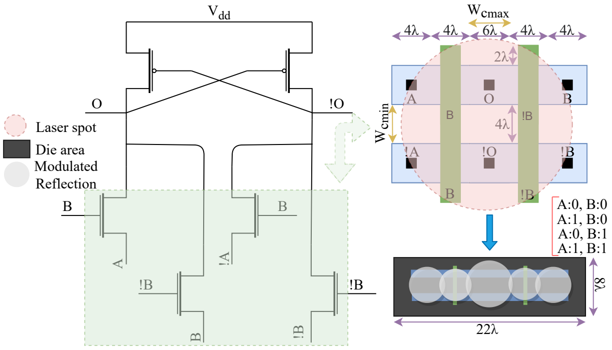

Fig. 4. (a) DRL NAND2-AND2 gate from DCVSPG logic family under OPA, (b) layout of pull-down network for this differential NAND2-AND2 logic.

[2] Balanced layout means that both branches of a DRL gate have an equal contribution to the RCV. This means that both branches of DRL have a similar layout, or they have equal active areas contributing to the RCV.

TABLE II

PERFORMANCE AND OP ROBUSTNESS OF VARIOUS LOGIC STYLES.

Logic	G	Performance			Security									
		A	D	P	OS	IS	M	DRL	BL	CARD_{min}	CARD_{max}	RCV_{diff}		
												PDN	PUN	Both
CMOS	INV	L	L	M	1.2	0.6	✓	✗	✗	∞	∞	12.85	15.03	13.85
	ND2	L	L	M					✗	∞	∞	22.59	43.98	29.10
NTV CMOS	INV	L	H	L	0.5	0.25	✓	✗	✗	∞	∞	5.37	10.77	5.77
	ND2	L	H	L					✗	∞	∞	9.41	14.38	12.12
STV CMOS	INV	L	VH	VL	0.3	0.15	✓	✗	✗	∞	∞	3.21	4.70	3.32
	ND2	L	VH	VL					✗	∞	∞	5.65	8.63	7.27
CMOS w/ Limiter	INV	L	L	M	0.6	0.4	✓	✗	✓	∞	∞	4.04	7.21	9.33
	ND2	L	L	M					✗	∞	∞	22.27	41.47	26.17
Diff. CMOS	INV	M	L	M	1.2	0.6	✓	✓	✗	0.06	0.11	0.22	0.07	0.28
	ND2	M	L	M					✗	0.08	0.17	13.28	17.90	4.74
CNTL	INV	H	M	M	0.8	0.3	✓	✓	✓	0.11	0.17	0.03	0.08	0.39
	ND2	H	M	H					✗	0.11	0.11	47.56	0.09	96.83
SRPL	INV	M	M	M	1.2	0.3	✓	✓	✓	0.00	0.17	0.16	1.03	0.55
	ND2	M	M	M					✓	0.00	0.17	1.90	1.20	1.60
DCVS	INV	M	M	M	1.2	0.3	✓	✓	✗	0.06	0.11	0.22	0.07	0.28
	ND2	M	H	M					✗	0.11	0.17	12.74	1.63	13.54
DCVSPG	INV	M	L	M	1.2	0.3	✓	✓	✓	0.06	0.11	0.22	0.07	0.28
	ND2	M	L	M					✓	0.11	0.17	4.26	3.52	5.25
EEPL	INV	M	L	M	1.2	0.3	✓	✓	✓	0.00	0.17	0.16	1.40	0.78
	ND2	M	L	M					✓	0.00	0.17	0.48	1.12	3.46
MCML	INV	M	M	H	0.2	0.1>	✗	✓	✓	0.06	0.11	0.12	0.03	0.21
	ND2	M	M	H					✗	0.11	0.17	5.71	0.40	4.38

STV: subthreshold voltage, **NTV**: near-threshold voltage, **diff. CMOS**: differential CMOS, **CNTL**: CMOS nothreshold logic, **SRPL**: swing restored pass-transistor logic, **DCVS**: differential cascode voltage switch, **DCVSPG**: differential cascode voltage switch with pass-gate, **EEPL**: energy economized pass-transistor logic, **MCML**: mosfet current mode logic; **A**: area, **D**: delay, **P**: power consumption, **OS**: output swing (V), **IS**: input threshold to change the output (V), **M**: minimum sized transistors design, **DRL**: dual-rail logic gate, **BL**: balanced layout; **(V)L**: (very) low, **M**: medium, **(V)H**: (very) high

D. Limiting the output swing

Limiting the output swing results in encoding logical ”1” and ”0” to voltage values different from the supply voltage and 0 V, respectively. It also results in always having a voltage on the drain of the output transistors. For instance, upon transition from logical 1 $\rightarrow$ 0, OP analysis still sees a modulation on the transistor, because ”0” is encoded in, for say 300 mV, which causes the transistor to be slightly on. While keeping the transistor slightly on, injected carrier concentration under gate and the modulation of SCR’s depth of drain and substrate contribute to the light reflection upon OP. Consequently, the transistors carrying ”0” contribute to the light modulation, which results in information obfuscation. Limiting the output swing comes at the cost of lowering the noise margin.

V. INVESTIGATION OF POTENTIAL LOGIC STYLES AND CIRCUIT DESIGN TECHNIQUES

We examined several logic gates and design techniques in terms of performance and security merits that can be used to alleviate OP attacks. We only evaluated non-clocked logic gates, because dynamic logic families suffer from various problems in deep submicron technologies [19], e.g., charge leakage, charge sharing, etc. The performance and security merits of the candidate non-clocked logic families are presented in Table II. It must be noted that “diff. CMOS” and “CMOS w/ Limiter” in Table II represent the differential formation of conventional CMOS gates (having both CMOS NAND2 and CMOS AND2 next to each other) and CMOS NAND2 logic gate with limiter circuitry to limit the output swing, respectively. In this work, we only considered Inverter (INV) and NAND2 (ND2) gates from each logic family. All the logic gates are simulated using Cadence Virtuoso tool using the NCSU-45nm technology [20]. The supply voltage and the maximum achievable swing are both 1.2 V in this technology.

A. Performance Evaluation

We compared the performance results in Table II qualitatively. In Table II, A, D, and P stand for occupied area on chip, delay, and power consumption, respectively. Among all the variants of CMOS logic in the table, CMOS logic and its limited output swing variant logic gates have similar performance in terms of delay. In contrast, the limited output swing variant logic gates suffer from leakage current. Also NTV CMOS and STV CMOS gates sacrifice the speed and noise margin for lower dynamic power consumption and higher security. Moreover, all the listed differential logic families have degraded performance in comparison to CMOS logic gate (except diff. CMOS logic gate). Generally, they have higher delay, higher power consumption, and occupy more area in comparison to conventional CMOS gates.

B. Security Evaluation

The OP security metrics shown in Table II are the ones discussed in Section IV; design with minimum size , DRL, output swing, input sensitivity, CARD values, and RCVs. In the table, RCV_{diff} means the maximum difference of the $\text{RCV}_{Log.Gate}$ evaluated for all input value combinations of the logic gate. The smaller the RCV_{diff} is, the better a gate can obfuscate information from OP. Based on these metrics, we can choose candidate logic styles that can be used to design OP robust circuits. The ideal robust circuit has a limited output swing, a low supply voltage, a balanced layout, a low CARD value, and an RCV_{diff} of 0. These qualifications compromise the SNR of the reflected light as much as possible on a circuit design level and therefore contribute to information obfuscation from OP.

The adversary can easily read out the state of CMOS logic and its variants because no region carries the complementary signal in the same well. For this reason, the CARD value for single-ended logic gates is ∞. To have both good performance and security, we can use differential CMOS logic. It has a similar performance in terms of speed like conventional CMOS logic gates, but it is differential. Hence, it results in a low CARD value. Furthermore, among all the variety of logic gates listed in Table II, EEPL, SRPL, DCVSPG logic gates have tolerable performance in comparison to the CMOS logic gates, but at the same time, these logic families are differential. This means that they have low CARD values.

In addition to use logic gates with low CARD values to achieve robustness against OP, we analyzed the RCVs as described in Section III-B. In this regard, we simulated a parked laser spot on the center of the PDN, the PUN, and in the middle of these two regions to cover them both. We modeled the logic gates as polygons, and based on the applied input values to the gates, only a subset of the polygons contribute to the modulation. Furthermore, we assumed a fabrication-related constant K for PMOS as $K_p \times \beta = -1.3$ and for NMOS as $K_n \times \beta = 1$) and a laser wavelength of 1300 nm and an NA of 0.75. The results show that using differential logic results in an RCV much smaller than for the single-ended logic gates. This means the reflection light from DRL is lightly dependent on the processed data. The reason why the RCV_{diff} is larger for some of the DRL gates is that their layout is not balanced. Consequently, one branch of the DRL's PDN or PUN contributes more to the reflected light (e.g., compare unbalanced layout NAND2 from DCVS, diff. CMOS, MCML, and CNTL families with balanced layout NAND2 of DCVSPG, SRPL, EEPL). Nevertheless, the small CARD value causes regions with complementary signals to be juxtaposed, and therefore, being harder to distinguish for the attacker. As a result, an attacker can not distinguish which transistor is contributing to the reflected light upon different applied input values. A CARD value of zero means that there exists a transistor in a logic gate whose gate and drain carry complementary signals.

Moreover, by reducing the applied supply voltage in NTV and STV CMOS, RCV_{diff} is reduced significantly. This means that designing DRL gates in NTV and STV can significantly help hiding information on the chip. Additionally, limiting the output swing has a similar effect on the RCV of a logic gate. From Table II can be deduced that logic gates with limited output swing result in smaller RCV differences upon each input state (compare RCV_{diff} of CMOS and CMOS with Limiter). The reason is that when a logic gate has a limited output swing, upon each input transition, both NMOS and PMOS modulate the incoming light under OP analysis. In contrast, in the case of a conventional CMOS Inverter gate, upon the input transition $0 \rightarrow 1$, only the NMOS drain's SCR contributes to the modulation of the reflected light. Additionally, the internal nodes of the logic gate have a voltage that contributes to light reflection.

It is worth to mention, all DRL Inverter gates in Table II have balanced layout and have small CARD value. These features result in really low RCV_{diff}. This means, DRL Inverters can obfuscate information well.

C. Candidate Logic Styles and Circuit Techniques

Based on our security metrics and performance trade-offs of each logic style as shown in Table II, Differential CMOS, NTV CMOS, SRPL, DCVSPG, EEPL, and MCML logic can serve as good candidates for circuits robust against OP attacks. DCVS and CNTL are less suitable in terms of security and performance than the other DRL logic gates for more complex gates. Besides, it must be noted that all the logic families can be designed to operate in STV, NTV. Consequently, combining a DRL logic design with NTV or STV can even further compromise the OP attack. In other words, to reduce the SNR of the reflected light using circuit-level techniques, a combination of the circuit techniques listed in Section IV must be employed. Eventually, designing circuits using a DRL family can result in robust circuit toward OP and lower area on-chip in comparison to the single-ended logic families [21], creating a performance advantage.

VI. Summary and Conclusions

In this paper, we first formulated the reflection caliber of transistors and a logic gate under OP. Then we proposed several circuit-level countermeasures against OP attacks and evaluated their performance and security in simulations. We showed a circuit can become more robust toward OP by using DRL gates. To make a circuit even more robust toward OP, a circuit can be designed using DRL that operates in STV or NTV and has a limited output swing. Building on our results, we are planning to implement these logic gates in a test chip manufactured in a recent technology to expose them to a real attack. In this work, we only evaluated EOP. In our future work, we will investigate circuit design techniques against EOFM and LLSI as well.

Acknowledgments

The work described in this paper has been supported by the Deutsche Forschungsgemeinschaft (DFG – German Research Foundation) under the priority programme SPP 2253 – 439918011.

References

[1] H. Lohrke, S. Tajik, C. Boit, and J.-P. Seifert, "No place to hide: Contactless probing of secret data on fpgas," in *Cryptographic Hardware and Embedded Systems – CHES 2016*, B. Gierlichs and A. Y. Poschmann, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, pp. 147–167.

[2] S. Tajik, H. Lohrke, J.-P. Seifert, and C. Boit, "On the power of optical contactless probing: Attacking bitstream encryption of fpgas," p. 1661–1674, 2017. [Online]. Available: https://doi.org/10.1145/3133956.3134039

[3] 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," pp. 262–272, 2020.

[4] 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 *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, Aug. 2021, pp. 627–644. [Online]. Available: https://www.usenix.org/conference/usenixsecurity21/presentation/krachenfels

[5] T. Krachenfels, F. Ganji, A. Moradi, S. Tajik, and J.-P. Seifert, "Real-world snapshots vs. theory: Questioning the t-probing security model," in *2021 IEEE Symposium on Security and Privacy (SP)*, 2021, pp. 1955–1971.

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

[7] H. Shen, N. Asadizanjani, M. Tehranipoor, and D. Forte, "Nanopyramid: An Optical Scrambler Against Backside Probing Attacks," vol. ISTFA 2018: Conference Proceedings from the 44th International Symposium for Testing and Failure Analysis, pp. 280–289, 10 2018. [Online]. Available: https://doi.org/10.31399/asm.cp.istfa2018p0280

[8] M. T. Rahman, N. F. Dipu, D. Mehta, S. Tajik, M. Tehranipoor, and N. Asadizanjani, "Concealing-gate: Optical contactless probing resilient design," *J. Emerg. Technol. Comput. Syst.*, vol. 17, no. 3, Jun. 2021. [Online]. Available: https://doi.org/10.1145/3446998

[9] R. Soref and B. Bennett, "Electrooptical effects in silicon," *IEEE Journal of Quantum Electronics*, vol. 23, no. 1, pp. 123–129, 1987.

[10] 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 Transactions on Device and Materials Reliability*, vol. 7, no. 1, pp. 19–30, 2007.

[11] B. Niu, G. M. E. Khoo, Y.-C. S. Chen, F. Chapman, D. Bockelman, and T. Tong, "Laser Logic State Imaging (LLSI)," vol. ISTFA 2014: Conference Proceedings from the 40th International Symposium for Testing and Failure Analysis, pp. 65–72, 11 2014. [Online]. Available: https://doi.org/10.31399/asm.cp.istfa2014p0065

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

[13] C. Boit, H. Lohrke, P. Scholz, A. Beyreuther, U. Kerst, and Y. Iwaki, "Contactless visible light probing for nanoscale ics through 10 um bulk silicon," pp. 215–221, 2015, available Open Access publishedVersion at http://depositonce.tu-berlin.de/handle/11303/6402.

[14] M. von Haartman, S. Rahman, S. Ganguly, J. Verma, A. Umair, and T. Deborde, "Optical Fault Isolation and Nanoprobing Techniques for the 10 nm Technology Node and Beyond," ser. International Symposium for Testing and Failure Analysis, vol. ISTFA 2015: Conference Proceedings from the 41st International Symposium for Testing and Failure Analysis, 11 2015, pp. 52–56. [Online]. Available: https://doi.org/10.31399/asm.cp.istfa2015p0052

[15] 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.

[16] U. Ganesh, "Laser voltage probing (lvp) – its value and the race against scaling," *Microelectronics Reliability*, vol. 64, pp. 294–298, 2016, proceedings of the 27th European Symposium on Reliability of Electron Devices, Failure Physics and Analysis. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0026271416301986

[17] *MOSIS Service*. Design Rules MOSIS Scalable CMOS(SCMOS), 2009.

[18] e. a. Bernstein, Kerry, *High speed CMOS design styles*. John Wiley & Sons, Ltd, 1999.

[19] C. Cornelius, F. Grassert, S. Koppe, and D. Timmermann, "Deep submicron technology: Opportunity or dead end for dynamic circuit techniques," pp. 330–338, 2007.

[20] J. E. Stine and et.al, "Freepdk: An open-source variation-aware design kit," in *MSE*, 2007.

[21] H. Reyserhove and W. Dehaene, "A differential transmission gate design flow for minimum energy sub-10-pj/cycle arm cortex-m0 mcus," *IEEE Journal of Solid-State Circuits*, vol. 52, no. 7, pp. 1904–1914, 2017.