CONCEALING-Gate: Optical Contactless Probing Resilient Design

M. TANJIDUR RAHMAN, NUSRAT FARZANA DIPU, and DHWANI MEHTA,
University of Florida
SHAHIN TAJIK, Worcester Polytechnic Institute
MARK TEHRANIPOOR and NAVID ASADIZANJANI, University of Florida

Optical probing, though developed as silicon debugging tools from the chip backside, has shown its capability of extracting secret data, such as cryptographic keys and user identifications, from modern system-on-chip devices. Existing optical probing countermeasures are based on detecting any device modification attempt or abrupt change in operating conditions during asset extraction. These countermeasures usually require additional fabrication steps and cause area and power overheads. In this article, we propose a novel low-overhead design methodology to prevent optical probing. It leverages additional operational logic gates, termed as "CONCEALING-Gates," inserted as neighbor gates of the logic gates connected to the nets carrying asset signals. The switching activity of the asset carrying logic is camouflaged with the switching activity of the concealing-gate. The input signal and placement in the layout of the concealing-gates must be selected in such a way that they remain equally effective in preventing different variants of optical probing, i.e., electro-optical frequency mapping and Electro-optical probing. The methodology is suitable for the existing ASIC/FPGA design flow and fabrication process, since designing new standard logic cells is not required. We have performed a comprehensive security evaluation of the concealing-gates using a security metric developed based on the parameters that are crucial for optical probing. The attack resiliency of the logic cells, protected by concealing-gates, is evaluated using an empirical study-based simulation methodology and experimental validation. Our analysis has shown that in the presence of concealing-gates, logic cells achieve high resiliency against optical contactless probing techniques.

CCS Concepts: • **Security and privacy** → Hardware reverse engineering; **Hardware attacks and countermeasures**; *Hardware security implementation*; *Tamper-proof and tamper-resistant designs*; **Hardware attacks and countermeasures**; *Embedded systems security*; **Hardware attacks and countermeasures**; **Embedded systems security**; Hardware reverse engineering;

Additional Key Words and Phrases: Backside protection, hardware security, logic locking, optical probing

ACM Reference format:
M. Tanjidur Rahman, Nusrat Farzana Dipu, Dhwani Mehta, Shahin Tajik, Mark Tehranipoor, and Navid Asadizanjani. 2021. CONCEALING-Gate: Optical Contactless Probing Resilient Design. *J. Emerg. Technol. Comput. Syst.* 17, 3, Article 39 (June 2021), 25 pages.
https://doi.org/10.1145/3446998

Authors' addresses: M. T. Rahman, N. F. Dipu, D. Mehta, M. Tehranipoor, and N. Asadizanjani, University of Florida, FL; emails: {mir.rahman, ndipu, dhwanimehta}@ufl.edu, {tehranipoor, nasadi}@ece.ufl.edu; S. Tajik, Worcester Polytechnic Institute, MA; email: stajik@wpi.edu.

1550-4832/2021/06-ART39 $15.00
https://doi.org/10.1145/3446998

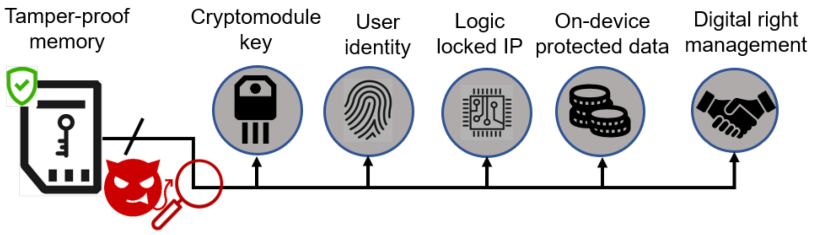


Fig. 1. Key extraction during the key transfer between the secure memory and key-protected modules.

1 INTRODUCTION

The ubiquitous modern-day technologies for applications, ranging from low-power computing devices to automated vehicles to internet-of-things, are made viable due to the advent of **System on Chips (SoCs)**. The sheer complexity in design, faster yield analysis, and defect localization have catalyzed the formulation of different **integrated circuit (IC)** debug and **failure analysis (FA)** techniques and tools. The existence of several metal layers on the frontside of the IC and new packaging technologies, such as **ball grid arrays (BGA)** and flip-chip technologies, resulted in a paradigm shift in the world of failure analysis. As a result, over the past two decades, there has been a significant advancement in FA and defect localization in ICs through chip backside using optical techniques, such as optical probing and its derivatives [12, 28, 48]. **Electro-Optical Probing (EOP)** and **Electro-Optical Frequency Mapping (EOFM)** are examples of optical probing techniques, where the electric field in the device modulates the photons injected by a laser from the chip backside. Since the bulk silicon at the backside of the ICs is transparent to the near-infrared photons, these "contactless" optical probing methods have facilitated functionality analysis and defect localization to predict the root-cause analysis of transistors and logic gates failure.

While these techniques have been initially developed for FA, it has been shown that an adversary can also misuse the FA's tools to violate the confidentiality, integrity, and availability of the hardware through physical attacks [19, 21, 22, 33, 41]. Security features in SoCs have evolved to cope with physical attacks. For instance, tamper-proof memories, such as physical unclonable functions, flash, EEPROM, have been proposed as a secure key-storage to protect the hardware secrets from invasive and semi-invasive attacks. Moreover, researchers have proposed security measures, e.g., protective shield, charge sensors, and opaque layers, to safeguard the SoC assets [6, 26, 30]. However, all these countermeasures are based on a common assumption that device modification, for instance, backside polishing, or **focus ion beam (FIB)** editing, is always necessary for optical attacks. The security designers have consistently underestimated the capability of the modern FA tools and techniques. Optical probing enables an adversary to steal the chip secrets, such as cryptographic keys, user identity, data encryption keys, and logic locking key, without triggering any alarm implemented in the chip. Furthermore, in the case of flip-chip packaging, which is widely used for most SoCs, optical probing can be performed in a non-invasive manner, i.e., without polishing the bulk silicon. Though the tamper- and read-proof memory may protect the assets in a powered-off device, the capability of optical probing techniques lies in the fact that they can probe either combinatorial or sequential logic elements [23, 33, 41] connected to the protected memory and extract the assets during its transfer from the memory (see Figure 1).

Several preventive and detection-based approaches have been already proposed to protect against optical attacks at different levels: packaging, device, and circuit. For example, at the device-level, an active optical layer is coated on the die backside [2]. In this case, reflection from protective layers due to photons emitted from the light sources is monitored by the photon detector to identify any attempt of protective layer removal. Though this approach provides a general solution

against the backside attacks, it still requires costly steps to integrate the layers and detectors into the standard **complementary metal–oxide–semiconductor (CMOS)** circuits. Similarly to the protective optical layer, implementing metal layer and through-silicon vias [3, 9, 49] to prevent polishing and FIBing attempts also suffer from high manufacturing cost and area overhead. However, classical solutions such as silicon-based photo sensors cannot be used to detect optical probing attempts, since the thermal laser used in probing does not generate any electron-hole pairs. In this case, thermal sensitive circuits, e.g., Ring-oscillators, were used to capture abrupt temperature variations due to thermal laser [40]. However, such sensors suffer from a higher area and power overhead, as well as a high rate of false positive.

In summary, existing countermeasures are ad hoc and provide inefficient protection, and therefore, significantly undermine the capability of an adversary. Moreover, none of the current techniques are evaluated against the security metrics developed based on the physics behind optical probing, parameters related to standard logic cells, and capability of the optical probing tool, i.e., the **laser scanning microscope (LSM)**. Besides, the aforementioned solutions require additional process steps and resources (e.g., area and power) overhead. Instead of adding new manufacturing steps, in this article, we propose a standard logic cell-based preventive approach to hide the state or stored bit in a logic gate and register. We have used conventional **application-specific integrated circuit (ASIC)** design flow to identify security-critical circuits and careful placement of additional CMOS logic gate with selective input to obscure the asset carrying gates activity. We call this additional logic gates as "Concealing-Gate" in the rest of the article. The primary contributions of this research are as follows.

(1) We propose a preventive approach using a careful selection of combinatorial and sequential logic gates, their inputs, and placement to camouflage the activity of the asset carrying logic elements. This approach will compel an adversary to focus on full-blown reverse engineering and extract the full functionality of IPs for each logic gates, and hence significantly increasing the time-cost of optical probing attack.
(2) A security metric is developed to identify the vulnerability of security-critical combinatorial and sequential logic gates against optical probing attacks. This metric estimates the time-cost required for launching the electro-optical analysis by an adversary.
(3) Instead of proposing a new standard cell, integration of new layers, or modification in packaging techniques, the proposed method uses the existing design ASIC flow. The proposed approach is evaluated using a simulated-based approach, and later validated with experimental analysis performed on a 28-nm FPGA by a common LSM.

2 BACKGROUND

2.1 Optical Contactless Probing

Optical contactless probing is a contactless IC FA technique from the chip backside. Contactless interaction with the transistor requires much less effort than contact-based counterparts, e.g., electrical probing and circuit editing with FIB. In optical contactless probing, the logical state of a sequential and combinatorial logic is identified based on the interaction between the laser and transistors. The varying electric field and free carrier density due to switching of the applied voltage in the transistors modulate the amplitude and phase of the photons, reflected from different interfaces of the device, e.g., active region, oxide, and interconnects [16–18, 50]. However, the effect of free carrier density, ΔN_e and ΔN_h, is dominant for 1.3-μm laser, which is used in the most modern-day optical probing. The variation in absorption coefficient, $\Delta\alpha$, and the

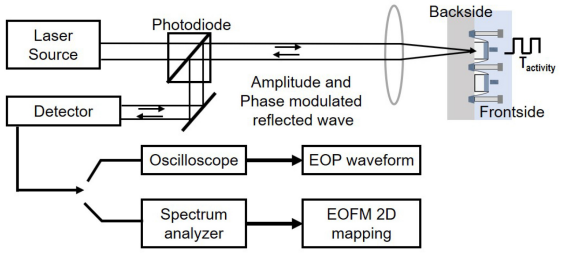


Fig. 2. Simplified illustration of contactless optical probing signal acquisition.

index of refraction, Δn, depend on free carrier density, which can be defined as [39]

$$\Delta n = \frac{\lambda^2 q^2}{8\pi^2 {c_0}^2 \epsilon_0 n_0} \left[\frac{\Delta N_e}{m_e} + \frac{\Delta N_n}{m_h} \right] \tag{1}$$

and

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

where q, λ, c_0, and ϵ_0 represent the charge of the carrier, laser wavelength, speed of light, and permitivity of the free space, respectively. m_e, m_h are the effective mass of the electrons and holes, respectively. The carrier mobility, μ, is a function of the temperature.

A photo-diode converts the modulated photons reflected from the device into an electrical signal (see Figure 2). Depending on the nature of measurement, i.e., EOP or EOFM, the electrical signal is fed to a digital sampling oscilloscope or spectrum analyzer. In EOP measurement, the oscilloscope averages the collected electrical signal and synchronizes it with a trigger signal to create a time-domain waveform of the related voltage in the transistor [14, 15]. While EOP focuses on a single transistor, in the case of EOFM, the laser scans the **region of interest (RoI)** on the device and the reflected light is fed into a spectrum analyzer acting as a narrow band frequency filter. Therefore, EOFM synthesizes an activity mapped image of the RoI operating at the frequency set in the spectrum analyzer.

2.2 Reverse Engineering

Reverse engineering can be interpreted in different ways in the context of hardware security. In this work, we make a distinction between *full-blown* and *partial* reverse engineering. The full-blown reverse engineering focuses on analyzing the internal structure and implementation of the device. The objective of full-blown reverse engineering is to extract the functionality of the device [5, 32].

However, obtaining information about the operation and functionality of the chip without exposing the RTL netlist is defined as partial reverse engineering. Side-channel leakages, such as electromagnetic radiation, power leakage, and photon emission, reveal sensitive information about chip operation and functionality.

2.3 Tamper- and Read-Proof Memory

The existence of a tamper- and read-proof memory is the primary assumption in all key-based security primitives, such as cryptomodule, secure boot-up, digital right management, and logic locking. There are memory technologies where it is tough to read the content, even with the most sophisticated FA tools, if no electrical interface is available to the outside world. A conventional example of such memory is the flash/EEPROM technology, where measuring the trapped charges in the floating gate of transistors is not a straightforward task [8]. In contrast to flash/EEPROM

memories, other NVM technologies, e.g., eFuses, battery-backed RAMs, and ROM, are more susceptible to direct readout [24, 31].

However, regardless of the tamper-resiliency and security of the memory itself, the transmission of data from/to the memory still leaves the door open for an adversary to probe or tamper with the content of the memory, as shown Figure 1. An adversary with FA capability can localize and probe the buffers and registers, responsible for the movement of security-sensitive data. Naturally, established countermeasures, such as memory encryption and authentication, are also not sufficient, since these solutions still require a secure memory to store encryption/authentication keys. Consequently, it is not sufficient to assume the existence of secure storage, ensures the security of the key.

2.4 Logic Locking

Logic locking or logic obfuscation is a mechanism to hide the functionality of an IP by inserting additional logic gates into the netlist of IP. In logic locking, additional combinational or sequential logic gates are embedded into the design. The extra embedded logic gates are known as *key-gates*, which are connected to *key*, fed through a set of *key-registers*. The key-gates and key-registers comprised the key-delivery unit, a core-component of logic locking [31, 33]. The functionality of the chip/IP is unlocked once the correct sequence of the key is available at the input of the key-gates, hence, making the chip/IP inoperative for an unauthorized user or adversary. Logic locking is a classical example where the locking key is protected in a tamper-proof memory. Outside the tamper-proof memory, the key travels through the key-delivery unit and interconnects.

3 OPTICAL CONTACTLESS PROBING

In this section, we present the attack approach using EO techniques. the optical probing signal source, analysis approach and relevant parameters are also discussed.

3.1 Attack Approach

During the physical attack, the ultimate goal of an adversary is to acquire the chip assets with minimum perturbing in the device. Therefore, the attacker may use the following steps to extract the target asset form the device,

3.1.1 Localizing the Point of Interest. An adversary requires physical access to the **device under attack (DUA)** to extract the asset with optical probing. She needs to identify a suitable combinatorial or sequential logic, which is termed as **point-of-interest (PoI)**, for probing the asset. She can identify the location of PoI using full-blown or partial reverse engineering. Without access to GDSII or netlist of the chip, automated delayering and imaging tool, invasive full-blown reverse engineering for functionality and connectivity extraction is an expensive, human labor intensive, and error-prone process. The objective of an unscrupulous entity, without access to GDSII, is fast asset extraction. Therefore, she most likely to rely on a non-reverse engineering approach or partial reverse engineering. In a non-reverse/partial reverse engineering approach, an adversary can easily localize the non-volatile memory, cache, and ASIC, if she has access to a LSM, photon emission microscope, and/or optical image of the die [42, 44]. Such a localization approach is faster and less expensive than a full-blown reverse engineering approach. This is most probably the most threatening attack scenario, where a single entity can rage a war against all the key-based security implementation of the device. For logic locking, the key-delivery unit can be optically probed to extract the locking key [31]. Therefore, she can localize the key-registers and key-gates in a similar approach described in Reference [33].

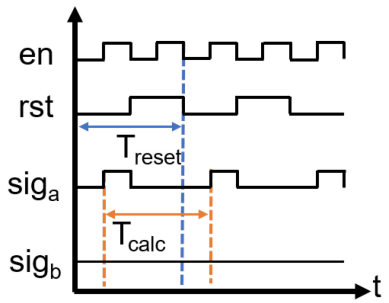


Fig. 3. Waveforms of the enable (en), reset (rst), and two input signal (sig_a and sig_b). The input signal, sig_a, provides bit "1" and the input signal, sig_b, provides bit "0" to the connected gates/registers.

3.1.2 Optical Probing Measurement. In this section, we discuss the EO signal measurement approach during contactless probing. The optical probing measurement for either EOP and EOFM can be explained with the waveform shown in Figure 3. Two signals, sig_a and sig_b are acting as input bit "1" and bit "0" to registers *A* and *B*, respectively. The reset signal is depicted with the waveform rst. sig_a starts at the logic level low and then changes its state, as soon as the time needed for the preceding calculation (T_{calc}) has elapsed. The rst signal resets the registers with a time period of T_{reset}. As the time period for each consecutive power-on is constant, the time period for T_{calc} is equal to the time period of T_{reset}. Since sig_a switches at the frequency of reset signal, the registers (to be specific transistors) connected to sig_a also experience a change in the free carrier density and modulate the laser focused on the registers. Therefore, feeding the modulated signal to spectrum analyzer, a frequency domain two-dimensional (2D) EOFM activity mapping can be generated. Similarly, feeding the modulated signal along with the rst signal to oscilloscope, instead of spectrum analyzer, a time domain waveform can be generated that is known as EOP signal. The rst signal acts as a reference signal for EOP analysis. Unlike sig_a, sig_b does not change its status with reset signal, hence does not affect the outcome of EOP/EOFM measurement.

3.2 Influential Elements in Optical Probing

In this section, we discuss the elements that influence the optical probing evaluation and performance of the LSM during optical contactless probing.

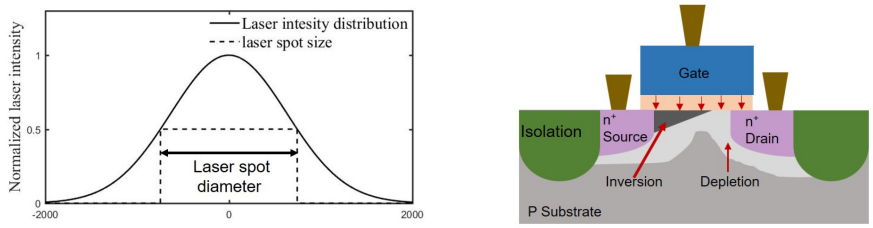
3.2.1 Optical Resolution. Optical resolution is the minimum distance required to distinguish between two point-source through any optical system [4]. According to Abbey's criterion, optical resolution, *R*, of any diffraction-limited microscope objective, which is also applicable for laser scanning microscope, is defined by [36]

$$R = \frac{\lambda}{2NA}, \tag{3}$$

where *NA* is the numeric aperture of the objective lens. Lowering the wavelength of laser or increasing the *NA* can significantly improve the resolution of the optical probing.

As the semiconductor industry scale down the technology nodes, the distance between the transistors and logic gates also reduces. Since in EOFM analysis, 2D mapping of two different logic gates activity requires distinguishable edges between two logic gates/transistors, reaching the limit to optical resolution impact the EOFM measurement.

3.2.2 Laser Properties. Laser wavelength, spot size, and intensity distribution play an important role in the optical probing analysis. *Laser Wavelength:*. The influence of the wavelength on the



(a) (b)

Fig. 4. (a) Gaussian distribution of the laser intensity profile. The diameter of the laser spot size is defined at the full width half of the maximum intensity [20]; (b) different space charge region in MOSFET at saturation state.

Table 1. Optical Resolution and Laser Spot Size for Different Laser Wavelengths and Lens Used in LSM

lens	Numerical Aperture (NA)	Optical Resolution (nm)		Laser Spot Size (nm)	
		λ = 1,300 nm	λ = 1,064 nm	λ = 1,300 nm	λ = 1,064 nm
20×	0.40	1,625	1,330	2,803	2,295
50×	0.76/1	855/650	700/532	1,476/1,121	1,208/918

absorption coefficient is a major concern for the measurement. Laser with higher energy than silicon bandgap ($\lambda < 1.1\ \mu$m) generates photo carriers in the silicon devices. This effect is widely known as photoelectric laser stimulation [30], which is responsible for injecting unintentional faults in the device. Hence, 1.3-μm lasers are mostly used in most industry-standard LSM. However, smaller wavelength lasers promise better resolution for optical probing (see Equation (3)) [22, 30].

Laser Spot Size. The reflected laser response during EOFM/EOP measurement is influenced by all the transistors covered by the laser spot size. It is assumed, the laser intensity used for optical probing follows the Gaussian distribution function. The diameter of the laser is defined at the full width at half maximum of the intensity of the laser (see Figure 4(a)), which is equal to the diameter of the Airy disk, D_{airy} [36],

$$D_{airy} = \frac{1.22\lambda}{NA}. \tag{4}$$

In confocal microscopy, the spread of the laser beam is further reduced by $\sqrt{2}$. Therefore, the spot size of the probing signal is [20, 36]

$$D_{spot\ size} = \frac{1.22\lambda}{\sqrt{2}NA}. \tag{5}$$

Table 1 presents the optical resolution determined from Equation (3) and the laser spot size calculated from Equation (5) for two different widely used lens (20× and 50×) in state-of-the-art LSM.

The reflected laser is modulated not only by the transistor or logic gate on which the laser is focused. The intensity of the reflected laser is a complex sum of intensity modulation caused by each logic gates under the laser spot. Hence, the EOFM and EOP measurements can significantly differ from the expected outcome. The intensity of the reflected modulated photons can be represented

in a simplified way,

$$I_{total} = \sum_{x=-D_{spot\ size}/2}^{D_{spot\ size}/2} I_x, \tag{6}$$

where I_x is the reflected modulated laser intensity. The intensity of the reflected laser is dependent on the node size, operating voltage, and device terminal, e.g., source/drain and gate, under laser spot. Such dependency of reflected laser modulation can be utilized to induce cross-talk during EOFM and EOP measurements. The intensity of the I_{total}, to some extent, can be maintained constant for the RoI, by keeping the free-carrier density stable and total number of switching in logic gates/transistors fixed.

3.2.3 Position of Laser Beam on Device. One of the major challenges in the optical probing signal acquisition is low SNR. The probing signal is acquired multiple times by running the device in a reset loop to mitigate low SNR. The laser modulation depends on the the laser beam position on the transistor, i.e., the drain, source, and gate region. The laser travels through different **space charge region (SCR)** depending on the area under the laser. For instance, in Figure 4(b), if the laser is focused on the drain of the transistor, the photons get modulated at the SCR-diffusion interface. Unlike the drain region, focusing the laser on the gate terminal allows free carriers in the inversion channel and depletion region to modulate the reflected laser [18].

CMOS standard cell contains complementary NMOS and PMOS transistor. The logic state of the cell can be extracted by focusing the laser on either PMOS or NMOS [1, 35]. The output waveform in the EOP signal is inverted to each other. In EOFM analysis, both PMOS and NMOS will appear as active nodes; however, the intensity of NMOS is higher than the PMOS transistors [1].

4 WIDTH OF CMOS GATES

Continuous shirking in technology node allows more transistors in the same area. Due to the bottleneck of optical resolution, the width and height of transistors in a chip have a significant influence on the end-result of EO measurement. For instance, the laser can be focused on a single logic gate for a larger technology node [18]. However, the same laser spot may cover multiple logic gates in smaller technology nodes. Therefore, the area of the transistors and logic gates, i.e., the height and width of the logic gates, is crucial for any circuit-based countermeasure.

The width of the logic gate, $W_{logic\ gate}$, can be defined as a multiplier of **contact gate pitch (CGP)** (also known as contact poly pitch or simply gate pitch), and metal pitch, respectively [10, 11, 27]. Therefore, the width of the logic gates can be defined as

$$W_{logic\ gate} = (n + 1) \times CGP, \tag{7}$$

where n is the number of poly gates in the logic cell. Figure 5 represents the width of INVERTER and NAND gate, where n is 1 and 2, respectively. From Equation (7) the width of the logic gates can be calculated for different technology nodes. The diffusion break width is $1 \times CGP$ for device implemented with double diffusion break FinFET technology [10, 47]. In half-pitch, $\lambda_{halfpitch}$, based design rule, the width of source drain is defined as $7\lambda_{halfpitch}$ and the spacing between the two diffusion can be defined as $4\lambda_{halfpitch}$ [37].

During EO-based attacks, the logic gate targeted for optical probing and neighbor logic gates under laser spot modulates the photons amplitude and phase (see Section 3.2.3 for detail). Therefore, the total logic gate width under laser spot facilitate in calculating the I_{total} in Equation (6). The total width, $W_{total\ Width}$, of the logic gates under laser spot can be expressed as

$$W_{total\ width} = W_{target\ cell} + \sum_{i=0}^{n} K_i \times W_{neighbour\ cell_i} + nW_{break}. \tag{8}$$

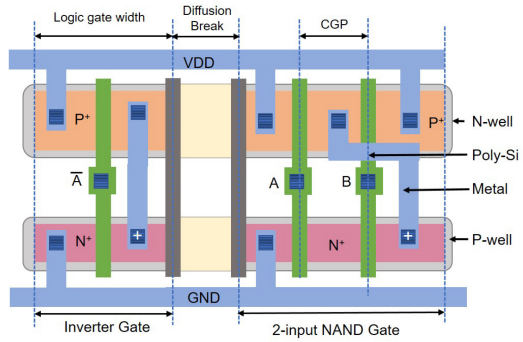


Fig. 5. Nominal logic gate width for an INVERTER gate and 2-input NAND gate.

Here, $W_{targetcell}$, $W_{neighbourcell}$, and W_{break} represent the width of target cell for optical probing, neighbor cell, and diffusion break, respectively. The maximum of total logic gate width under laser stimulation, $W_{totalWidth}$, is the diameter of the laser spot size. The width of the logic gates can be calculated from Equation (7) and $\lambda_{halfpitch}$-based design rules. K_i is the ratio of logic gate width covered by the laser spot and total width of the logic gate. The value of K_i can be less than or equal to 1 for the logic gates at the edges of the laser spot.

5 PROPOSED COUNTERMEASURE AND SECURITY EVALUATION

In this section, we present the threat model considered for the proposed optical probing countermeasure. The detail of optical probing countermeasure idea is also described here along with the security metrics considered for evaluating the protection mechanism's performance. The effectiveness of the proposed solution is evaluated against the logic locking scenario.

5.1 Attack Model

In logic locking, during the boot-up process, the key-delivery unit read the key value from the key-storage and, through interconnects, feed the key in the key-delivery unit, i.e., the key-registers and key-gates. An adversary can use optical probing to extract the key from the key-delivery unit, i.e., the key-gates and key-registers. Though the interconnects carry key signals, interconnects' contribution to optical modulation is negligible [18, 31]. Consequently, the interconnects are considered secured against electro-optical attacks. We assume an electrical probing protection mechanism is available in the DUA.

For a successful attack against key-protected security primitives, we assume the following information is available to the attacker. The adversary has access to an operational IC and knows the functionality of the chip. Second, the attacker has access to an optical probing system. In addition to that, she may need standard lab equipment, e.g., hotplate, logic analyzer, which are available in the market. We have assumed that the adversary is interested in partial/non-invasive reverse engineering to utilize the fast key localization approach.

5.2 Proposed Countermeasure

5.2.1 The Idea of Concealing-Gate. CMOS is mostly used in logic gates to implement complex Boolean functions in digital implemented circuits. Depending on free carrier density in the transistors, the ON/OFF state of the MOS device can be determined. At static condition, all inputs are held at some valid logic level, i.e., input signal switching $0 \rightarrow 0$ and $1 \rightarrow 1$, and the circuit is not switching its state. At this state, CMOS logic consumes static power. The leakage current is the primary

cause of static power consumption in the circuit. Consequently, the density of the free carrier in the MOS transistor does not change significantly. Therefore, the amplitude and phase modulation of photons are negligible. However, CMOS logic gates consume dynamic power when the input switches, i.e., switching from $0 \rightarrow 1$ and $1 \rightarrow 0$, at a high frequency. Charging and discharging of load capacitance in a logic gate acts as the source of dynamic power consumption. The charging and discharging of load capacitance affects the free-carrier density in the MOS transistor, hence modulating the reflected laser. Therefore, irrespective of the change in the logic state, i.e., the output of the CMOS gate, transition in the input signal ($0 \rightarrow 1$ transition and vice versa), modulates reflected photons. An adversary uses the modulated reflected laser to extract the time-domain and frequency-domain state of the logic gates.

Our objective is to hide the switching activity of the logic elements, connected with the key carrying nets, from optical contactless probing. The logic gates and registers connected to the key nets are the *target-logic gate* and *target-register* for an adversary. The switching activity of the target-logic elements can be concealed by introducing additional logic gates as neighbor cells. These additional neighboring logic gates are termed as "CONCEALING-Gate" throughout the article. The activity of the key-gates/registers can be camouflaged using the following two principles,

(1) **EOFM Concealing:** The EOFM activity of the target-logic gates are camouflaged if the concealing-logics/transistors and target-logics/transistors are placed at a lower distance than optical lens resolution. Therefore, the absence of EOFM activity due to the static state of target-logics/transistors, i.e., $0 \rightarrow 0$ due to reset operation, can be camouflaged by inducing dynamic state, i.e., $1 \rightarrow 0$ due to reset operation, in concealing-logics/transistors.
(2) **EOP Concealing:** In a certain time-frame, the amplitude of the EOP waveform can be maintained at a constant value if the integrated reflected photon intensity remains constant within a tolerable limit. This can be achieved by inducing cross-talk in the EOP waveform by turning ON concealing-logics/transistors when the transistors of the target-logic are operating at static state.

The aforesaid principle can only be fulfilled through the following conditions,

(1) EOFM Concealing:
    (a) *Frequency Matching:* The nodes operating at the center frequency of the low-pass filter in the spectrum analyzer, only appear in the 2D mapping of EOFM signal. Therefore, concealing-logics' switching frequency must be the same as target-logics' switching frequency.
    (b) *Switching Inputs:* The transistors connected to the input signal, switching $1 \rightarrow 0$ during reset operation, only appear in the EOFM signal. Hence, concealing-logic must be at the dynamic state when the target-logic is operating at a static state. Note that in EOFM mapping, the activity of NMOS transistors is more prominent than the PMOS transistors' activity.
    (c) *Distinguishable Edges:* Extracting the logical state of a transistor/logic gate from an EOFM measurement requires an understanding of the shape and distinguishable edges of active nodes [31, 36, 50]. In addition, EOFM measurement contains spatial information of an active node. Therefore, indiscernible EOFM activity edges of concealing- and target-logic/transistor improve the camouflaging of the key-gate/register activity. An abrupt change in the shape of concealing- and target-logic/transistor is also undesirable, since the change may be detectable through image processing and computer vision.

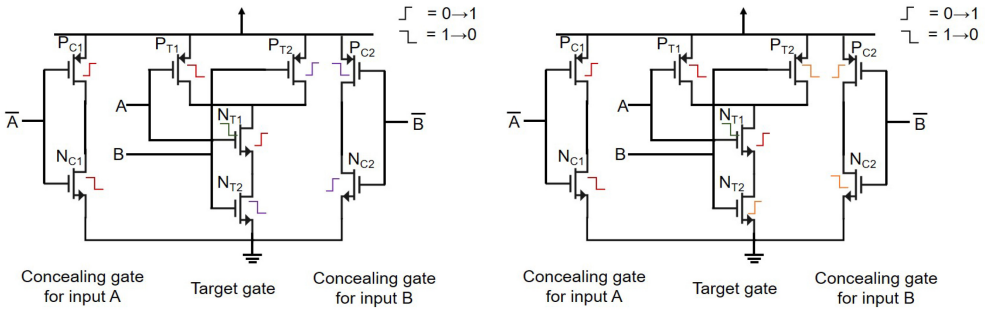


Fig. 6. Proof-of-concept implementation for concealing NAND gate activity. The concealing-gates are connected with the inverted input signal of the target-NAND gate. MOSFET input switching direction is (a) $A = 0 \rightarrow 1$ and $B = 1 \rightarrow 0$; (b) $A = 0 \rightarrow 1$ and $B = 0 \rightarrow 1$.

(2) EOP Concealing:
   (a) *Integrated Output:* Transistors'/Logic gates' contribution to the EOP signal is dependent on the free carrier density in the device. Therefore, the ON/dynamic state of the concealing-gates/transistors can contribute to the EOP signal, when the target-gates/transistors operate at OFF/static state, hence, impede the EOP signal to change its state. Therefore, alternating ON/OFF state of concealing- and target-logics/transistors facilitate in maintaining a similar free-carrier density.
   (b) *Reference Signal:* the trigger signal provided to the oscilloscope act as a reference signal for the time-dependent EOP waveform generation. The amplitude of the EOP output must be comparable to the reference signal output to camouflage the asset signal.

5.2.2 Selection of Concealing-Gate and Concealing-Input. As discussed in Section 3, the free carrier density of a logic gate varies with the transistors' switching activity. It is a well-known fact that the MOSFET current is a function of the inversion charge density. The charge density of two adjacent identical transistors, i.e., transistors with same width and length, operating at the matching drain/source/gate voltage can be considered identical. Therefore, between two transistors, total free carrier density can be maintained similar, if the poly-gate input voltage of the two transistors is inverted. This can be explained by the example presented in Figure 6(a). In Figure 6(a), the NAND gate and the INVERTER gate are assumed to be target-gate and concealing-gates, respectively. For input $A = 1$, the NMOS, N_{T1}, of NAND gate is turned ON, whereas the NMOS, N_{C1}, of the INVERTER operates at the cutoff region and vice versa. Therefore, the total free carriers on the area of the two NMOS transistors, N_{T1} and N_{C1}, can be considered constant within a tolerable limit. Applying the inverted target input signal to concealing-logic/transistor allows the transistors mentioned above to operate at the same switching frequency. In addition, one of the transistors must appear as an active node in the EOFM 2D mapping, since at least one of the transistors must switch from $1 \rightarrow 0$ during reset operation. Hence, the "frequency matching" and "switching inputs" conditions for EOFM concealing are fulfilled. Due to similar reason, either concealing-gate or target-gate act as the source of modulation of reflected photons and contribute to integrated EOP signal. Consequently, the EOP signal can be interpreted as "1" when compared with the reference signal. A security designer can choose INVERTER, NAND/NOR gate, to conceal the target-logic activity.

5.2.3 Concealing-Gate Placement in Layout. To mask the EOFM activity of the target-gate, the edges between the concealing- and target-logic/transistor need to be indistinguishable. Therefore,

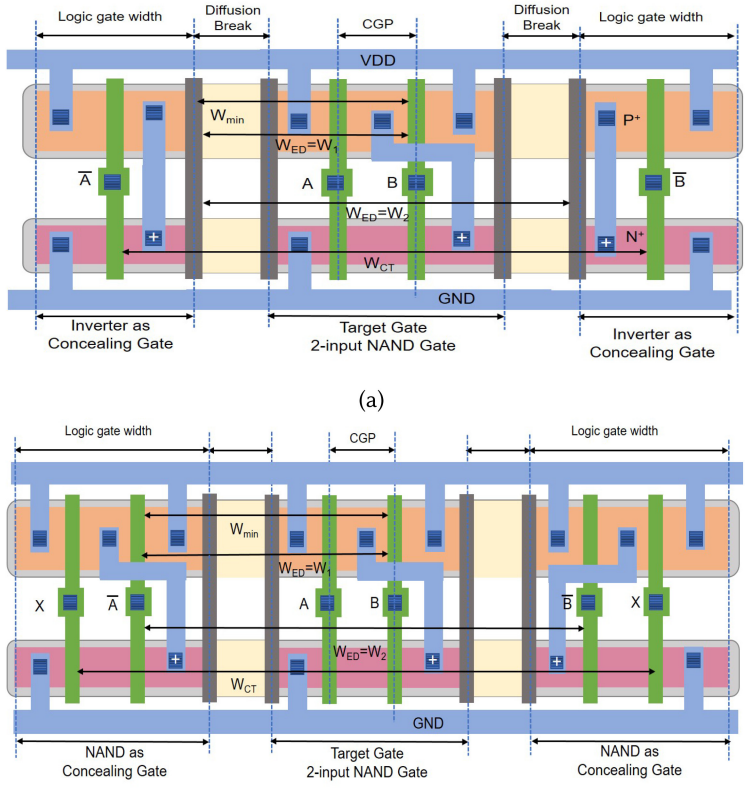


Fig. 7. (a) The asset signal carrying NAND logic gate switching activity is concealed with INVERTER gates. The INVERTER gates are placed at both ends of the NAND gate to camouflage the input A and B signal swtching. The drain of the concealing-gates are placed at a minimum distance of its corresponding signal carrying target-gates; (b) camouflaging the switching activity of the target-NAND gate with concealing-NAND gates. All the concealing-gates are connected to the inverted signal of its corresponding target-transistor/logic. In both cases, signal A is considered as the net connected to key.

the concealing- and target-gates need to be placed at a distance less than the optical resolution considered during the IC security design. It has already been proved that photons modulated at the drain terminal contribute the most in EOFM/EOP measurement [18, 41]. Hence, in the device layout, the drain terminals of the concealing-transistors must be placed at the minimum distance from the corresponding target transistors (see W_{min} in Figure 7). The activity of the asset carrying transistors can be camouflaged by maintaining the distance, W_{min} between the drain edge of the concealing-gate and the furthest edge of the asset carrying transistor lower than the optical resolution, i.e., $W_{min} \leq R$, although this is a condition for hiding the target-gate activity but not the sufficient one. An adversary may apply different input patterns to identify the edge of the EOFM activity of the concealing- and target-gate. The EOFM activity edges of two transistors operating at opposite phase change can be resolved, though the gates are placed at a distance lower than optical resolution [36]. The edges of EOFM activity become obscure if the adjacent transistors, placed at optical resolution distance, are switching in the same direction, i.e., $1 \rightarrow 0$ and vice versa. The distance between the two same direction phase changing transistors is defined as W_{ED} (see Figure 7).

Table 2. The W_{ED} for A Signal Concealing-gate for Different Logic Gates/Transistors Depending on Their Phase Change Direction

Input Signal	Phase Change After Reset	Distance with the Concealing-gate in Terms of CGP
*concealing-Gate Signal, $\bar{A}$	$1 \rightarrow 0$	—
Key-gate Input Signal (Key Value), A	$0 \rightarrow 0$	No EOFM activity
Key-gate Input Signal,B (Two possible inputs)	$1 \rightarrow 0$	$3 \times CGP$ (W_1 in Figure 7(a)) $4 \times CGP$ (W_1 in Figure 7(b))
	$0 \rightarrow 0$	No EOFM activity
concealing-Gate Signal, $\bar{B}$ (Two possible inputs)	$0 \rightarrow 0$	No EOFM activity
	$1 \rightarrow 0$	$5 \times CGP$ (W_2 in Figure 7(a)) $7 \times CGP$ (W_2 in Figure 7(b))

*=it is assumed that A is the key bit signal. Therefore all distance is presented in terms of concealing-gate for signal A.

For example, in Figure 6(a), the N_{C1} and N_{T2} transistors change phase in the same direction, i.e., $1 \rightarrow 0$, when reset is pressed. According to Figure 7, the distance between these two transistors is defined as W_1. Therefore, the transistors' edges in the EOFM activity is not distinguishable, if the distance between the two transistors, is less than the optical resolution, i.e., $W_1 \leq R$. The worst-case scenario is, transistors N_{C1} and N_{T2} are changing phases in the opposite direction (see Figure 6(b)). However, the target-logic's activity remains hidden if the distance between N_{C1} and N_{C2} transistors, W_2 in Figure 7, is less than optical resolution.

5.3 Security Evaluation of Proposed Countermeasure

To evaluate the optical probing resiliency of the proposed countermeasure we have developed a security metric based on the two crucial parameters for optical contactless probing: (a) Optical resolution of the LSM, (b) Spot size of the laser source.

5.3.1 EOFM Differentiability Metric. An adversary can probe a logic gate, if edge differentiability metric, $f(ED)$, for an optical probing system is larger than "1,"

$$f(ED) = \frac{W_{ED}}{R}. \tag{9}$$

Lower the value of $f(ED)$ indicates higher complexity in EOFM analysis. w_{ED} is the interspacing between two adjacent *nearest edges* of transistors switching at the same phase change direction.

In NAND gate in Figure 7, the input signal A is assumed to be the key-bit signal. The minimum w_{ED} is achieved when the concealing-gate input, $\bar{A}$ and NAND gate input, B changes phase at same direction. The maximum distance appears when the concealing-gates, $\bar{A}$ and $\bar{B}$, switching direction is the same. Table 2 summarize the w_{ED} for different inputs switching scenarios. The diffusion break is assumed to be equal to CGP. The EOFM measurement complexity metric for NAND/NOR gate has been calculated for different node technology and presented in Table 3. As seen in Table 3, it is evident that logic gates fabricated at a technology node lower than 45 nm can be concealed effectively.

5.3.2 EOP Cross-talk Metric. In the proposed countermeasure, the concealing-gates are the neighbor cells for the target-cell. Therefore, if the $W_{total\ Width}$ calculated from Equation (8) is smaller than laser spot size, $D_{spot\ size}$, then the concealing-gate will contribute to the EOP signal while the target-transistors are either turned OFF or static state. The cross-talk induced in an EOP signal is proportional to the total transistor width covered by the laser spot size. The calculated

Table 3. EOFM Edge Differentiability Metric Calculated for Different Node Technology for Concealing-INVERTER Gate and Target NAND Gate

Technology Node (nm)	CGP (nm)	$W_{ED} = W_1 = 3 \times CGP$	$f(ED)$ for λ= 1,300 nm	$f(ED)$ for λ = 1,064 nm	$W_{ED} = W_2 = 5\times CGP$	$f(ED)$ for λ = 1,300 nm	$f(ED)$ for λ = 1,064 nm
90	260	780	0.91	1.11	1300	1.5	1.9
65	220	660	0.78	0.94	1100	1.3	1.6
45	160	480	0.56	0.69	800	0.94	1.14
32	112	360	0.42	0.51	600	0.70	0.86
22	90	270	0.31	0.39	450	0.53	0.64
14	70	210	0.24	0.3	350	0.41	0.5

Table 4. EOP Cross-talk Metric Calulated for Different Node Technology

Techn-ology Node (nm)	CGP (nm)	INVERTER as concealing-Gate, $W_{CT} = 7 \times CGP$ (nm)	f(CT)		NAND as concealing-gate, $W_{CT} = 9 \times CGP$ (nm)	f(CT)	
			λ = 1,300 nm	λ = 1,064 nm		λ = 1,300 nm	λ = 1,064 nm
90	260	1,820	1.23	1.50	2,340	1.58	1.93
65	220	1,540	1.04	1.27	1,980	1.34	1.63
45	160	1,120	0.75	0.92	1,440	0.97	1.19
32	112	784	0.53	0.64	1,008	0.68	0.83
22	90	630	0.42	0.52	810	0.54	0.67
14	70	490	0.33	0.40	630	0.42	0.52

$W_{total\ width}$ must include the drain regions of concealing-gates, see the distance W_{CT} shown in Figure 7(a). Hence, the EOFM measurement complexity metric in terms of induced cross-talk is

$$f(CT) = \frac{w_{CT}}{D_{spot\ size}}. \tag{10}$$

Table 4 shows the security metric evaluation for different technology nodes. It is evident from the analysis that concealing-gates can be used to protect the target-gates implemented in 45-nm or smaller technology nodes.

5.4 Proposed Countermeasure for Latch and Flip-flop

The proposed countermeasure is equally applicable in hiding the asset information stored in the flip-flop. The sequential logic elements can be protected by two different approaches. First, each combinatorial logic used to design target-flip-flop must be protected with a concealing-gate connected to the inverted input of that combinatorial logic. Second, a security designer can use concealing-flip-flop to protect the target-flip-flop. In the latter approach, the logic gates used as building block for the concealing-flip-flop must be placed next to its corresponding target-flip-flop building block logic gates in the layout. Hence, no additional standard cell design is required.

5.5 Target-gate Selection

Adding a concealing-gate for each of the target-logic increases the area and power overhead. Besides, random insertion of concealing-gates does not offer any improvement in security against optical probing. In logic locking, we selected key-gates/registers to protect using the concealing-gate. Note that, in more general scenarios, a security designer can identify the key carrying net and corresponding target-logic gate/registers in a more systematic manner using the target-gate selection metric described in Reference [45].

6 VALIDATION OF PROPOSED COUNTERMEASURE

In this section, we evaluate the concealing-logic gate-based logic gate activity camouflaging approach through simulated EOP waveform generation.

6.1 Fundamentals of Simulated EOP Waveform Generation

The reflected photon modulation capacity of devices, such as free carrier absorption, is linearly related to the voltage at the MOSFET terminals. The modulation capacity of each terminal of the transistor can be calculated from the area of each terminal and piecewise voltage changes [20]. For simplicity, we have assumed that over the entire width or area of a MOSFET terminal, the voltage only varies with time, i.e., each transistor terminal acts as an equipotential surface. The modulation capacity of the terminal can be defined as [20],

$$M_i = k_i \times W_i \times \Delta v_i, \tag{11}$$

where k_i is a relative modulation constant, which depends on the type of transistor, i.e., PMOS or NMOS, terminals of the transistor under consideration. The value of k_i can be defined empirically [20] or based on the BSIM-CMG model [1]. In our analysis, we only considered the pull-up network of the logic gates. In PMOS transistors, the source/drain contribution is 1.5 times stronger than the gate terminal [1]. W_i and v_i is the width of the terminal and temporal voltage changes on that terminal. The amplitude of EOP signal amplitude, R_T is [20]

$$R_T = \sum_{i=1}^{W_{total\_width}} P_i \times M_i. \tag{12}$$

6.2 EOP Signal

The effectiveness of concealing-gates in hiding the target-logic elements activity is evaluated against both EOP and EOFM analysis. There are two scenarios where an adversary may attempt while probing the target-gates,

(1) **Scenario-1:** Focusing the laser spot on the target-gate, hence, photons modulated by the concealing- and target-gates are collected by the photo-detector (see Figure 8(a)).
(2) **Scenario-2:** The target-gate is placed at one end of the laser spot to reduce the cross-talk from the concealing-gates (see Figure 8(b)).

We have evaluated both of the scenarios using the NAND gate implemented at 32-nm technology node as a target/asset-carrying logic gate. INVERTERs are used as concealing-logic gates due to low power and area overhead. Note that a security designer can choose any logic gate as a concealing-gate to hide the functionality of the target-logic element, as long as the inputs of the concealing-gates are Inverted. The EOP signal is generated using Equation (11) and Equation (12). The gates are implemented in 32-nm technology nodes. The total width of the logic gates can be defined by Equation (7) and Equation (8). It is assumed that the laser is focused on PMOS transistors.

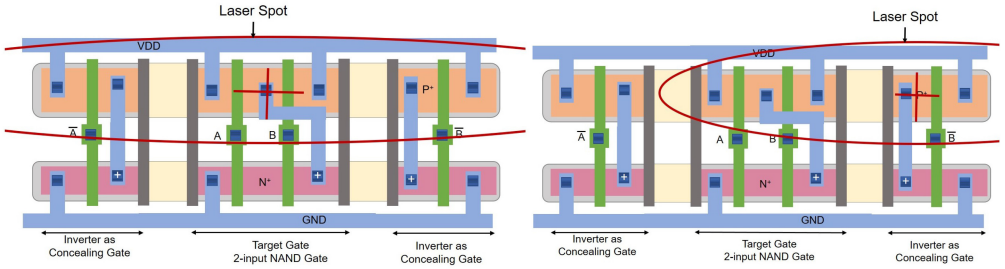


Fig. 8. (a) The laser is focused at the center of two PMOS used in target-NAND gate. Therefore, all the concealing-gates are covered by the laser spot. (b) The target-NAND gate is placed at one end of the laser spot. Hence, the concealing-gate for input A transistors is not covered by the laser. This is the worst-case scenario from the security perspective of the proposed countermeasure. Note that, the shape of laser spot showed in the image is only for illustration purpose, does not represent the original laser spot shape and dimension.

The input to the target-NAND gates, and concealing-gates and the NAND cell output, Z, is presented in Figure 9(a). The simulated optical probing signal of a NAND gate without and with concealing-gates, for scenario-1, are showed in Figure 9(b). Though the EOP measurement of the NAND gate without concealing-gate follows similar behaviour collected empirically in References [1, 20], EOP measurement with concealing-gates reads a higher value than the prior one for certain input combinations. The cross-talk introduced by the concealing-gate forced the EOP signal of the NAND gate to maintain optical probing output as "1." Therefore, the switching activity of the target-gate is camouflaged by the concealing-INVERTER gates. Similarly, in scenario-2, the EOP signal with concealing-gates maintain a higher value when the NAND gate output is switched to "0." It is important to note that placing the target-gate at one end of the laser spot, i.e., creating the scenario-2 in real life implementation, requires an in-depth understanding of the laser property, precise control over the stage movement, and higher optical resolution. Therefore, the "Concealing-Gate" approach is effective against an adversary without extensive reverse-engineering capability.

6.3 Modulation Capability of the Logic Gates

EOFM analysis represents the reflected photons got modulated by transistors operating at a certain frequency. Therefore, the modulation capacity, defined by the Equation (11) is related to the modulation properties of the reflected photons. Therefore, variation in modulation capacity along the width of logic cells represent the possible EOFM activity source along with its spatial location. Note that the modulation capacity cannot be used as a representation of original EOFM or simulated EOFM activity, since it does not consider complex photon-material interactions and laser properties. We have evaluated the modulation capability of the PMOS transistors for the scenario-1 (see Figure 8(a)), where the activity of the target-NAND gates are disguised with concealing-INVERTER gates. We have extracted the distance between probable EOFM activity edges, i.e., the w_1 and w_2. Figure 10, we represent the spatial changes in modulation capability along the logic gates width. It has been identified, the w_{1l} and w_2 are 240 nm and 576 nm appears for the input sets, $\{A, B\} = \{0, 1\}, \{1, 0\}$ and $\{A, B\} = \{1, 1\}$, respectively. According to Table 1, either w_1 and w_2 are less than the optical resolution of 1,300-nm and 1,064-nm laser. Besides, the phase change direction of concealing-input signal and the target-NAND gate inputs are the same, which emphasizes the difficulty in identifying edges of concealing- and target-NAND gate

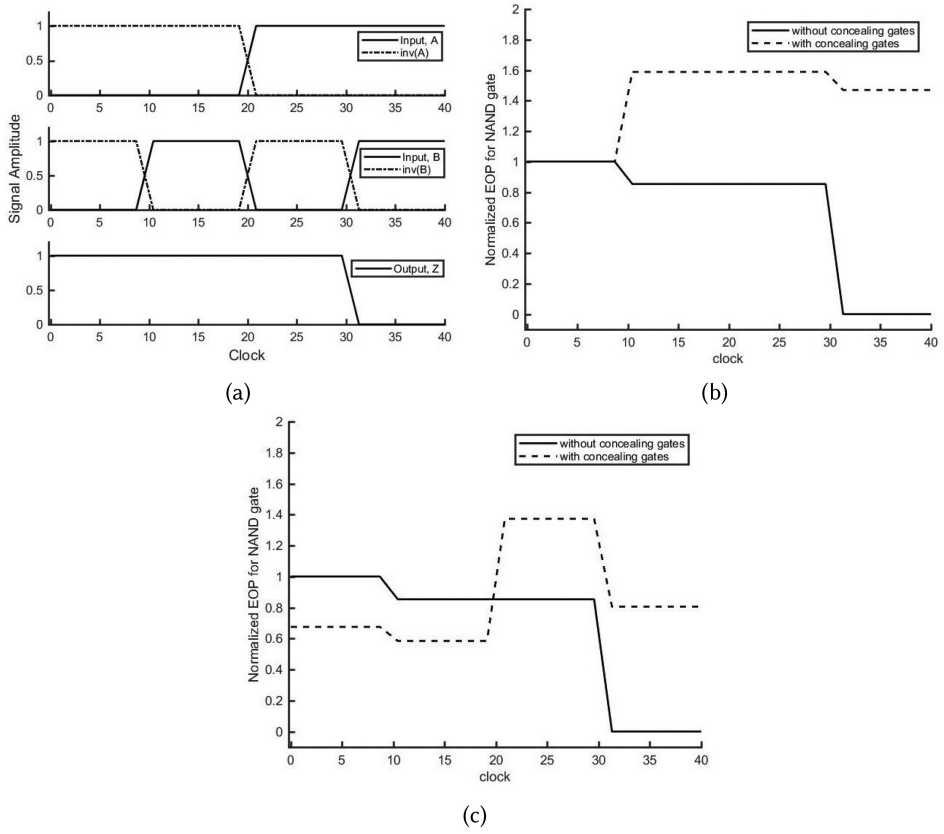


Fig. 9. (a) The input, A and B, signals for NAND logic gate and corresponding concealing-gate input, $\bar{A}$ and $\bar{B}$, signals. The output, Z, signal from NAND gate is also presented; (b) the EOP signal for a NAND gate implemented with concealing-gates and a single NAND logic gate (implemented without concealing-gate). The NAND gate is at the center of laser spot size, the location shown in Figure 8(a)); (c) the EOP signal for a NAND gate with concealing-gate and a single NAND logic gate (implemented without concealing-gate). The NAND gate is placed at one end of the laser spot size to remove cross-talk from one of the concealing-gate, the location shown in Figure 8(b)).

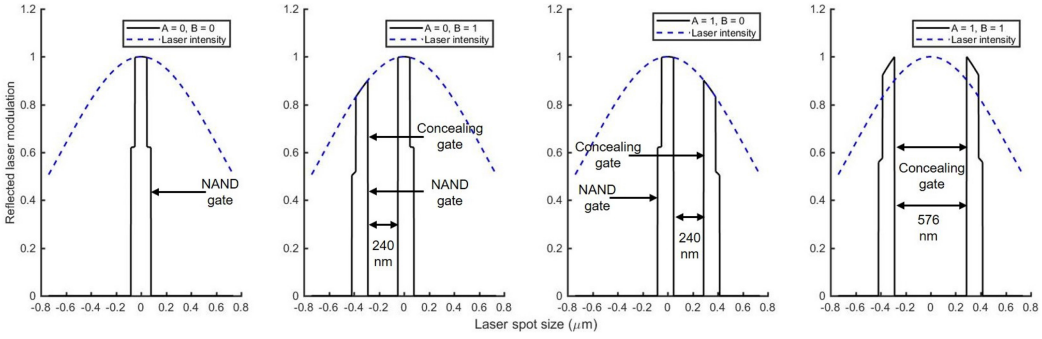


Fig. 10. Modulation capability of concealing-INVERTER gate and target-NAND gate. Modulation capability represents the spatial location EOFM activity sources. The distances between the edges of the INVERTER gate and NAND gate are also annotated.

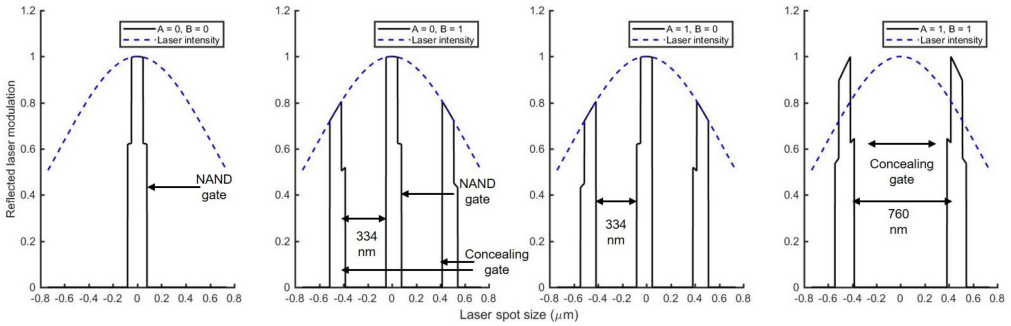
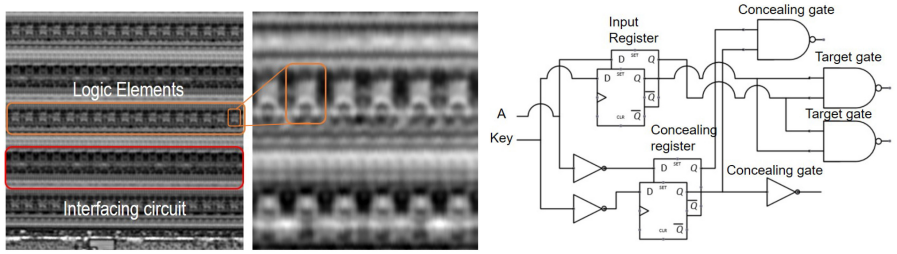


Fig. 11. Modulation capability of concealing-NAND gate and target-NAND gate.



(a) (b)

Fig. 12. (a) FPGA logic fabric structure and zoomed-in view of logic elements (orange rectangle area); (b) PoC implementation of the circuit where the target-NAND cells are protected by concealing-gates.

transistors. However, analyzing the modulation capacity for different input signals in Figure 10, asymmetric footprint in EOFM 2D mapping can be predicted. A security designer can eliminate the asymmetric in EOFM activity shape by using 2-input logic gates, e.g., NAND/NOR gates, to hide logic gates activity (see Figure 11).

7 EXPERIMENTAL VALIDATION

7.1 Device Under Test

The attack resiliency of the proposed countermeasure against optical probing is evaluated in a FPGA platform. We chose a Flash-based Microsemi MPF300 Polarfire FPGA manufactured with 28 nm technology in a flip-chip BGA package. The FPGA is implemented in an Avalanche FPGA development board. There is no heat sink on top of the package, and hence, we have direct access to the silicon substrate on the backside of the chip without any package preparation or silicon polishing. According to our measurements, the thickness of the substrate is about 700 μm. A 1.3-μm light source is used for acquiring the image of the die without any substrate thinning. Figure 12(a) presents the FPGA logic fabric consists of several identical **configurable logic blocks (CLBs)**. The FPGA logic resources are fabricated as logic clusters, as presented in the orange rectangular box in Figure 12(a). The interfacing circuit responsible for the routing between CLBs of the FPGA, is shown in the red rectangle in Figure 12(a). Each cluster consists of 12 logic elements. Each logic element consists of a 4-input LUT with a D-flip-flop. The logic element is fracturable, which means the LUT and flip-flop can be used either together or independently [7].

7.2 Measurement Setup

A Hamamatsu PHEMOS-1000 LSM used for FA is used to perform EOFM analysis over the **Device Under Test (DUT)**. The equipment consists of a suitable probing light source (Hamamatsu C13193), and an optical probing preamplifier (Hamamatsu C12323). The development board is placed inside the PHEMOS and a PC is connected to the board to program the FPGA. Programming of the FPGA is performed through USB, which is handled by an FTDI chip and powered by the development board supply. We have used a 50×/0.76 NA lens to generate the 2D mapping of the EOFM activity of the circuit.

7.3 Proof-of-Concept Circuit Implementation

For our experiment, we have implemented a **Proof-of-concept (PoC)** circuit in the DUT. The target-NAND, in the PoC circuit (see Figure 12(b)), gates are connected to input A and Key-input, Key. Each target-gate is implemented with a single concealing-gate. The concealing-gates are connected to the inverted signal of the key-input and signal A. The inputs in the PoC circuit are fed through flip-flops. We implemented four of the PoC concealing-gate circuit in the FPGA and the EOFM activity is measured for with and without concealing-INVERTER and NAND gates.

7.4 Experimental Results

The concealing-gates are considered successfully camouflaged if the following properties are fulfilled:

(1) the target-gate activity if the EOFM activity is always present. This satisfies the frequency matching and switching inputs property of EOFM concealing.
(2) the EOFM activity edges of concealing- and target-logic gates are indistinguishable, irrespective to the input pattern applied to the device. This satisfies the distinguishable edges property of the EOFM concealing.

To probe the keys from key-registers and target-logic gates, we have compared three input vectors, x_0, x_1, and $\bar{x}_1$ where the inputs for x_0, x_1, and $\bar{x}_1$ are 0000, 1100, and 0011. Since the chip does not perform any functions during the boot-up process, it can be assumed that all the input ports are set to an inactive or grounded state. Hence, the input vector $\mathbf{x_0}$ can be a representation of the boot-up condition of the chip.

An adversary can identify the area containing the sequential and combinatorial logic gates by analyzing the EOFM activity of clock signal, as shown in Figure 13(a). The EOFM measurement of target-logic elements with concealing-gates, shown in Figure 13(b) and Figure 13(c)), are measured for the same key value. Figure 13(d) contains the inverted key compared to the aforementioned figures. Since, either target-or concealing-logic elements is active for different inputs (see Figure 13), the logical state of the target-gate cannot be predicted without the knowledge of gate-level netlist, which can be extracted with only full-blown reverse engineering. In addition, inverting the inputs does not induce significant change in EOFM activity that can be interpreted with human eyes (see Figure 13(c) and Figure 13(d)). Unlike PoC implemented with concealing-gates, the activity of the key-registers and key-gates can be exposed from the EOFM activity (see Figure 14(a) and Figure 14(b)). The key value extracted from the EOFM activity is "0101."

7.5 Resiliency against Image Processing and Computer Vision Analysis

An adversary may attempt to distinguish the activity of the key-gates/registers from concealing-gates in EOFM measurement, using image processing and computer vision techniques. An adversary can collect multiple EOFM measurements for different input patterns and use image

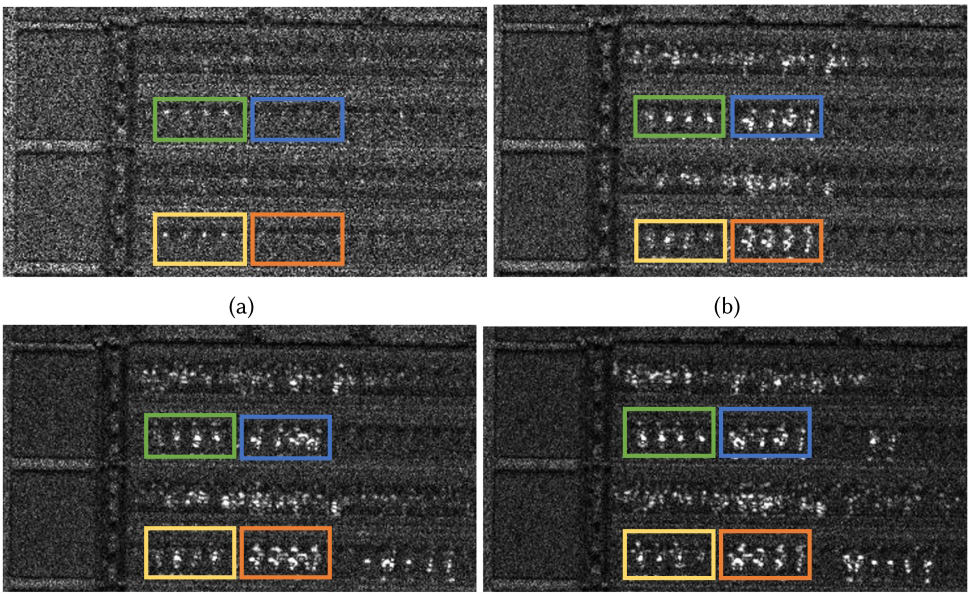


Fig. 13. (a) Localizing the flip-flop and combinatorial circuit locations in the FPGA. The green and yellow rectangles represent input register and key-register, respectively, both implemented with concealing-registers. The blue and orange rectangles represent the location of target-gate with concealing-NAND gate, and target-gate with concealing-INVERTER gate, respectively; (b) EOFM activity for the input signal, x_0; (c) EOFM activity for the input signal, x_1; (d) EOFM activity for inverted key-input, $\bar{K}$, and input signal, $\bar{x}_1$.

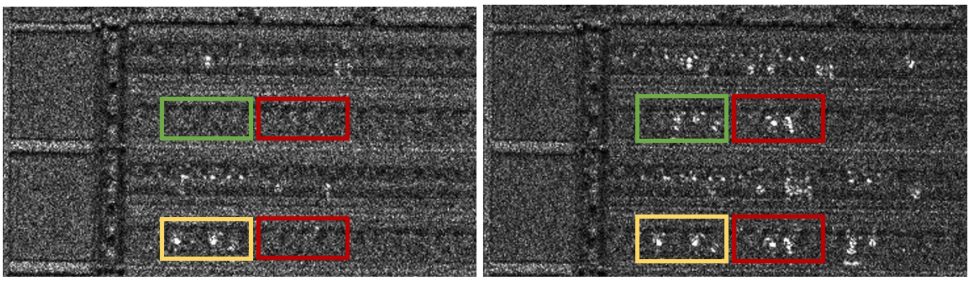


Fig. 14. (a) EOFM activity analysis without concealing-gate implementation for the input x_0; (b) EOFM activity implementation for the input x_1. The green, yellow, and red rectangles in the figures represent input register, key-register, and target-NAND logic gates activity, respectively.

processing to extract the key value. To evaluate the performance of the concealing-gate, we have implemented flip-flop protected with concealing-flip-flop (see orange rectangle in Figure 15(a) and Figure 15(b)) and compared the EOFM activity with the exposed target-flip-flop (see white rectangle in Figure 15(a) and Figure 15(b)). The input signal of the protected target-flip-flops are flipped in the images to evaluate whether change in input data cause significant variation in EOFM activity mapping. 50×/0.76 NA lens is used to evaluate the attack resiliency for the proposed countermeasure. It is evident that due to the presence of concealing-gates, the optical

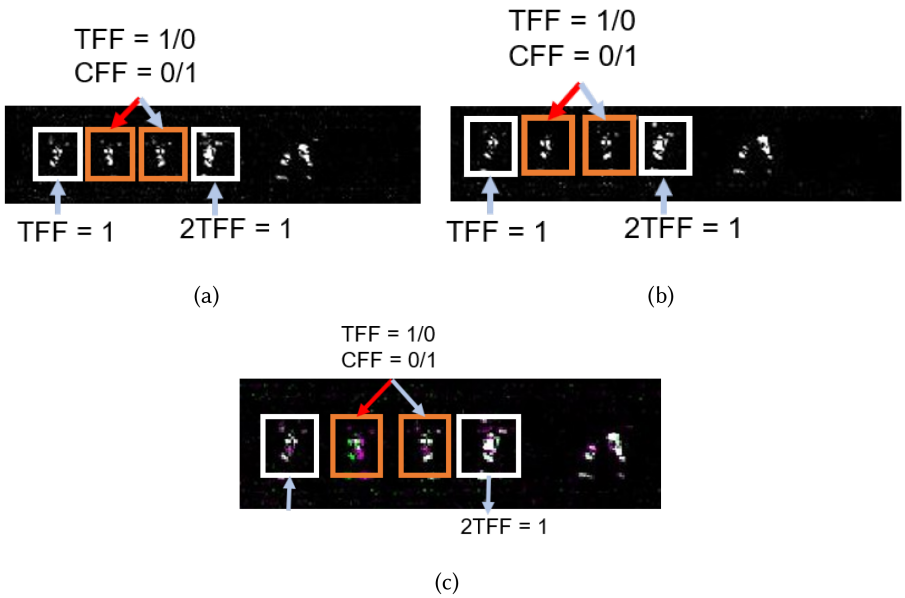


Fig. 15. (a) EOFM activity mapping of flip-flop implemented with and without concealing-flip-flop; (b) EOFM activity mapping of flip-flop implemented with and without concealing-flip-flop. The input of one target-flip-flop protected with concealing-gate is flipped (marked with red arrow); (c) EOFM activity of Figure 15(a) and Figure 15(b) after image registration.

Table 5. Optical Resolution and Laser Spot Diameter for Different Wavelength Laser and Lens

Wavelength + Lens	NA	Resolution (nm)	Diameter (nm)
1,300 nm + 50× lens*	0.76	855	1,476
1,064 nm + 50× lens*	0.76	700	1,208
1,300 nm + SIL**	3.5	185	453
650 nm + SIL**	3.4	95.6	233

*=50× is objective lens used in optical attacks.
** = SIL stands for solid immersion lens.

probed data form EOFM activity is "1," irrespective to the data stored in target-flip-flop. The registered images of the Figure 15(a) and Figure 15(b) is shown in Figure 15(c), which shows negligible spatial shift due to change in input signal to protected target-flip-flop.

8 DISCUSSION

8.1 Optical Resolution and Laser Spot Size

It is mostly argued that optical probing is reaching its limit due to low optical resolution. However, in reality, an adversary attempts to probe the entire logic gate, register or cache memory cells. The optical resolution can be further increased once the adversary has access to a **solid immersion lens (SIL)**. SIL can improve the NA by the refractive index times of the SIL material. Table 5 presents the resolution and laser spot size with SIL. The resolution can further be improved by moving to visible light spectrum with SIL [25]. The challenge of making use of visible light and SIL is that the DUT must be polished down to 10–30 μm [25]. Though there has been a significant advancement in automated backside polishing, the process still require higher processing time.

Besides, in the flip-chip BGA packages, the ball grid leaves shadow marking due to higher pressure applied during bulk silicon polishing. In addition, the effort significantly increases if the chip is implemented in a PCB.

8.2 Attack Resiliency

The success of proposed countermeasure depends on increasing time-cost of standard cell identification and full-blown reverse engineering. The reverse engineer's task can be made difficult by implementing physical layout obfuscation techniques like camouflage cells, covert gate, dummy vias, filler cells, obfuscated finite-state machine, and so on, in the chip [13, 31, 34, 38]. In addition, only extracting the standard cell library or module functionality are not enough to exploit the target logic. Recently proposed covert gate-based physical layout obfuscation methods can protect the logic gate detection from imaging tools and functional analysis [38]. Since understanding the input signal to each logic element and identifying the implemented logic gates can only facilitate interpreting the optical probing signal, implementing concealing-gates with covert gates-based layout obfuscation will make an SoC bulletproof against optical probing attack. Therefore, an attempt to bypass the necessity of full-blown reverse engineering by recognizing the standard cell library using active layer and via detection using the methods described in References [43, 46] is futile. Such a technique can be used or extended to develop masking against photon emission analysis or detect laser-fault injection. However, the resiliency of the proposed approach against laser logic state imaging [19] attack is yet to be evaluated.

Recent studies show that weak obfuscation techniques can act as a double edge sword for the chip [13]. the output or the interconnects of concealing-gate can be used by a malicious insider or untrusted foundry to implement backdoor or hardware Trojan in the chip. But we also acknowledge that this is in fact, the case for any gates/flip flop in a circuit that processes or observes sensitive information. Detecting Trojans is outside the scope of this article. We do not believe concealing-gate would increase the opportunity for counterfeiters. Please note that the threat model of concealing gate considers a trusted design house to protect the identity of the concealing-gate.

8.3 Resource Overhead

The resource overhead, e.g., speed, area, and power, is always a concern for any hardware application, such as low power IoT devices. The resource overhead of the proposed approach largely depends on the nature of the target application, e.g., cryptomodule or logic locking. Similarly, the number of gates considered as target-logic also plays a crucial role in the overhead calculation. For instance, implementing concealing-gate with all the logic gates connected to key-gates and key-signal in logic locking scheme can potentially introduce a significant area and power overhead. Therefore, developing a methodology to select appropriate target logic cell selection, which maintains resource constraints, needs to be developed. To understand the resource overhead, the proposed approached is implemented in four open core designs, namely (a) MSP430 microcontroller, (b) OR1200 SoC, (c) ARM Cortex-M0 Processor, and (d) CEP SoC [29]. Those designs are all logic locked with 128-bit key. The area and power overhead for protecting the key-gates with concealing-NAND gate is presented in Table 6. It is evident form the analysis that the power overhead is well below 1%. However, the area overhead is dependent on the design and target-logic selection.

9 CONCLUSION

We presented a design methodology to implement a optical probing resistance design. This techniques uses standard cell library to prepare a circuit-based countermeasure against optical probing

Table 6. Area and Power Overhead for Concealing-gate Approach

Design	No. of key bits/Gates	Total no. of cells	Area (μm^2)	Power (μW)	Area Over-head	Power Over-head
MSP430 micro-controller	128	4,018	62097.408	3877.4	2.28%	0.26%
OR1200 SoC	128	7,300	197133.644	5387.6	0.72%	0.184%
ARM Cortex -M0 Processor	128	12,000	439675	12500	0.32%	0.081%
CEP SoC	128	15,000	2269535.457	14079.6078	0.063%	0.070%

2-input NAND logic are used to protect the target-cells.

attacks, namely EOP and EOFM techniques, mounted from the chip backside. The method can be readily applied to both ASIC and FPGA design flow. A security metric is developed to evaluate the optical attack resiliency of the device. A simulation-based study validates the efficacy of the countermeasure. Moreover, experimental results have demonstrated that the proposed countermeasure is an effective technique to protect the chip activities from chip backside optical attacks. Since this technique is based on the equal number of switching in the asset carrying modules, the protection mechanism can be extended to protect device secrets form side-channel analysis as well.

REFERENCES

[1] Eli Abuayob et al. 2016. Complex waveform analysis for advanced CMOS ICs: Physics of complex waveform signals for design validation and debug application. In *Proceedings of the International Symposium for Testing and Failure Analysis (ISTFA'16)*.

[2] Elham Amini, Anne Beyreuther, Norbert Herfurth, Alexander Steigert, Bernd Szyszka, and Christian Boit. 2018. Assessment of a chip backside protection. *J. Hardw. Syst. Secur.* 2, 4 (2018), 345–352.

[3] Stephan Borel, L. Duperrex, E. Deschaseaux, J. Charbonnier, J. Cledière, R. Wacquez, J. Fournier, J.-C. Souriau, G. Simon, and A. Merle. 2018. A novel structure for backside protection against physical attacks on secure chips or sip. In *Proceedings of the 2018 IEEE 68th Electronic Components and Technology Conference (ECTC'18)*. IEEE, 515–520.

[4] Max Born and Emil Wolf. 2013. *Principles of Optics: Electromagnetic Theory of Propagation, Interference and Diffraction of Light*. Elsevier.

[5] Ulbert J. Botero, Ronald Wilson, Hangwei Lu, Mir Tanjidur Rahman, Mukhil A. Mallaiyan, Fatemeh Ganji, Navid Asadizanjani, Mark M. Tehranipoor, Damon L. Woodard, and Domenic Forte. 2020. Hardware trust and assurance through reverse engineering: A survey and outlook from image analysis and machine learning perspectives. *arXiv:2002.04210*. Retrieved from https://arxiv.org/abs/2002.04210.

[6] Robert C. Camilletti, Loren A. Haluska, and Keith W. Michael. 1995. Tamper-proof electronic coatings. US Patent 5,458,912.

[7] Microsemi Corporation. [n.d.]. User Guide: Polarfire FPGA Fabric. Retrieved July 14, 2018 from https://www.microsemi.com/document-portal/doc_view/136522-ug0680-polarfire-fpga-fabric-user-guide.

[8] Franck Courbon, Sergei Skorobogatov, and Christopher Woods. 2016. Reverse engineering flash eeprom memories using scanning electron microscopy. In *Proceedings of the International Conference on Smart Card Research and Advanced Applications*. Springer, 57–72.

[9] Ana Covic, Qihang Shi, Haoting Shen, and Domenic Forte. 2019. Contact-to-silicide probing attacks on integrated circuits and countermeasures. In *Proceedings of the 2019 Asian Hardware Oriented Security and Trust Symposium (AsianHOST'19)*. IEEE, 1–6.

[10] Suman Datta. 2018. Ten nanometre CMOS logic technology. *Nat. Electr.* 1, 9 (2018), 500–501.

[11] Alexandre Ayres de Sousa. 2017. *3D Monolithic Integration: Performance, Power and Area Evaluation for 14nm and Beyond*. Ph.D. Dissertation.

[12] H. K. Heinrich, B. R. Hemenway, R. A. Marsland, and D. M. Bloom. 1988. A noninvasive optical probe for detecting electrical signals in silicon IC's. In *Review of Progress in Quantitative Nondestructive Evaluation*. Springer, 1161–1166.

[13] Max Hoffmann and Christof Paar. 2021. Doppelganger obfuscation—Exploring the defensive and offensive aspects of hardware camouflaging. In *IACR Transactions on Cryptographic Hardware and Embedded Systems*. 82–108.

[14] Steven Kasapi, Roy Ng, Joy Liao, William Lo, Bruce Cory, and Howard Marks. 2012. Comparison of applications of laser probing, laser-induced circuit perturbation and photon emission for failure analysis and yield enhancement. In *Proceedings of the 2012 IEEE International Reliability Physics Symposium (IRPS'12)*. IEEE, 2D–1.

[15] Ulrike Kindereit. 2009. *Investigation of Laser-Beam Modulations Induced by the Operation of Electronic Devices. Doctoral Thesis*. TU Berlin, Berlin. https://doi.org/10.14279/depositonce-2143

[16] Ulrike Kindereit. 2014. Fundamentals and future applications of laser voltage probing. In *Proceedings of the 2014 IEEE International Reliability Physics Symposium*. IEEE, 3F–1.

[17] Ulrike Kindereit, Gary Woods, Jing Tian, Uwe Kerst, and Christian Boit. 2007. Investigation of laser voltage probing signals in CMOS transistors. In *Proceedings of the 2007 IEEE International Reliability Physics Symposium Proceedings*. IEEE, 526–533.

[18] Ulrike Kindereit, Gary Woods, Jing Tian, Uwe Kerst, Rainer Leihkauf, and Christian Boit. 2007. Quantitative investigation of laser beam modulation in electrically active devices as used in laser voltage probing. *IEEE Trans. Device Mater. Reliabil.* 7, 1 (2007), 19–30.

[19] Thilo Krachenfels, Fatemeh Ganji, Amir Moradi, Shahin Tajik, and Jean-Pierre Seifert. 2021. Real-world snapshots vs. theory: Questioning the t-probing security model. In *Proceedings of the 2021 IEEE Symposium on Security and Privacy (SP'21)*. IEEE.

[20] R. Krishnan, S. Xuan, Lim Gabriel, Tan Abel, Lua Winson, Gopinath Ranganathan, P Angelina, and C Meng. 2018. Pattern search automation for combinational logic analysis. In *Proceedings of the International Symposium for Testing and Failure Analysis*. 86.

[21] Leonidas Lavdas, M. Tanjidur Rahman, Mark Tehranipoor, and Navid Asadizanjani. 2020. On optical attacks making logic obfuscation fragile. In *Proceedings of the 2020 IEEE International Test Conference in Asia (ITC-Asia'20)*. IEEE, 71–76.

[22] Heiko Lohrke, Philipp Scholz, Anne Beyreuther, Ulrike Ganesh, Eckart Uhlmann, Stefan Kühne, Marco Jagodzinski, Yoshitaka Iwaki, Robert Chivas, Scott Silverman, et al. 2016. Contactless fault isolation for FinFET technologies with visible light and GaP SIL. In *Proceedings of the 42nd International Symposium for Testing and Failure Analysis*.

[23] Heiko Lohrke, Shahin Tajik, Christian Boit, and Jean-Pierre Seifert. 2016. No place to hide: Contactless probing of secret data on FPGAs. In *Proceedings of the International Conference on Cryptographic Hardware and Embedded Systems*. Springer, 147–167.

[24] Heiko Lohrke, Shahin Tajik, Thilo Krachenfels, Christian Boit, and Jean-Pierre Seifert. 2018. Key extraction using thermal laser stimulation. *IACR Transactions on Cryptographic Hardware and Embedded Systems* 3 (2018) 573–595.

[25] Heiko Lohrke, Hannes Zöllner, Philipp Scholz, Shahin Tajik, Christian Boit, and Jean-Pierre Seifert. 2017. Visible light techniques in the finfet era: Challenges, threats and opportunities. In *Proceedings of the 2017 IEEE 24th International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA'17)*. IEEE, 1–6.

[26] Salvador Manich Bou, Daniel Arumi Delgado, Rosa Rodríguez Montañés, Jordi Mujal Colell, and David Hernández García. 2015. Backside polishing detector: A new protection against backside attacks. In *Proceedings of the Conference on Design of Circuits and Integrated Systems (DCIS'15-XXX)*. 1–6.

[27] Sravan K. Marella, Amit Ranjan Trivedi, Saibal Mukhopadhyay, and Sachin S. Sapatnekar. 2015. Optimization of FinFET-based circuits using a dual gate pitch technique. In *Proceedings of the 2015 IEEE/ACM International Conference on Computer-Aided Design (ICCAD'15)*. IEEE, 758–763.

[28] Yin S. Ng, Ted Lundquist, Dmitry Skvortsov, Joy Liao, Steven Kasapi, and Howard Marks. 2010. Laser voltage imaging: A new perspective of laser voltage probing. In *Proceedings of the International Symposium for Testing and Failure Analysis (ISTFA'10)*. 5–13.

[29] Opencores.org. [n.d.]. openMSP430. Retrieved from June 6, 2020 https://opencores.org/projects/openmsp430.

[30] Mir Tanjidur Rahman and Navid Asadizanjani. 2019. Backside security assessment of modern SoCs. In *Proceedings of the International Workshop on Microprocessor/SoC Test, Security and Verification (MTV'19)*. 18–24.

[31] M. Tanjidur Rahman, M. Sazadur Rahman, Huanyu Wang, Shahin Tajik, Waleed Khalil, Farimah Farahmandi, Domenic Forte, Navid Asadizanjani, and Mark Tehranipoor. 2020. Defense-in-depth: A recipe for logic locking to prevail. *Integration* 72 (2020), 39–57.

[32] M. Tanjidur Rahman, Qihang Shi, Shahin Tajik, Haoting Shen, Damon L. Woodard, Mark Tehranipoor, and Navid Asadizanjani. 2018. Physical inspection & attacks: New frontier in hardware security. In *Proceedings of the 2018 IEEE 3rd International Verification and Security Workshop (IVSW'18)*. IEEE, 93–102.

[33] Mir Tanjidur Rahman, Shahin Tajik, M. Sazadur Rahman, Mark Tehranipoor, and Navid Asadizanjani. 2020. The key is left under the mat: On the inappropriate security assumption of logic locking schemes. In *Proceedings of the Conference on IEEE International Symposium on Hardware Oriented Security and Trust (HOST'20)*.

[34] Jeyavijayan Rajendran, Michael Sam, Ozgur Sinanoglu, and Ramesh Karri. 2013. Security analysis of integrated circuit camouflaging. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*. 709–720.

[35] Venkat Krishnan Ravikumar, Winson Lua, Seah Yi Xuan, Gopinath Ranganathan, and Angeline Phoa. 2015. Combinational logic analysis using laser voltage probing. In *ISTFA 2015*. ASM International, 35–41.

[36] Venkat Krishnan Ravikumar, G. Lim, J. M. Chin, Kin Leong Pey, and J. K. W. Yang. 2018. Understanding spatial resolution of laser voltage imaging. *Microelectr. Reliabil.* 88 (2018), 255–261.

[37] MOSIS Service. 2009. Design Rules MOSIS Scalable CMOS(SCMOS). Retreived on July 14, 2018 from https://www.ece.rice.edu/Courses/422/manual/mosis_scmos7_2.pdf.

[38] Bicky Shakya, Haoting Shen, Mark Tehranipoor, and Domenic Forte. 2019. Covert gates: Protecting integrated circuits with undetectable camouflaging. *IACR Trans. Cryptogr. Hardw. Embed. Syst.* (2019), 86–118.

[39] Richard A. Soref and Brian R. Bennett. 1987. Electrooptical effects in silicon. *IEEE J. Quant. Electr.* 23, 1 (1987), 123–129.

[40] Shahin Tajik, Julian Fietkau, Heiko Lohrke, Jean-Pierre Seifert, and Christian Boit. 2017. Pufmon: Security monitoring of fpgas using physically unclonable functions. In *Proceedings of the 2017 IEEE 23rd International Symposium on On-Line Testing and Robust System Design (IOLTS'17)*. IEEE, 186–191.

[41] Shahin Tajik, Heiko Lohrke, Jean-Pierre Seifert, and Christian Boit. 2017. On the power of optical contactless probing: Attacking bitstream encryption of FPGAs. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 1661–1674.

[42] Shahin Tajik, Dmitry Nedospasov, Clemens Helfmeier, Jean-Pierre Seifert, and Christian Boit. 2014. Emission analysis of hardware implementations. In *Proceedings of the 2014 17th Euromicro Conference on Digital System Design*. IEEE, 528–534.

[43] Nidish Vashistha, Hangwei Lu, Qihang Shi, M. Tanjidur Rahman, Haoting Shen, Damon L. Woodard, Navid Asadizanjani, and Mark Tehranipoor. 2018. Trojan scanner: Detecting hardware trojans with rapid SEM imaging combined with image processing and machine learning. In *Proceedings from the 44th International Symposium for Testing and Failure Analysis (ISTFA'18)*. ASM International, 256.

[44] Nidish Vashistha, M. Tanjidur Rahman, Olivia P. Paradis, and Navid Asadizanjani. 2019. Is backside the new backdoor in modern SoCs? In *Proceedings of the 2019 IEEE International Test Conference (ITC'19)*. IEEE, 1–10.

[45] Huanyu Wang, Qihang Shi, Adib Nahiyan, Domenic Forte, and Mark M. Tehranipoor. 2019. A physical design flow against front-side probing attacks by internal shielding. *IEEE Trans. Comput.-Aid. Des. Integr. Circ. Syst.* 39, 10 (2019), 2152–2165.

[46] Ronald Wilson, Rabin Y. Acharya, Domenic Forte, Navid Asadizanjani, and Damon Woodard. 2019. A novel approach to unsupervised automated extraction of standard cell library for reverse engineering and hardware assurance. In *Proceedings of the 45th International Symposium for Testing and Failure Analysis (ISTFA'19)*. ASM International, 249.

[47] Ruilong Xie, Kwan-Yong Lim, Min Gyu Sung, and Ryan Ryoung-Han Kim. 2016. Methods of forming single and double diffusion breaks on integrated circuit products comprised of FinFET devices and the resulting products. US Patent 9,412,616.

[48] Wai Mun Yee, Mario Paniccia, Travis Eiles, and Valluri Rao. 1999. Laser voltage probe (LVP): A novel optical probing technology for flip-chip packaged microprocessors. In *Proceedings of the 1999 7th International Symposium on the Physical and Failure Analysis of Integrated Circuits (Cat. No. 99TH8394)*. IEEE, 15–20.

[49] Kyungsuk Yi, Minsu Park, Sungyong Cha, and Seungjoo Kim. 2019. Practical silicon-backside-protection method for abnormally detection. *J. Semicond. Technol. Sci.* 19, 6 (2019), 577–584.

[50] Haus Zhang, Power Tian, Xuejian Qian, and Winter Wang. 2017. Electro optical probing/frequency mapping (EOP/EOFM) application in failure isolation of advanced analogue devices. In *Proceedings of the 2017 IEEE 24th International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA'17)*. IEEE, 1–5.

Received June 2020; revised October 2020; accepted January 2021