Nanopyramid: An Optical Scrambler Against Backside Probing Attacks

Haoting Shen, Navid Asadizanjani, Mark Tehranipoor, and Domenic Forte
Florida Institute for Cyber Security (FICS) Research
ECE Department, University of Florida
{htshen, dforte}@ece.ufl.edu

Abstract

Optical probing from the backside of an integrated circuit (IC) is a powerful failure analysis technique but raises serious security concerns when in the hands of attackers. For instance, attacks using laser voltage probing (LVP) allow direct reading of sensitive information being stored and/or processed in the IC. Although a few sensor-based countermeasures against backside optical probing attacks have been proposed, the overheads (fabrication cost and/or area) are considerable. In this paper, we introduce nanopyramid structures that mitigate optical probing attacks by scrambling the measurements reflected by a laser pulse. Nanopyramid structure is applied to selected areas inside an IC that requires protection against optical probing attacks. The fabrication of nanopyramids is CMOS compatible and well established for photovoltaic applications. We design the nanopyramid structure in ICs, develop the LVP attacking model, and perform optical simulations to analyze the impact of nanopyramids on LVP. According to the simulation results, the nanopyramid can disturb the optical measurements enough to make LVP attacks practically infeasible. In addition, our nanopyramid countermeasure has no area overheads and works in a passive mode without consuming any energy.

I. Introduction

Over the past two decades, optical probing techniques have been developed for failure analysis of integrated circuits (ICs) with the photon emission microscopy (PEM) and later laser voltage probing (LVP) [1]–[3]. These techniques are based on the measurement of optical signals, and thus are considered as "contactless" probing. Although such techniques are greatly helpful for signal tracking and understanding the functionality of ICs for failure analysis and debug, they can also be used to perform attacks and cause serious security concerns. Reported studies have shown that PEM and LVP can read the information from memory cells, registers, and hardware security primitives such as physical unclonable functions (PUFs) [4]– [6].

To perform such attacks, the adversaries firstly need to have knowledge about the layout of the device under test (DUT). At a minimum, transistors, memory cells and registers should be localized to an area of interest (AOI). They should also have access to the equipment needed to acquire clear optical images of the DUT, such as a photon emission microscope. Optical signals may then be collected from the AOI, usually when the DUT is working, analyzed, and used to extract the sensitive information such as cryptographic keys, proprietary firmware, or unencrypted bitstreams. For example, in typical complementary metal-oxide-semiconductor (CMOS) devices, there is significant current only when the transistors are switching. The current transportation is fulfilled by the recombination of electrons and holes in transistors, which results in photoemission that directly indicates the switching of transistors. Since modern IC device feature sizes are below the wavelength of the light used by optical microscopes (from visible to infra-red), solid-immersion-lenses (SIL) have been used to improve the spatial resolution of imaging [7]. Meanwhile, with smaller transistor channel size and decreasing supply voltage, the inherent photon emission from each transistor and logic gate is significantly reduced [8], making the detection more difficult. Therefore, later techniques such as LVP employ external laser source to provide more photons for probing [3]. Novel imaging techniques such as phase lock scanning in frequency domain have also been developed [9], [10]. There are other optical attacks like laser fault injection [11], [12] that do not necessarily require optical images of the AOI. Instead, they analyze the changes in the IC output caused by the faults to derive secret information. Note that such attacks are outside the scope of this paper. Here we focus on probing attacks that are based on optical measurements obtained by the aid of a laser.

Several countermeasures against the optical probing attacks have been proposed. For example, a protective optical layer was coated on the backside of the dies, while light emitting diodes (LEDs) and photon detectors are fabricated on the front side [6]. The protective layer reflects the light from the LEDs and the reflection is monitored by the photon detectors. Any silicon thinning occurring on the backside that is necessary for optical attacks will damage the layer and change the reflection, thus can be captured by the detector. This technique provides a general solution against the backside attacks, but may require costly steps to integrate the LEDs and detectors into standard complementary metal–oxide–semiconductor (CMOS) circuits. In other research [13], [14], ring-oscillator PUFs (RO-PUFs) were utilized as sensors to capture incident laser signals to trigger the alarm on attacks. In such designs, the RO-PUFs represent additional overhead and need to be placed close to the protected circuits. In addition, all the countermeasures mentioned above work in active mode. In other words, the sensors require additional power to detect the attack and self-destruct sensitive data upon detection.

In this paper, we introduce nanopyramid structures into transistors to scramble the optical measurements during the attack, and consequently protect the sensitive information from

being revealed. We summarize our major contributions as follows:

- We propose nanopyramid-based security design that works in completely passive mode, without consuming any extra power.
- We integrate nanopyramids into the standard CMOS fabrication flow and introduce several optional techniques for the fabrication.
- We perform optical simulations to demonstrate that the nanopyramids can strongly disturb the light reflection from transistors and discuss how this can be used as a countermeasure against optical probing attacks.
- We are planning on the fabrication of nanopyramid devices to demonstrate the scrambling in silicon.

The rest of this paper is organized as follows. In Section II, we introduce the background of optical probing attacks and silicon nanopyramids. In Section III, we describe the structures of CMOS devices with nanopyramids embedded. The fabrication processing is also discussed. In Section IV, simulation results obtained from standard transistors and those with nanopyramid-embedded are compared. Then in Section V, we discuss how the nanopyramids can help protect the information from LVP attacks. Finally, the conclusion is given in Section VI.

II. Preliminaries

A. Optical Probing Attacks

In contrast to destructive reverse engineering, optical attacks typically require a working device to extract the desired secret information. Therefore, the entire circuit should be maintained functional. Due to the materials optical properties, the optical signals used for the attack are from semiconductors (i.e., transistors made from silicon in most cases). Due to the complex and dense metal structure on the front side of modern CMOS devices that blocks light from the silicon, most optical attacks are performed from the backside. First, the backside of the IC needs to be exposed (through partial decapsulation) so that the light has access to/from the active region of the die. Then, the thick silicon substrate (about a few hundreds of microns) must be thinned down to a few microns without destroying the diffusion layer. At that thickness, infrared (IR) photons with wavelength longer than 1000 µm in air can effectively pass through. Although recent technology nodes are entering the sub-10 nm region, which is way below the resolution of optical microscope, attack targets such as memory cells or registers are comparably larger and thus can still be spatially distinguished by the microscopy. Meanwhile, SIL is used to further improve the spatial resolution, making the visible-IR optical attacks even possible for 10 nm technology nodes [6].

Photon Emission Microscopy (PEM) is a popular optical probing technique [5], [6]. The photon emission in IC devices mainly occurs when transistors are in saturation mode. In digital CMOS devices, transistors go into saturation mode only when they are switching; hence the photon emission is directly related to the transistors operating status which can leak sensitive information. Since photon emission strongly depends on the bias voltage, it has been significantly reduced on modern CMOS devices that operate at lower supply voltages. With decreasing supply voltage, the photon emission is expected to be further reduced, making the PEM attacks more and more difficult on latter CMOS devices.

Laser Voltage Probing (LVP). It has been known for decades that the carrier distribution in semiconductor materials impacts the optical properties of the materials [15]. In CMOS devices, the changes of carrier distribution are controlled by the applied voltage (i.e., signal/data, as shown in Fig. 1), which can thus be probed by monitoring for changes in optical images. An early study on optical modulation as a voltage probe for CMOS devices was first reported in the 1980s [16]. Ten years later, laser was used as a probe to detect the voltage applied on semiconductor devices for failure analysis and was referred to as LVP for the first time [17]. Recently, this technique has been discussed for semi-invasive physical attacks on hardware [18]. With LVP, the cells in the CMOS device can be imaged in time domain or in frequency domain [9]. The LVP imaging in frequency domain is also called laser voltage imaging (LVI) to distinguish it from the traditional LVP imaging in the time domain.

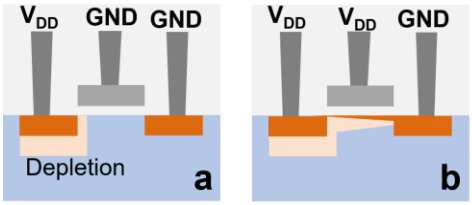

Fig. 1: Transistor cross section under different bias voltages. The carrier distribution changes with bias voltage, and thus changes the optical properties of the materials. By measuring the changes, the semiconductor devices operating mode can be captured.

Typical targets of optical probing attacks are memory cells, registers, and PUFs that process sensitive data, e.g. secret keys. As PEM attacks are more challenging on scaled-down CMOS devices, we focus our discussion on LVP attacks. Here, we consider an LVP attack on an 8-bit register based on D-type flip-flops (FFs) as a running example. The register includes eight flip-flops, corresponding to Bit 1 - Bit 8. To find out the value of Bit 1, the laser beam (typical spot size about 1 μm^2) is aimed directly on back of the first flop-flop (FF4), vertically entering the device. The light will be diffused and scattered in the materials. Some of the light is absorbed, some transmitted, and the rest is reflected. As the optical system cannot exclude the reflections from neighbor regions, the total reflection signal is collected from a region (i.e., the field of view of the microscope) wider than the target area. However, due to the planar layer structure of CMOS devices,

only a small part of the light is scattered to/from neighboring ones (e.g., FF2 - FF8); thus the reflection signal is mainly conveying the status of FF4, as shown in Fig. 2. The same argument applies to the remaining bits (FF2 - FF8) when the laser is centered on them. When the 8-bit register is waiting for input (we refer to this as "waiting period"), the voltage applied on all the bits (FF1-FF8) is the same. Assuming the outputs are "0", the intensities of the reflection signals from FF1-FF8 are close to each other (generally dark in Fig. 2, reflections from standard CMOS devices). When the register is fetching and outputting data (e.g., secret key), the voltage applied depends on the input and output value (we refer to this as "outputting period"). The reflection of the flip-flops corresponding to "0" outputs does not change from the "waiting period", while the reflection of those corresponding to "1"s changes due to re-distributed carriers in silicon. Although variations may be present (depicted in Fig. 2 by different grayscales) because of the process variations of materials properties (e.g. doping, geometry, etc.) and background noise, differential reflection analysis (by calculating $\Delta R(i) = R'(i) - Ro(i)$) can effectively eliminate the variations and thus clean signals can be obtained.

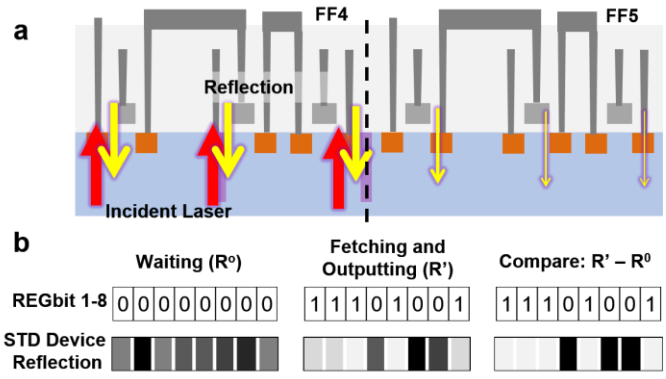

Fig. 2: Standard device: (a) the reflection of the laser mainly depends on the status of the illuminated flip-flops (FF4), hardly affected by the neighbor ones (FF5) and (b) by observing the reflection changes from "waiting" to "outputting" ($\Delta R(i)$), each bit value corresponding to each flip-flop can be revealed.

For convenience, we define R(i) as the reflection measured from the DUT when the laser beam is located on the ith flip-flop (FF i). We use superscript "o" (i.e., Ro) and apostrophe (i.e., R') to denote measurements during the "waiting period" and the "outputting period", respectively. In the following discussion, subscript "STD" and "NP" are also used to represent standard CMOS devices and those with nanopyramids, For instance, R'NP2(4) is the reflection measured on nanopyramid device No.2, when the laser is located on FF4 and the register is outputting the key. The difference of reflection between Ro(i) and R'(i) for a given key, e.g. (0010 1001), is written as ΔR0010 1001(i).

B. Nanopyramids

Because of anisotropic crystal structures, many crystal materials present different chemical reaction activities on different facets. For example, the etching rate of crystal silicon in chemical etchants (wet etching), such as potassium hydroxide (KOH) and tetramethylammonium hydroxide (TMAH), is fast on (110) and (100) facets but very slow on {111} facets [19]. Give a surface of Si(100) or Si(110) on most silicon wafers for electronic devices, such anisotropic etching eventually ends with Si{111} facets presenting on the surface, textured in pyramid structure [20]. The morphology of the pyramids can be controlled by using a mask during etching [21]. Besides wet etching, dry etching such as reactive ion etching (RIE) can also be used on silicon to obtain textured surfaces [22]. Because such pyramid texture structure can dramatically increase the scattering of incident light on the surface, it has been widely used in solar cell fabrication as one part of surface treatment to enhance the light harvesting.

C. Design

As discussed in Section II-A, a successful LVP attack on a register is based on a reliable measurement of the laser beam reflection relative to the register bit switching. The security design goal in this study is to scramble the measurement during LVP attacking. To realize this objective, we propose to insert randomly distributed silicon nanopyramids in the CMOS devices to interfere with the light absorption, scattering, and reflection (Fig. 3a). Considering the 8-bit register example again, two effects can be expected due to the nanopyramids: 1) the reflection from FF1 - FF8 now varies randomly due necessarily correspond to the switching of FF i, but can arise from neighbor ones (FF j, where j is not equal i), as shown in Fig. 3.

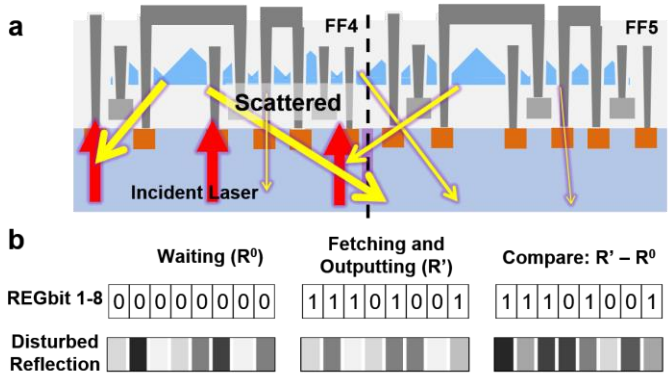

Fig. 3: Nanopyramid device: (a) incident laser is scattered around, leading to the reflection includes the light from not only the illuminated flip-flop (FF4) but also the neighbor ones (FF5) and (b) revealing the bit values become difficult since the observation of reflection changes ($\Delta R(i)$) is scrambled

To sufficiently diffuse the light reflection, the nanopyramids should be prepared as close to the transistor layer as possible. They can be placed above or below the transistors. In the former case, pyramids could be inserted between transistor layer and Metal 1 layer. One concern for such a structure is that the pyramid silicon layer may result in shorts among vias/contacts. To avoid shorts, the CMOS processing should be modified, as shown in Fig. 4. Compared to standard CMOS

processing, the sidewall surface of the vias between transistor layer and Metal 1 layer should be coated with insulating materials (e.g., silicon oxide or silicon nitride) by atomic layer deposition to prevent shorts between vias caused by the nanopyramids (Fig. 4f). Then, anisotropic etching should be performed to expose the bottom vias, and to allow good electrical contact (Fig. 4g) for the subsequent via filling. Nanopyramids can be inserted below transistors for silicon on insulator (SOI) wafers fabricated by the bonding-based processing. In this case, the nanopyramids can be easily incorporated in the insulator layer under the transistors before the bonding of surface crystal silicon layer, without any concerns of shorts, as shown in Fig. 5. For simplicity, we consider the structure above the transistors throughout the rest of the paper. As the nanopyramid structure is placed either above or beneath the active register-transistor-layer (RTL), the structure and the performance of the transistors are not impacted. In other words, the nanopyramid structure can be applied on Fin-FET structure as well.

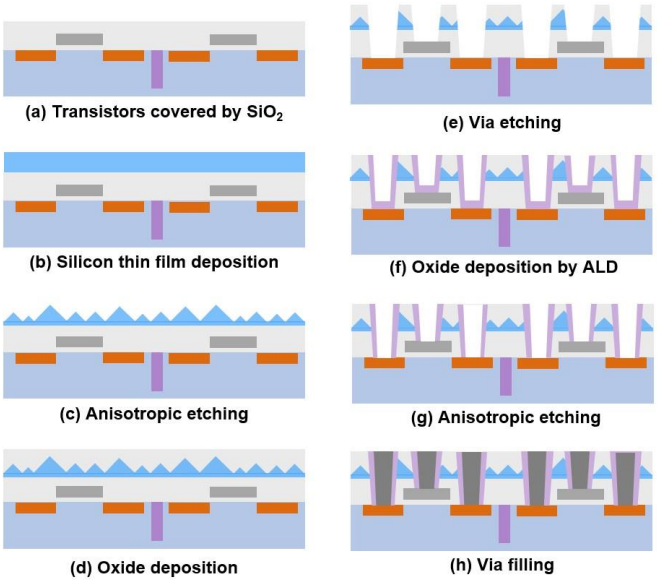

Fig. 4: Modified fabrication steps for nanopyramid CMOS devices: (a) transistors covered by oxide, (b) silicon thin film deposition, (c) anisotropic etching of silicon thin film to form nanopyramid structure on protected area while the rest area covered by mask to prevent the etching, (d) oxide deposition followed by CMP polishing, (e) via etching, (f) ALD deposition of isolation layer, (g) anisotropic etching to expose the via bottom, and (h) via filling.

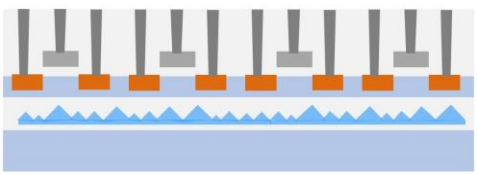

Fig. 5: Nanopyramids in bonding-based SOI devices.

IV. Modeling and Results

A. Modeling

To evaluate the influence of nanopyramid design, optical simulations based on metal gate 16nm CMOS devices are performed. The details are described below.

Attack. In this study, we assume that an 8-bit secret key is fetched by a flip-flop based 8-bit register in parallel mode and the register is the target under LVP attack. The attacker will scan the laser beam from FF1 to FF8. When the laser beam is located on FF4 for instance, the attacker observes the reflection by optical microscope system. Once a change higher than the preset critical value observed, the attacker assumes the change is caused by a switching (0→1 transition) that occurs on the corresponding FF4, which means the 4th bit of the key is 1. By repeating this processing on all the register bits, all bits of the secret key are eventually guessed.

Device. To simulate the attack, we use an 8-bit register based on D flip-flop for the secret key fetching and outputting. In each D flip-flop, the regions where charge carrier distribution changes during the 0→1 switching are counted according to the layout. The corresponding carrier concentration changes are calculated based on the drain/source/well doping densities and the applied voltage from PTM 32nm HP Model Card [23]. A compact D type flip-flop layout design [24] is used for a case study. The area of each flip-flop is about 6 µm. Fig. 6 illustrates that the laser beam is located on FF4 to read the bit information.

Pyramid. In this study, we assume the silicon thin film prepared for the pyramids preparation is crystal and in (100) plane. Then the inclination facets after etching are {111} planes. The angle between the bottom and the facets is about 54o. The size of the pyramids is controlled in the range of 10-400 nm. Because of the angle between crystal planes are constant, the height of the pyramids depends on the size. Based on these, the size and the location of the pyramids are generated randomly, following a normal distribution. The settings here can be modified for silicon thin films prepared under different conditions. For example, the silicon thin film grown by popular techniques such as low pressure chemical vapor depositions (LPCVD) is typically poly-crystalline rather than single crystal. After the etching, the orientation of the pyramids may vary accordingly. The size and the distribution of the pyramids can be control by a surface mask during the etching. The height of the pyramids can also be modified by chemical mechanical planarization (CMP).

Optical parameters. The wavelength of the laser is set as 1064 µm, which is the one most commonly used for LVP attacks. Once the carrier distribution in the register is determined, materials refractive index (n) and extinction coefficient (k) [25] are used for the reflection calculation. Since the change of free carrier density in insulating materials (e.g., silicon oxide and high k materials) and metals (e.g. tungsten and copper) are negligible, we only consider the changes of silicon's n and k during the flip-flop switching. The changes of silicon's n and k can be described by [26]:

$$\Delta n = -\frac{e^2\lambda^2}{8\pi^2 c^2 \epsilon_0 n}\left(\frac{\Delta N_e}{m^*_{ce}} + \frac{\Delta N_h}{m^*_{ch}}\right) \quad (1)$$

$$\Delta\alpha = \frac{\omega}{c}\Delta k = \frac{e^2\lambda^2}{8\pi^2 c^2 \epsilon_0 n}\left(\frac{\Delta N_e}{m^{*2}_{ce}}\mu_e + \frac{\Delta N_h}{m^{*2}_{ch}}\mu_h\right) \quad (2)$$

where e is the elementary charge, λ is the light wavelength in air, c is the light speed in air, ε0 is the vacuum permittivity, ΔNe is the change of electron carrier concentration, ΔNh is the change of hole carrier concentration, m∗ce is the effective mass of one electron carrier, m∗ch is the effective mass of one hole carrier, µce is the mobility of one electron carrier, µch is the mobility of one hole carrier, and ω is the angular frequency of the light.

B. Simulation Observations

The simulation is firstly performed on both standard devices and nanopyramid devices when the register is not fetching the key from memory and the outputting of all the flip-flops is 0. Partial cross-sections of the standard register and the nanopyramid register are shown in Fig. 7, with laser beam located on FF4 of each one. For consistency, we always put the laser beam on FF4 in the following discussion, which means i is 4 in all examples discussed in this paper. The color scale from red to blue corresponds to normalized light intensity from 1 to 0. As we can see from the standard device, given the normally incident laser beam, the light path is quite regular and symmetric. The light is confined over a relatively small region. Only a small portion of the light spread to neighbor flip-flops (e.g. FF2, FF3, FF5, etc.). While on the nanopyramid device, the light scattering is dramatically increased. Instead of symmetric distribution, the light intensity distribution is highly disordered, which can be attributed to the randomly distributed and sized nanopyramids. It is clear on the simulation results that a considerable amount of the incident light is scattered in the device and reaches cells far away. Simulation in larger scale shows the pyramids scatter the light to cells that are further than several tens of microns.

Switching on Standard Devices. When the register is fetching the 8-bit secret key from memory, the flip-flops switch according to the bit values of the key. For this case study, we set the laser beam on FF4. To investigate the reflection behavior used for the LVP attack, we assume the laser beam is moved from FF1 in the register to the last one (FF8). When the laser beam is located on one FF i (i is 1-8), we switch every flip-flop one by one to study the "individual switching impacts" on the reflection. For instance (see Table I), when the laser is on FF4, FF1 switches (0 → 1) first. The switching, as discussed above, leads to optical property changes and results in reflection changes. By calculating ΔR(4) when only FF1 is 1 (i.e. given key as 0000 0001 in binary or 1 in decimal), we can see whether the individual switching of FF1 will affect the reflection in a detectable way. Such calculation and comparison are carried out for all the flip-flops. The results obtained from the standard register is summarized in Table I and shown in Fig. 8(left). As illustrated, when the laser beam is located on FF4, only the switching of FF4 causes a considerable change in reflection, while the reflection change from the switching of other flip-flops is much less. A criteria (Cr.) can thus be easily set (e.g., $\Delta R_{STD}(4) > 2\times10^4 V^2/m^2$) for key bit (KB) guessing: if a reflection change larger than 2 × 104 V 2/m2 is observed with laser beam on FF4, then the 4th bit of the key (KB4) is 1. Otherwise KB4 is 0. The observation and guessing process is summarized in Table I (Column 3 and 4). According to simulations performed with laser beam located on other flip-flops (FF2 - FF8), similar observation results are obtained.

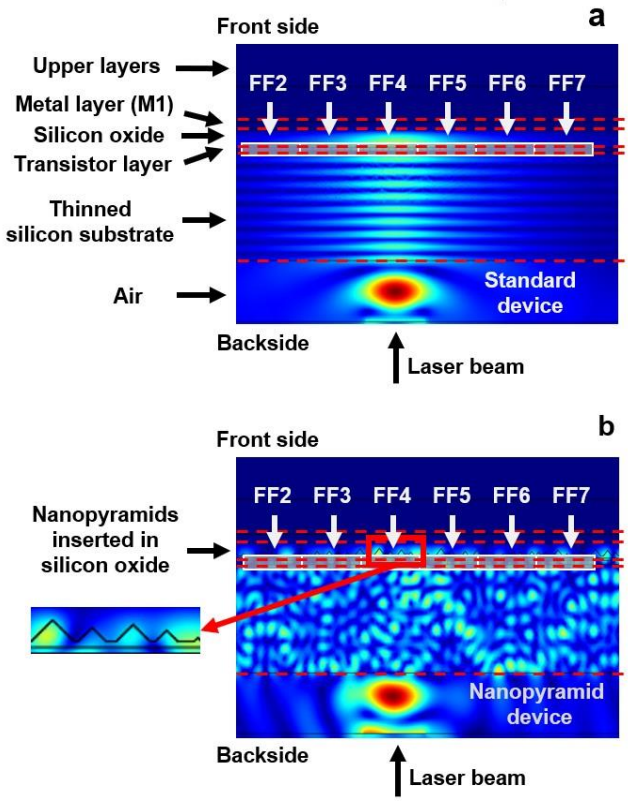

Fig. 7: Optical simulation of the laser reflection from (a) standard device and (b) nanopyramid device.

In practical cases, the 8-bit secret key can be from 0 to 127. Keeping the laser beam on FF4, we calculate $\Delta R_{STD}(i)$ for every possible key value (i.e. 0 - 127) and plot the results in Fig. 8(right). The red data points present those with KB4 of "1", while the blue ones present those with KB4 of "0". As shown, all the red spots come with significantly higher $\Delta R_{STD}(4)$ than all the blue ones, which means when the laser beam is on FF4, as long as the KB4 is "1", increasing reflection can be observed, regardless of the values of other key bits. Very similar results are obtained from cases with the laser beam located on other flip-flops. A clear and constant criteria ($\Delta R_{STD}(i) > 2 \times 10^4 V^2/m^2$) is thus found to be used for guessing all the bit values with high confidence, indicating the feasibility of efficient LVP attacks on the standard register.

Switching on Nanopyramid Devices. When the nanopyramid layer is inserted in the device, the light reflection significantly depends on the geometry and distribution of the pyramids. To study the reflection behavior, we randomly generate the nanopyramid layer for 100 devices and calculate the reflection

changes along with the flip-flops switching. The results from four representative samples are plotted in Fig. 9.

Table 1: Guessing KB4 on Standard Devices.

Switching FF	Reflection Diff.	Guessing (bit 4)
FF1	$R_{std}^{0000\,0001}(4) - R_{std}^{o}(4) < Cr.$	0 (Correct)
FF2	$R_{std}^{0000\,0010}(4) - R_{std}^{o}(4) < Cr.$	0 (Correct)
FF3	$R_{std}^{0000\,0100}(4) - R_{std}^{o}(4) < Cr.$	0 (Correct)
FF4	$R_{std}^{0000\,1000}(4) - R_{std}^{o}(4) > Cr.$	1 (Correct)
FF5	$R_{std}^{0001\,0000}(4) - R_{std}^{o}(4) < Cr.$	0 (Correct)
FF6	$R_{std}^{0010\,0000}(4) - R_{std}^{o}(4) < Cr.$	0 (Correct)
FF7	$R_{std}^{0100\,0000}(4) - R_{std}^{o}(4) < Cr.$	0 (Correct)
FF8	$R_{std}^{1000\,0000}(4) - R_{std}^{o}(4) < Cr.$	0 (Correct)

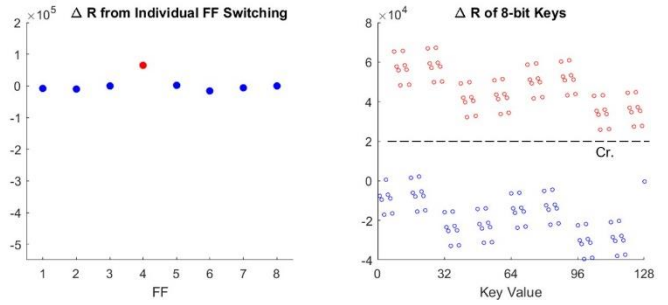

Fig. 8: Simulated $\Delta R_{STD}(4)$ from the individual switching of FF1 - FF8 (left) and all possible 8-bit keys (right). Data points in red means FF4 switches (KB4=1) and the blue means the opposite (KB4=0).

As shown in Fig. 9a(left), we can see that the switching occurring on FF5 and FF8 in device Nanopyramid 1 result in reflection changes (ΔR_{NP}11000 0000(4) and ΔR_{NP}10001 0000(4)) that are comparable to the change resulted by FF4 switching ((ΔR_{NP}10000 1000(4)). This can be explained via the enhanced scattering from the pyramid structure. As described in II-A, during the observation, light reflection is collected from a region much larger than the whole register. The influence of neighbor flip-flops is incorporated in the reflection measurement. On the standard device, when the laser is located on one flip-flop (e.g. FF4), only a small part of the incident light is dispersed to neighbor flip-flops and reflected. Although the light reflected from the neighboring ones carries the neighbor flip-flops' switching information, its weight in total reflection signal is too low to disturb the interpretation of the illuminated flip-flop (FF4). On nanopyramid devices, unlike in the standard device, a considerable amount of incident light is dispersed to neighbor flip-flops in the nanopyramid device (Fig. 7b). As there is much more light dispersed to the neighbors, the weight of one neighbor flip-flop's influence can be much higher during the interpretation compared to that of the standard device. If the weight is so high that it is comparable to the weight of the illuminated one (FF4), the reflection changes from the neighbor flip-flop switching present in the observation and thus can interfere the interpretation of FF4. Following the standard LVP attacking strategy, the attacker has to assume that any observed increasing reflection with laser beam located on FF4 means the KB4 is 1 (FF4 switching).

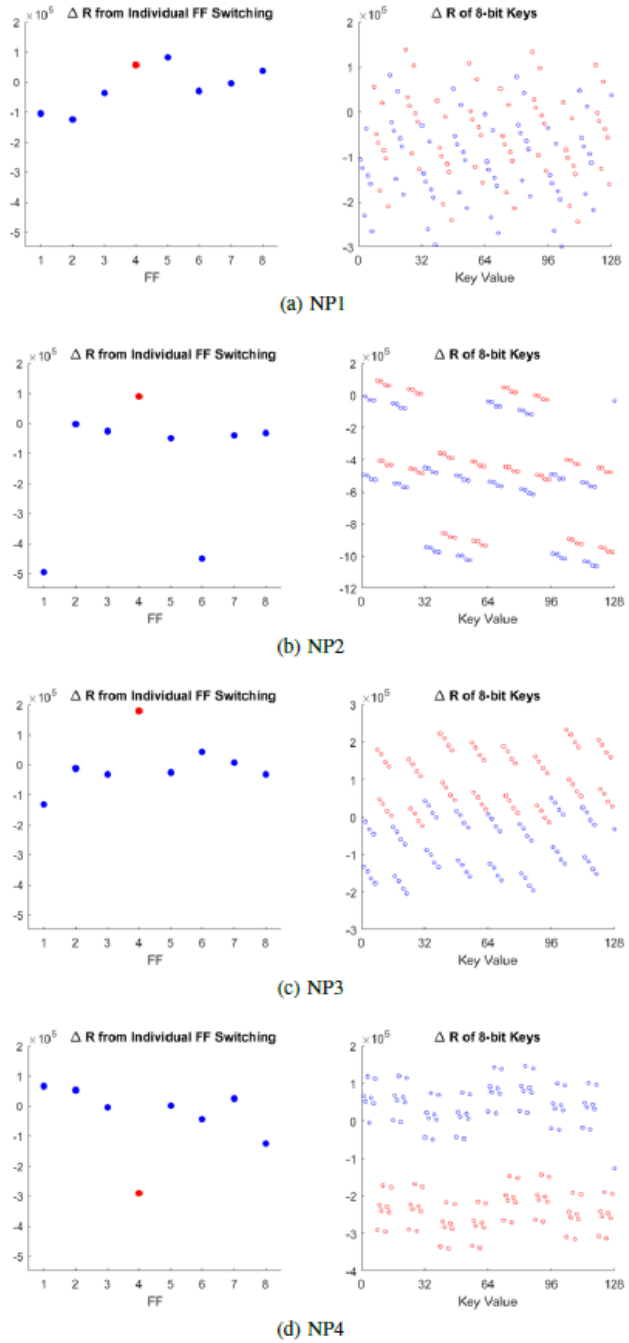

Fig. 9: Simulated $\Delta_{RNP1}(4)$ - $\Delta R_{NP1}(4)$ from the individual switching of FF1 - FF8 (left ones) and all possible 8-bit keys (right ones). Data points in red means FF4 switches (KB4=1) and the blue means the opposite.

However, given the fact that the switching of FF5 or FF8 also increases the reflection, the attacker is mislead, which could result in a prediction error (Table II). This is just for one bit (KB4) out of an 8-bit key. The differential reflections

($\Delta R_{NP1}(4)$) for every possible key value with laser beam on FF4 are also plotted in Fig. 9a (right). As seen, it is impossible to set a single criterion that separates the data points with KB4 is "1" and "0" for all simulated devices.

Instead of increasing the total reflection, the switching flip-flops in a nanopyramid device sometime reduces the total reflection (i.e. $\Delta R_{NP} < 0$, e.g. FF1 and FF6 on Nanopyramid 2 in Fig. 9b (left)). Because of the optical property, flip-flop switching from "0" to "1" increases the reflection index (n) of affected materials and thus increases light reflection "locally". In the nanopyramid devices, if the increasing local reflection deviates from the normal direction because of the pyramids, the light may need to travel longer in the device materials the light may need to travel longer in the device materials before leaving the device and being measured. The increasing local reflection on FF4 actually makes more incident light travels longer, thus leads to more light absorption and eventually reduces the "total" reflection. For Nanopyramid Device 2, although the FF4 switching still increases the total reflection as it does in a standard device, the FF1 and FF6 reduce the total reflection when switching, which makes it is impracticable to discriminate the keys with KB4 of "1" and "0", as shown in Fig.9b (right).

Table II: Guessing KB4 on Nanopyramid Devices

FF Switched	Reflection Diff.	Guessing KB4
FF1	$R_{NP1}^{0000\,0001}(4) - R_{NP1}^{o}(4) < Cr.$	0 (Correct)
FF2	$R_{NP1}^{0000\,0010}(4) - R_{NP1}^{o}(4) < Cr.$	0 (Correct)
FF3	$R_{NP1}^{0000\,0100}(4) - R_{NP1}^{o}(4) < Cr.$	0 (Correct)
FF4	$R_{NP1}^{0000\,1000}(4) - R_{NP1}^{o}(4) > Cr.$	1 (Correct)
FF5	$R_{NP1}^{0001\,0000}(4) - R_{NP1}^{o}(4) > Cr.$	1 (Wrong)
FF6	$R_{NP1}^{0010\,0000}(4) - R_{NP1}^{o}(4) < Cr.$	0 (Correct)
FF7	$R_{NP1}^{0100\,0000}(4) - R_{NP1}^{o}(4) < Cr.$	0 (Correct)
FF8	$R_{NP1}^{1000\,0000}(4) - R_{NP1}^{o}(4) > Cr.$	1 (Wrong)

For some nanopyramid devices, the laser illuminated flipflop (e.g., FF4) may play the most important role in the light reflection, but the ΔR is still affected more or less, leading to a less efficient LVP attack. In the case of Nanopyramid Device 3, we notice that $\Delta R_{NP3}(4)$ caused by individual FF4 switching is high. However, when FF1 switching occurs with FF4 switching, the effective $\Delta R_{NP3}(4)$ is reduced. As shown in 9c (right), some red data points (KB4 is "1") indicate similar $\Delta R_{NP3}(4)$ with some blue data points (KB4 is "0"). Since the attacker only has very limited number of data points, it is difficult to optimize the guessing criteria to achieve a high accuracy.

In a few cases, the switching of the illuminated flip-flop (e.g. FF4) still dominates the ΔR, as shown in 9d(right). However, in the example of Nanopyramid Device 4, the negative $\Delta R_{NP4}(4)$ from FF4 makes it is possible to discriminate the keys with Bit 4 of "1" from the keys with KB4 of "0", by setting the criteria as $\Delta R_{NP4}(4) < -1{\times}10^5\ V^2/m^2$.

V. Security Analysis

As discussed in II, key fetching which is usually realized by registers is the typical target of the LVP attack. Since the registers discussed in this study are for secret key fetching, it is reasonable to assume that the attacker does not have direct access to feed the register with different inputs to study the reflection behavior. With that assumption, when the register fetches the secret key value in a parallel way (e.g., 8-bit register to fetch a 8-bit key), the attacker is able to obtain only two reflection measurement results from one flip-flop: one is during the "waiting" ($R^o(i)$) and one is during the key outputting ($R'(i)$). During the attack, the attacker first assumes that the illuminated flip-flop (FF i) switching always causes significant $\Delta R(i)$ while the other flip-flops (FF j, where $j \neq i$) switching has insignificant influence on $\Delta R(i)$. This means that a significant $\Delta R(i)$ has to be from the switching of the illuminated flip-flop (FF i), but not resulted by the switching of the neighbor flip-flops (FF j, where $j \neq i$). This is the fundamental assumption of the LVP attack. Based on this assumption, a criterion (Cr) is further required to evaluate the significance: if the $\Delta R(i) > Cr$ (when $Cr > 0$) or $\Delta R(i) < Cr$ (when $Cr < 0$), the flip-flop is switched and the correspond Key Bit is "1". Otherwise, the Key Bit is "0".

On the standard devices, the Cr_{std} that is valid and applicable for all flip-flops is easy to be found as all the devices reflection behaviors are very close to each other. To attack the standard register, the attacker basically measures the $R^o_{STD}(i)$ and $R'_{STD}(i)$, calculates $\Delta R_{STD}(i)$ (= $R^o_{STD}(i) - R'_{STD}(i)$), tests $\Delta R_{STD}(i)$ with the Cr_{STD}, and tell if the KBi (FF i) is "0" or "1". However, when the attack is performed on nanopyramid registers, two factors, including the large variation of $\Delta R_{NP}(i)$ and the possible significant $\Delta R_{NP}(i)$ form neighbor flip-flops (FF j, where $j \neq i$), make the attacking extremely difficult.

On nanopyramid devices, the simulation results show that the $\Delta R_{NP}(i)$ varies from device to device. It can vary from negative to positive, in a much wider range compared to that on the standard devices (Figs. 8 and 9). Such an enhanced variation of $\Delta R_{NP}(i)$ makes the choice of Cr_{NP} difficult. The bigger problem for the attacker is the significant $\Delta R_{NP}(i)$ from neighbor flip-flops FF j ($j \neq i$), which invalidates the fundamental assumption of the LVP attack: the significant $\Delta R_{NP}(i)$ does not necessarily mean the switching of the illuminated flip-flop (FF i) any longer, as described in Section IV-B.

When a secret key, e.g., 0101001 (41 in decimal), is given on STD, NP1 and NP4 devices. $\Delta R_{STD}(4)$ of 4.2×10^4, $\Delta R_{NP1}(4)$ of -6.5×10^4, and $\Delta R_{NP4}(4)$ of -2.5×10^5 are observed on the STD, NP1 and NP4 devices, respectively (Figs. 8 and 9). Using the constant criteria "$\Delta R_{STD}(i) > 2 \times 10^4 V^2/m^2$" for the STD one, the attacker can tell the KB4 is "1" (FF4 switched) with confidence. However, the clue to guess the KB4 on NP1 and NP4 is lacking. The attacker can still try to use Cr_{STD} obtained from standard devices for nanopyramid devices, but this does not help to get the correct guessing results for all devices.

If the key bit length is longer, such as 128 bit, and/or there are multiple keys, using one 8-bit register for the fetching of key(s) will process the data in patches sequentially. This allows the attacker observe the device reflection behavior with different outputs. Given enough observations, the attacker is able to estimate the distribution of the ΔR_{NP} (i) and figure out a more reasonable Cr_{NP} (e.g., the average value of ΔR_{NP} (i)). For instance, on both of NP1 and NP4, 16 keys (0010 1000 - 0011 1000, i.e. 40 - 56) are fetched and outputted by the 8- bit register sequentially. $\Delta R_{NP1}(4)$ varying from -2.5×10^5 to 0.6×10^5 and $\Delta R_{NP4}(4)$ varying from -3.4×10^5 to 0.9×10^5 are observed. Based on the observation, Cr_{NP1} and Cr_{NP4} are set as $< -0.95 \times 10^5$ and $< -1.25 \times 10^5$, respectively, by averaging observed $\Delta R_{NP}(4)$. For NP4, as the $\Delta R(4)$ is significant ONLY when FF4 switches, the Cr_{NP} 4(4) defined in this way allows the guessing of KB4 have a high chance (~ 1) of being correct. While on NP1, as the fundamental assumption is not valid, the $Cr_{NP1}(4)$ does not efficiently improve the probability of guessing KB4 correctly from random guessing, which is 0.5.

To statistically evaluate the probability of guessing based on allowed observations, we perform simulations of 100 nanopyramid devices (8-bit registers). On each device, we allow observations of $\Delta R_{NP}(4)$ based on random key values (RKs), with the number of different keys as 0, 4, 16, 64, and 128. For "0" observation, Cr_{STD} from standard device is used, otherwise Cr_{NP} is set as the mean value of all observed $\Delta R_{NP}(4)$. We should clarify again that according to the assumption that the attacker does not have the direct electrical access to the register, he obtains the observation results ($\Delta R_{NP}(4)$) without knowing the value of input random keys for the register under attack. With Cr established, we consider another target key (TK) that the attacker wants to reveal and test if the value of KB4 can be correctly revealed based on the corresponding ΔR_{NP}^{TK} (4).

The results from the devices based on the complete 128 observations are plotted in Fig. 10. As seen, although about 20% devices allow a high confident guessing, the majority devices (>60%) give a guessing rate around 0.5. The probability of guessing KB4 given different allowed observations is summarized in Table III. It shows that although more observations improve the probability of guessing, the improvement is very limited (from 0.6209 of "0" to 0.6695 of "128"). Similar results are obtained from other flip-flops, giving the chance to get the correct 8-bit key only about 0.04 even with 128 observations obtainable. It is worth noting that for the attacker, the observations of $\Delta R_{NP}^{TK}(i)$ (i is 1 - 8) only gives one predicted 8-bit key. If the predicted key turns out to be wrong, the attacker needs to make another guess, which is not based on the observation results anymore. The probability of 0.04 listed does not mean the 8-bit key can be expected to be revealed after 25 rounds of guess and test. In addition, the probability of guessing can be further diminished easily in practical circuits, by using registers with longer bits and/or limiting the number of different keys fetched by one register.

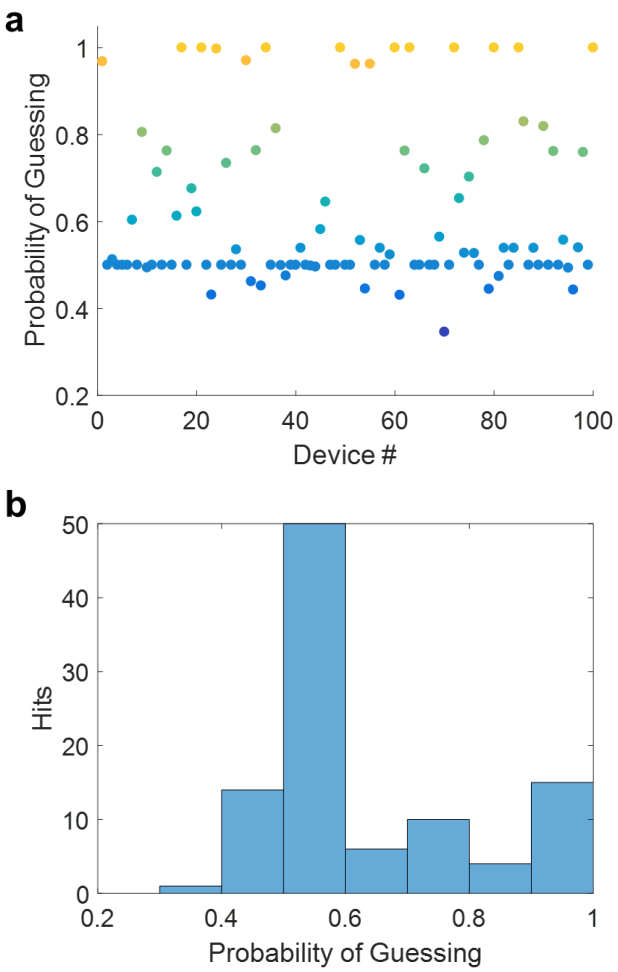

Fig. 10: The probability of guessing the KB4 of random 8-bit keys from 100 nanopyramid devices based complete reference observations (a) and the histogram (b).

Table III: Probability of guessing based on different allowed reference observations.

Obs.	0 (STD)	4	16	64	128
1 bit	0.6209	0.6294	0.6425	0.6588	0.6695
8 bit	0.0221	0.0246	0.0290	0.0355	0.0404

VI. Conclusion

In this paper, we proposed to use Si nanopyramids as a scrambler to protect the critical information in ICs, by interfering the optical measurement during the back side optical probing attacks. To achieve this goal, the nanopyramids are inserted between the transistor layer and metal layer 1. If the device is fabricated on bonding-based SOI wafer, the nanopyramids can be placed in the isolating layer beneath the transistors instead. The nanopyramid structure is applicable to both planar transistors and Fin-FETs. The fabrication is compatible to CMOS processing with several inexpensive steps and no extra mask is required. The optical simulation results from the standard device and the

nanopyramid devices demonstrate that the reflection behavior of the devices is changed due to the enhanced scattering arise from the pyramids. Because of the randomness of the nanopyramids, in terms of size and dislocation, the optical reflection collected the nanopyramid devices is not reliable to be used to reveal the corresponding circuit (e.g. flip-flops) status. As a result, an efficient LVP attack can be prevented.

Acknowledgment

This project was supported in part by an AFOSR MURI grant under award number FA9550-14-1-0351.

References

Literature references are numbered in the order of their appearance in the manuscript and are confined by brackets. They are listed at the end of the manuscript using the "ISTFA References" format. Here is an example of the correct format.

[1] C. Boit, R. Schlangen, U. Kerst, and T. Lundquist, "Physical techniques for chip-backside ic debug in nanotechnologies," IEEE Design & Test of Computers, vol. 25, no. 3, 2008.

[2] A. Schlo¨sser, D. Nedospasov, J. Kra¨mer, S. Orlic, and J.-P. Seifert, "Simple photonic emission analysis of aes," in International Workshop on Cryptographic Hardware and Embedded Systems. Springer, 2012, pp. 41–57.

[3] H. Lohrke, S. Tajik, C. Boit, and J.-P. Seifert, "No place to hide: Contactless probing of secret data on fpgas," in International Conference on Cryptographic Hardware and Embedded Systems. Springer, 2016, pp. 147–167.

[4] S. Tajik, E. Dietz, S. Frohmann, J.-P. Seifert, D. Nedospasov, C. Helfmeier, C. Boit, and H. Dittrich, "Physical characterization of arbiter pufs," in International Workshop on Cryptographic Hardware and Embedded Systems. Springer, 2014, pp. 493–509.

[5] F. Stellari, P. Song, M. Villalobos, and J. Sylvestri, "Revealing sram memory content using spontaneous photon emission," in VLSI Test Symposium (VTS), 2016 IEEE 34th. IEEE, 2016, pp. 1–6.

[6] C. Boit, S. Tajik, P. Scholz, E. Amini, A. Beyreuther, H. Lohrke, and J.-P. Seifert, "From ic debug to hardware security risk: The power of backside access and optical interaction," in Physical and Failure Analysis of Integrated Circuits (IPFA), 2016 IEEE 23rd International Symposium on the. IEEE, 2016, pp. 365–369.

[7] S. M. Mansfield and G. Kino, "Solid immersion microscope," Applied physics letters, vol. 57, no. 24, pp. 2615–2616, 1990.

[8] C. Boit et al., "Fundamentals of photon emission (pem) in silicon– electroluminescence for analysis of electronic circuit and device func- tionality," Microelectronics Failure Analysis: Desk Reference, vol. 356, p. 368, 2004.

[9] Y. S. Ng, T. Lundquist, D. Skvortsov, J. Liao, S. Kasapi, and H. Marks, "Laser voltage imaging: A new perspective of laser voltage probing," in ISTFA, 2010, pp. 5–13.

[10] H. Lohrke, H. Zo¨llner, P. Scholz, S. Tajik, C. Boit, and J.-P. Seifert, "Visible light techniques in the finfet era: Challenges, threats and opportunities," in Physical and Failure Analysis of Integrated Circuits (IPFA), 2017 IEEE 24th International Symposium on the. IEEE, 2017, pp. 1–6.

[11] J. G. Van Woudenberg, M. F. Witteman, and F. Menarini, "Practical optical fault injection on secure microcontrollers," in Fault Diagnosis and Tolerance in Cryptography (FDTC), 2011 Workshop on. IEEE,
2011, pp. 91–99.

[12] S. P. Skorobogatov, "Semi-invasive attacks: a new approach to hardware security analysis," Ph.D. dissertation, Citeseer, 2005.

[13] S. Tajik, J. Fietkau, H. Lohrke, J.-P. Seifert, and C. Boit, "Pufmon: Security monitoring of fpgas using physically unclonable functions," in On-Line Testing and Robust System Design (IOLTS), 2017 IEEE 23rd International Symposium on. IEEE, 2017, pp. 186–191.

[14] Y. Gao, H. Ma, D. Abbott, and S. F. Al-Sarawi, "Puf sensor: Exploiting puf unreliability for secure wireless sensing," IEEE Transactions on Circuits and Systems I: Regular Papers, 2017.

[15] J. I. Pankove, Optical processes in semiconductors. Courier Corpora- tion, 2012.

[16] G. N. Koskowich and M. Soma, "Optical charge modulation as an inter- nal voltage probe for cmos ics," IEEE journal of quantum electronics, vol. 24, no. 10, pp. 1981–1984, 1988.

[17] M. Paniccia, T. Eiles, V. Rao, and W. M. Yee, "Novel optical probing technique for flip chip packaged microprocessors," in Test Conference,
1998. Proceedings., International. IEEE, 1998, pp. 740–747.

[18] C. Boit, C. Helfmeier, and U. Kerst, "Security risks posed by modern ic debug and diagnosis tools," in Fault Diagnosis and Tolerance in Cryptography (FDTC), 2013 Workshop on. IEEE, 2013, pp. 3–11.

[19] K. Sato, M. Shikida, Y. Matsushima, T. Yamashiro, K. Asaumi, Y. Iriye, and M. Yamamoto, "Characterization of orientation-dependent etching properties of single-crystal silicon: effects of koh concentration," Sensors and Actuators A: Physical, vol. 64, no. 1, pp. 87–93, 1998.

[20] P. Papet, O. Nichiporuk, A. Kaminski, Y. Rozier, J. Kraiem, J.-F.
Lelievre, A. Chaumartin, A. Fave, and M. Lemiti, "Pyramidal texturing of silicon solar cell with tmah chemical anisotropic etching," Solar Energy Materials and Solar Cells, vol. 90, no. 15, pp. 2319–2328, 2006.

[21] A. Mavrokefalos, S. E. Han, S. Yerci, M. S. Branham, and G. Chen, "Efficient light trapping in inverted nanopyramid thin crystalline silicon membranes for solar cell applications," Nano letters, vol. 12, no. 6, pp.
2792–2796, 2012.

[22] S. Liu, X. Niu, W. Shan, W. Lu, J. Zheng, Y. Li, H. Duan, W. Quan, W. Han, C. Wronski et al., "Improvement of conversion efficiency of multicrystalline silicon solar cells by incorporating reactive ion etching texturing," Solar Energy Materials and Solar Cells, vol. 127, pp. 21–26,
2014.

[23] W. Zhao and Y. Cao, “Predictive technology model,” 2012.
[24] P. Dhoble and A. Kale, “Design of positive edge triggered d flip- flop using 32nm cmos technology,” International Journal of Innovative Research in Computer and Communication Engineering, vol. 3, pp.
3375–3384, 2015.
[25] M. N. Polyanskiy, “Refractive index database,” https://refractiveindex.info, accessed on 2017-09-01.
[26] R. Soref and B. Bennett, “Electrooptical effects in silicon,” IEEE journal of quantum electronics, vol. 23, no. 1, pp. 123–129, 1987.