A Twofold Clock and Voltage-based Detection Method for Laser Logic State Imaging Attack

Tasnuva Farheen, Sourav Roy, Shahin Tajik, *Member, IEEE,* and Domenic Forte, *Senior Member, IEEE*

***Abstract*—Powerful side-channel analysis (SCA) attacks based on failure analysis (FA) techniques can bypass conventional countermeasures on integrated circuits (ICs), and therefore, break the entire system's security. Laser Logic State Imaging (LLSI) from the IC backside is an example of such attacks, making the contactless probing of static on-die signals possible. Several countermeasures have been proposed to prevent optical probing attacks, such as LLSI. However, these schemes are designed according to the laser properties and its impact on transistors, and hence, they have complex fabrication steps and large area overhead. As a result, they are difficult to verify and implement. In this paper, we propose a twofold detection self-timed sensor, which is the first attempt, to our knowledge, for an easy-to-implement circuit-based countermeasure to thwart LLSI attacks. To perform LLSI, the attacker needs to freeze the clock at a point of interest and modulate the voltage supply line at a known frequency to leak the state of transistors through laser light reflections. With these two attack requirements in mind, we design, simulate, and implement clock- and voltage-based sensors that can detect LLSI attacks with very high confidence.** [1]

***Index Terms*—Laser logic state imaging, backside attacks, hardware security, clock freeze sensor, voltage modulation sensor, optical probing.**

I. Introduction

Embedded electronic devices are essential components of networked systems requiring strong cryptography to maintain data confidentiality and integrity. Despite such cryptographic primitives, the security of deployed devices can still be compromised by attackers, who gain access to them in hostile environments and launch physical attacks. Among various SCA methods, laser-assisted SCA attacks (e.g., optical probing [1], [2], [3] and laser stimulation [4], [5]) through the integrated circuit (IC) backside have been shown to be very powerful, and thus, threatening for the confidentiality of assets stored/computed on chips. Traditional SCA techniques, such as power [6] and electromagnetic analysis [7], can only provide a very coarse and integrated view of the chip's signal. On the other hand, contact-based probing techniques, like microprobing [8], can only give simultaneous access to a very limited number of internal signals, typically not more than 8 or so. However, unlike the conventional SCA techniques, optical probing through the chip backside potentially allows quantitative comparison of all signals of the IC in a contactless fashion. This feature was exploited in 2021 [3] with great success where an optical probing technique called Laser Logic State Imaging (LLSI), initially developed for failure analysis, bypassed randomness in the most prominent side-channel countermeasures, i.e., masking schemes [9], [10].

LLSI [11], [12] is a single trace optical probing technique, enabling the extraction of static data through the modulated laser light reflection without requiring repeated measurements of computations. In contrast, most of the conventional SCA attacks, such as power and electromagnetic analysis, capture data leakages only during state transitions. To perform this attack, the system clock is frozen by the attacker to keep the logical signals of the circuit in a static state. After that, the supply voltage is modulated with a known frequency. Due to the modulation of the transistor channel's electric field, transistors in the on-state give clear signatures on the LLSI image, while this is not the case for transistors in the off-state. Thus, logic '1' and '0' signals can be distinguished in a contactless manner. Deploying randomization in countermeasures, such as masking and hiding, is a conventional method to mitigate SCA attacks, as it prevents the repetition and integration of the measurements. However, randomness becomes ineffective if the adversary halts the circuit and recovers the entire state of the circuit using attacks like LLSI. Therefore, static and on-die secrets on both combinational and sequential logic gates [13] of unmasked circuits and key/randomness generation primitives outputs, such as physically unclonable function (PUF) responses [1] and true random number generator (TRNG) outputs [3], can be recovered by LLSI.

As algorithmic countermeasures based on randomness do not provide any protection against LLSI, protection schemes at the circuit or device level are required to avert this attack. Very few countermeasures exist to detect or prevent optical probing attacks. Those that have been proposed [14], [15], [16] focus more on the optical aspect rather than the circuit aspect of the attack. As a result, they are less natural to adopt, including complex fabrication steps, additional silicon area, CMOS-incompatibility, and nontrivial optimization. In addition, some are only applicable to ASICs, and not FPGAs. Thus, optical probing attacks, including LLSI, remain a significant threat.

Contributions. In this paper, we propose low-cost self-timed circuit-based sensors that are specifically designed to detect critical steps taken by attackers when performing LLSI attacks. In other words, our approach targets the two main attack requirements of LLSI – system clock freezing and supply voltage modulation. Using a twofold detection countermeasure, we can detect the LLSI attacks and perform zeroization to destroy sensitive assets before they are extracted. Our main

T. Farheen, S. Roy, and D. Forte are with the Department of Electrical and Computer Engineering, University of Florida (email: tasnuvafarheen@ufl.edu, sourav.roy@ufl.edu, and dforte@ece.ufl.edu)

S. Tajik is with the Department of Electrical and Computer Engineering, Worcester Polytechnic Institute (email:stajik@wpi.edu)

[1] Distribution Statement A: Approved for Public Release

contributions[2] in this paper are summarized as follows:

- To the best of our knowledge, our twofold detection technique is the first attempt at designing any circuit-based detection countermeasure for LLSI attack. Our sensors are low-cost, easy to parameterize, and verifiable during design. Besides LLSI, they are also applicable to other attacks that rely on clock freezing or supply voltage modulation.
- We design a self-timed clock-based sensor which is independent of the system clock, always active and suitable for both FPGAs and ASICs, to detect the frozen clock during attacks. In the proposed design, an internally generated clock measures the system clock and triggers an alarm if it is frozen for a designer-specified number of cycles. Further, to assess the reliability of the sensor, we analyze the effect of temperature and process variation on it.
- We design a voltage-based sensor that is suitable for ASICs. Our novel design expands on a frequency to voltage converter (FVC) with pre- and post-processing circuits to detect supply voltage modulation.
- For simulation-based analysis, we use ModelSim HDL simulator for clock-based sensor verification and Cadence Spectre for voltage-based sensor verification. Results indicate that the proposed sensors can detect clock freezing and voltage modulation with a high detection rate even in the presence of process and temperature variations. Moreover, we implement the clock-based sensor on an FPGA to demonstrate its effectiveness in silicon. The experimental results show that it successfully detects a frozen clock.
- Finally, we discuss how our proposed sensors can detect other classes of static SCA attacks, such as static power analysis, laser stimulation, and static photon emission analysis.

The rest of the paper is organized as follows. In Section II, we introduce the background of optical probing attacks, laser logic state imaging (LLSI), adversary model, and existing countermeasures. In Section III, we propose and describe two detection-based countermeasures, the clock freeze sensor and the voltage modulation sensor. Afterward, in Section IV, we discuss the simulation and silicon implementation results. Section V describes how our sensors can be used to detect physical attacks other than LLSI. Finally, the conclusion is given in Section VI.

II. Background

There are several metal layers on the frontside of modern ICs for signal routing purposes. As these metal layers obstruct the optical path, frontside IC analysis for both non-security purposes (e.g., failure analysis (FA)) and security purposes (e.g., data exfiltration) is challenging. On the other hand, analysis from the chip backside provides more flexibility since the silicon substrate does not contain any impediments [18]. Optical FA techniques such as photon emission (PE) analysis [19], [20], thermal laser stimulation (TLS) [4], [21], and optical probing [22], [2], [1] exploit the fact that infrared waves of wavelengths over 1.1μm can be transmitted through silicon. Such waves can be detected after reflection from the IC backside to analyze the behavior of the circuitry in a semi-invasive manner and in many cases non-invasive manner (e.g., in the case of flip chip devices).

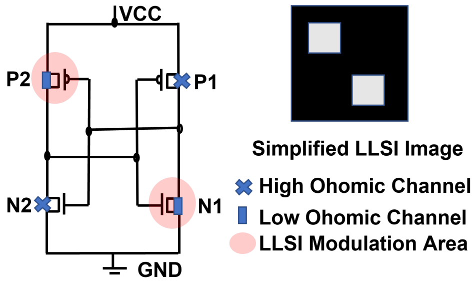


Fig. 1: An SRAM cell with transistors P2 and N1 in ‘on’ state and associated LLSI image with bright spots at P2 and N1.

Ironically, such FA techniques can be used by an attacker to extract secrets from the IC. This includes both data in memory elements (SRAM or registers) and logic gates. An attacker only needs access to FA equipment which can be rented hourly at low cost. Thus, optical probing attacks incur little investment and time.

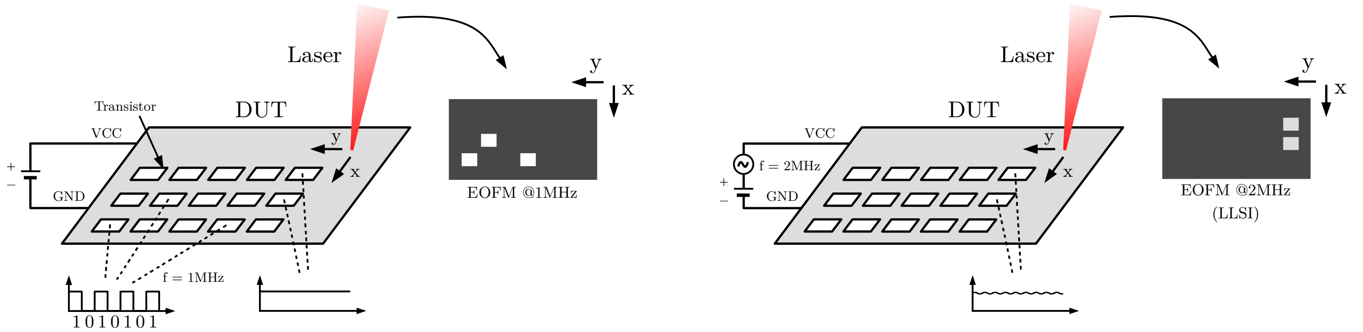
A. Optical Probing

In a classical optical probing scheme, a laser with wavelength above 1.1μm is focused at a point of interest on the chip backside. The reflection of the laser from transistors is measured by a detector to obtain a waveform representing the data in the IC at the point of interest. This technique is known as laser voltage probing (LVP) [23] or electro-optical probing (EOP). High SNR can be achieved by integrating many repetitions of the same waveform. In other words, the IC should be reset and the reflection at the region of interest should be measured multiple times. Alternatively, the laser can be scanned over the IC and the detected signals can be analyzed by spectrum analyzer set to a frequency of interest. This technique, known as laser voltage imaging (LVI) or electro-optical frequency mapping (EOFM), produces an image for the scanned region. In the case of EOFM, transistors can be localized which are switching at frequencies of interest while transistors which are switching at a frequency outside this band or transistors which are producing static signal cannot be localized. Similar to EOP, many repetitions are needed for EOFM to obtain a high SNR.

B. Laser Logic State Imaging (LLSI)

The main limitation of EOP and EOFM is that static signals cannot be detected. To overcome this limitation, laser logic state imaging (LLSI) [11], [3], [12] can be used. LLSI is an extension of EOFM [1], where instead of enforcing the

[2] This paper is an extended version of the [17], presented at ISQED 2022. Sensor’s application to other attacks, analytical description and simulation results of temperature and process variation to access the sensor’s reliability, implementation of the clock-based sensor to FPGA, area overhead analysis, additional measurements and discussion on the detection accuracy are the main additions of this version.



(a) Electro optical frequency mapping (EOFM)

(b) Laser logic state imaging (LLSI)

Fig. 2: (a) The EOFM image identifies transistors which are switching at 1MHz frequency but cannot detect static signals [5]; (b) The LLSI image shows static signals by freezing the clock and modulating the voltage supply line [5].

transistors to switch, their supplied voltage is modulated with a specific frequency. Due to the modulation of the transistor's channel electric field caused by the supply voltage modulation, transistors in the on-state, dynamic and static signal give a clear signature on the LLSI image while not for transistors in the off-state. For example, Fig. 1 depicts an SRAM cell, which consists of two cross-coupled inverters. Depending on the value stored in the memory cell, only one transistor in each inverter will be ON at any given time. LLSI imaging shows a signature (bright white spots) on the locations where transistors are on. Thus, from this image, an attacker can determine data stored in the SRAM cell.

A comparison of results between EOFM and LLSI is depicted in Figs. 2a and 2b, respectively. In Fig. 2a, EOFM detects the transistors which are switching at the detection frequency but cannot detect the transistors which are producing static signals. On the other hand, if the clock is frozen, an LLSI image can detect the transistors which are ON and producing a static signal as shown in Fig. 2b. As discussed in Section I, the LLSI attack has been used to break masking schemes by extracting and analyzing such static signals [3]. Recent work also shows that deep learning can be used to extract sensitive key automatically [5] without even knowing the design and what regions of the IC contain sensitive information.

C. LLSI Adversary Model

An overall picture of an adversary model with steps of LLSI attack is depicted in Fig. 3. A potential attacker should have access to a functioning device under test (DUT). Moreover, it is assumed that the attacker can tamper with the clock signal and supply voltage of the chip. The attack is performed in the following steps. At first, to read out the content of the IC at a specific clock cycle, the attacker should halt the clock in order for the content to remain intact in the registers and logic gates. To stop the clock when the clock is supplied to the chip externally, an adversary can easily tamper with the clock signal before it enters the chip and keeps it low/high at her desired periods to take a snapshot. However, when the clock is generated internally (e.g., ring oscillator), an attacker can either use laser fault injection to manipulate the clock or do circuit editing using a Focused Ion Beam (FIB). Laser fault injection is not practical in the case of an ASIC or a flash-based FPGA since only transient faults can be injected, which is usually not sufficient to halt the internal clock permanently. So, in this case, a more realistic solution, applicable to all platforms, is circuit editing using FIB. Using FIB, the attacker can physically cut the metal lines responsible for the clock signal delivery or damage the transistors of clock buffers to stop the clock. Next, the supply voltage is modulated with a known frequency. Since the supply voltage changes the transistor's electric field in the channel, transistors in the on-state, dynamic and static signals give a distinct signature on the LLSI image, whereas transistors in the off-state do not. We assume that the attack can be applied at one region or over the entire chip. In the case of the latter, snapshots of the hardware state are taken by scanning the laser over every region of the chip.

Under the above assumptions, in our threat model, we consider an end user, test facility, and foundry within the supply chain as the adversaries who have access to the chip, FA tools for laser scanning, imaging, and are motivated to avoid reverse engineering of the whole IC. Among the adversaries, the foundry can be considered the privileged one who already has the design and netlists, making the attack even easier. Depending on the capabilities, the adversary can determine the security-sensitive gates and registers using two templates as reference samples: one containing logic '0' and another containing logic' 1'. Afterward, the attacker applies cross-correlation over all the snapshots of elements under attack. In this case, the assumption is that the positions of the individual elements under attack are known, and the cross-correlation function can be employed to conduct the image registration. The reference sample best fits the targeted cell and determines the bit values/assets in the snapshot. The attacker's choice of which registers to attack depends on her knowledge of the implementation's netlist and layout. In the absence of design/layout information, deep learning can also be applied to extract assets [5].

D. Existing Countermeasures

From the above-described model, there are three critical attack requirements in LLSI:

1) Freezing the system clock to keep the IC logic and memory elements in a static state.

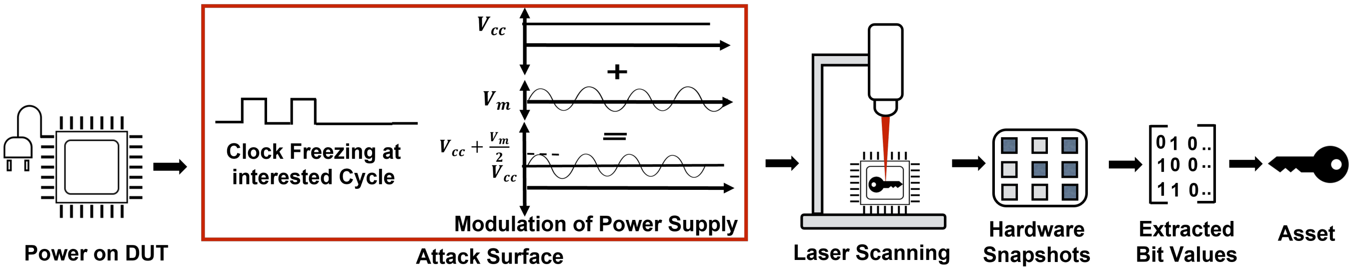


Fig. 3: The LLSI attack involves taking a hardware snapshots with a laser scanner while halting the clock and modulating the supply voltage to extract the bit values.

2) Modulating the supply voltage so that the reflection of on vs. off transistors can be distinguished.
3) Creating an LLSI image by scanning the IC through its backside with a laser. In some cases for certain wavelengths, this may require thinning the IC substrate first.

Two countermeasures against optical probing attacks have been proposed that both target the third attack requirement. For example, a protective optical layer was coated on the backside of dies, while light emitting diodes (LEDs) and photon detectors were fabricated in the active layer [14]. 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 being captured by the detector. This technique provides a general solution against the backside attacks, including LLSI, by detecting the sample preparation required to use the laser. However, the LEDs and detectors sensors must be spread throughout the chip layout resulting in large silicon area. Further, fabrication of a specialized extra protective layer comes with additional fabrication and verification steps.

In another countermeasure, nanopyramid structures were built into an IC to scramble the measurements reflected by laser irradiation [15]. This technique provides protection against optical probing by preventing unscrambled signals from being captured by the detector. While the nanopyramids are passive (do not require power) and do not require any silicon area, their integration requires additional fabrication steps in the first contact and metal layers. Further, the nanopyramid size and distribution need to be optimized for the best results.

In this paper, we aim to thwart LLSI attacks by targeting the first two attack requirements instead. That is, we propose to add low-cost, CMOS-compatible, self-timed sensors to the IC design that detect whether the clock is frozen, the supply voltage is modulated, or both. Compared to the optical sensors, only one sensor is needed to detect the attack. Compared to existing countermeasures, no additional fabrication steps and sample preparation are needed.

III. Proposed Countermeasures

A. Clock Freeze Detection Sensor

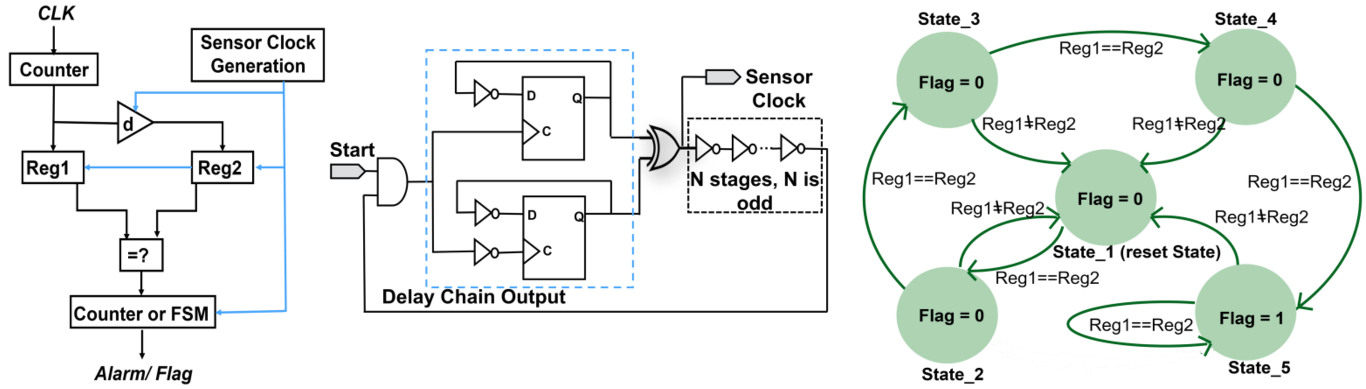
This sensor aims to detect when the system clock is frozen during an attack. The main idea of the sensor is to compare the synchronous system clock with an internally-generated asynchronous sensor clock. The sensor clock will check the system clock count at a specific interval, and if it finds the value frozen for multiple sensor clock cycles, it will raise the alarm[3]. It is worth mentioning that realistic LLSI attacks [5], [3], [11] require the clock to be frozen on the order of minutes to hours. Our sensor has nanosecond level detection capability and is free from any limitations imposed by the system clock, sensor clock, and reset time. Thus, it will be able to detect such attacks before they are successful.

1) Architectural Diagram and Basic Operation: The sensor's architectural diagram is shown in Fig. 4a. It includes a counter, two registers (denoted as $Reg1$ and $Reg2$), a one cycle delay block (d), a comparator, and a finite state machine (FSM). The interface of the sensor is defined by one input CLK, which represents the system clock, and one output $Alarm/Flag$. The system clock pulses trigger the counter to count upwards. $Reg1$ and $Reg2$ then store the system clock's count values which are taken and stored with respect to the current and previous sensor clock cycles. After that a comparator is used just to compare the consecutive count values contained in $Reg1$ and $Reg2$. A finite state machine (FSM) checks whether $Reg1$ and $Reg2$ are equal for more than one sensor clock cycle. In our later experiments, we triggered an alarm after five sensor clock cycles with a frozen system clock, but this parameter can be set by the designer. The reason for checking the comparator for more than one clock cycle is to avoid the false alarm in the sensor due to timing delays or synchronization issues. If the FSM outputs a 'Yes' to indicate that this condition is met, it will raise a flag that the system clock is frozen.

Our design makes sure that the sensor clock frequency (f_{sen}) is at least two times slower than the system clock (f_{sys}) to ensure enough time to capture the register values. Moreover, the slower sensor clock avoids metastability issues in the clock domain crossing the system clock and sensor clock. There can be four different scenarios in terms of the comparison of clock frequency between system clock and sensor clock.

(a) The sensor clock frequency can be faster than the system clock frequency. In that case, a full period of the sensor clock (T_{sen}) will occur before a full period of the system clock (T_{sys}), i.e., $T_{sen} < T_{sys}$. Hence, sensor clock can flag a

[3] The alarm triggers defensive actions to be taken on the chip, such as self-destruction [24], reset, or zeroization [25] of sensitive data. Since our paper focuses on detection, we consider the precise actions taken to be out of scope



(a) Architectural Diagram

(b) Sensor Clock Generation Circuit

(c) State Transition Diagram

Fig. 4: Various components of clock freeze detection sensor.

legitimate clock cycle as an event of clock freeze.

(b) The sensor clock frequency can be similar to the system clock frequency. In such case, both the system and sensor clock periods will occur simultaneously in the design, i.e., $T_{sen} = T_{sys}$. Considering the additional delay incurred by the longer interconnect, there is still chance that sensor clock may flag a legitimate clock as a clock freeze event.

(c) The sensor clock frequency can be slower than the system clock frequency but less than 2x slower, i.e., $T_{sys} < T_{sen} < 2T_{sys}$. We want to mention that the clock freeze detention of the proposed sensor works by counting the number of the clock pulses of the system clock. If the number is unchanged in two consecutive system clock pulses, then the sensor clock flags a clock freeze. In this case, the sensor clock period finishes before two consecutive clock period of the system clock and cannot increase the counter value accurately.

(d) The sensor clock frequency is at least 2x slower than the system clock frequency, i.e., $T_{sen} > 2T_{sys}$. In such case, two system clock period occurs within one sensor clock period. Therefore, at any particular time, the sensor clock can increase the counter value for two consecutive system clock pulses and properly detect any potential clock freeze event.

In the next section, we will describe the sensor clock generation circuit, which is the key element of our sensor.

2) Sensor Clock Generation Circuit: The critical element of the sensor consists of N number of inverters and two D-FFs, both clocked by the output of an AND gate of input delay chain output as depicted in Fig. 4b. This combinational logic is employed to generate a feedback local clock signal whose width depends on the external delay chain and allows the start of the signal utilizing the start input. To fully generate the delay pulse without noise, one of the D-FFs is triggered by the rising edge of the external delay chain output generated by an internal ring-oscillator (RO), and the other one by its falling edge. That is how the elements residing in the blue dotted square ensure noise-free sensor clock generation by the internal RO. The number of inverters can be designed based on frequency of the system clock as the primary assumption of our sensor clock is its should be at least two times larger than the system clock. As the sensor is created by the designer, the frequency of the system clock is known and the the number of inverters can be derived accordingly.The frequency of the sensor clock is fixed after design and fabrication without needing to be tunable anymore. As the sensor clock is no longer dependent on the system clock and can work independently, we call our sensor self-timed or independent. Another critical assumption of our sensor is that the attacker does not have access to the sensor clock generation circuit as it is generated internally. In other words, the 'Start' signal at the input to the circuit is always connected to the supply voltage (logic 1). Hence, if the circuit is live as during an optical probing attack, the sensor clock shall be running.

3) Finite State Machine (FSM): The FSM is responsible for controlling the output of the sensor. It will check and compare the values of $Reg1$ and $Reg2$ for a certain period of sensor clock cycles. If it finds the register's value to be identical, it will go to the next state. Otherwise, every time it will return to state 1. Ths FSM will check this condition for a number (e.g., five) of consecutive states as depicted in Fig. 4c. If the value of the register continues to remain the same for specific cycles, FSM will raise the flag detecting the clock freezing by an attacker. To avoid false alarm, we checked registers value for more than one state, e.g., five states. More than one state is enough for this purpose. The number of the states in the FSM is not related to the number of inverters.

4) Sensitivity of Temperature and Process Variation: Sensor clock generation circuit is affected by variations in temperature and process. It is thus crucial to study these effects on the circuit, as it is one of the control elements that will affect the complete sensor response. We discuss the effects of temperature and process variations on the sensor performance in this section for FPGA and ASIC implementations.

Temperature Variation Effect: The delay line in the FPGA implementation passes through a number of logic clusters, including both logic elements and local routing crossbars, as well as several switch boxes that connect logic clusters. All these can be modeled as a set of m_{inv} inverter equivalent circuits; m_{npt} chains of pass transistor equivalent circuits and m_{drc} distributed RC wires as shown in equation 1 [26].

$$t_{tot} = \sum_{i=1}^{m_{inv}} t_{inv_i} + \sum_{i=1}^{m_{npt}} t_{npt_i} + \sum_{i=1}^{m_{drc}} t_{drc_i} \qquad (1)$$

For an ASIC implementation, the delay line can be modeled as a set of m_{inv} inverter equivalent circuit and m_{drc} distributed RC wire. So, the total delay, t_{tot} can be approximated by the equation 2 [26]:

$$t_{tot} = \sum_{i=1}^{m_{inv}} t_{inv_i} + \sum_{i=1}^{m_{drc}} t_{drc_i} \tag{2}$$

where t_{inv_i}, t_{npt_i}, and t_{drc_i} represent the delays of the ith inverter, pass transistor, and wire.

We have considered the inverter delay and wire delay resulting from the implementation of the sensor on an ASIC depicted in equation 2 and additional pass transistor chains delay resulting from FPGA implementation as in equation 1. This section introduces the analytical description of the combinational delay block which controls the complete sensor response.

The delay of a CMOS logical inverter, t_{inv}, is governed by its physical features according to the following simplified equation [27]:

$$t_{inv} = 0.69 R_{eq} C_L \approx \frac{\left(\frac{L}{W}\right) C_L}{\mu C_{ox} V_{DSat}} \tag{3}$$

where C_L is the load capacitance; C_{ox} is the gate oxide capacitance; L/W is the aspect ratio of the N transistor; μ is the carrier mobility; and V_{DSat} is the saturation drain voltage. From the above equation we can see that inverter delay has inverse relationship with mobility assuming that supply voltage is very large compared to threshold voltage ($V_{dd} \gg V_{th}$).

In the case of a network of n pass transistors, the delay, t_{npt}, employing the Elmore approximation, is given by [27]:

$$t_{npt} = 0.69 R_{eq} C \frac{n(n+1)}{2} \tag{4}$$

$$t_{npt} \approx 0.69 \frac{\left(\frac{L}{W}\right)(V_{dd} - V_{out})}{\mu C_{ox} V_{DSat} (V_{dd} - V_{out} - V_{th})} C \frac{n(n+1)}{2} \tag{5}$$

where R_{eq} is the equivalent resistance of the pass transistor gate which is inversely dependent on the current it yields. Delay of pass transistor chain also increases with decreasing mobility assuming $V_{dd} \gg V_{th}$.

The propagation delay, t_{drc}, of wire with a distributed resistance, R and capacitance, C, is given by [27]:

$$t_{drc} = \sum_{i=1}^{m_{drc}} 0.38 R_i C_i \tag{6}$$

Here we can see that delay of wires depends on the resistance of each wire R_i as well as capacitance of each wire C_i and they both increase with temperature.

In Equations (3) and (5), delay is inversely proportional to mobility μ. μ which is a function of temperature, and decreases with temperature quasilinearly. Here, μ_o is the mobility at room temperature T_o and k_μ is a fitting parameter generally in the range of 1.2 to 2.0 [28].

$$\mu(T) = \mu_o \left(\frac{T}{T_o}\right)^{-k_\mu}. \tag{7}$$

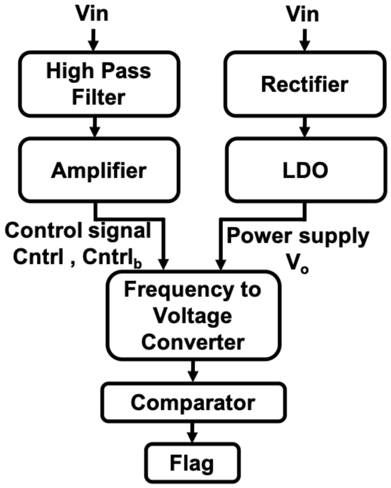


Fig. 5: High-level block diagram of voltage modulation sensor.

Process Variation Effect: In cutting-edge ICs with multi-million gates, processing variations in nanometer technologies are becoming a critical consideration. However, in advanced technologies such as 65 nm and below, the design-dependent systematic variations may be significant even with regular fabrics and replicated layout tiles in FPGAs. Meanwhile, it suffers from the increasingly large random variation as ASIC does. These variations have effects on the transistor's path delays on both ASICs and FPGAs. The performance depends on many process parameters such as channel length, threshold voltage, and oxide thickness [29]. The delay monotonically increases with the process variation [30].

The above analyses are based upon previous work that has been presented and validated in the scientific literature providing insight into how the corresponding delays behave under temperature and process variations. The analytical analyses and results presented in Fig. 9 and Fig. 10 verify that our sensor is not affected by this corresponding delay (see Sect. IV-A2 for more details). As we configured the sensor clock in such a way that its frequency should always be at least two times slower than the system clock. Therefore, in its literal meaning, adding a delay to the sensor clock is beneficial.

B. Voltage Modulation Sensor

During an LLSI attack, the attacker modulates the supply voltage. In order to thwart such attack, we propose a sensor that detects this modulation. According to the literature [3], voltage modulation as high as 0.7V peak to peak (p-p) with frequency of 90KHz is used to execute the LLSI attack. The amplitude of the modulation cannot exceed a threshold as it leads to either chip crash by too low voltage levels or chip damages by too high voltage levels. Note that high-frequency modulation might not reach the target chip on the printed circuit board (PCB) due to the bypassing behavior of decoupling capacitors at higher modulation frequencies.

1) Architectural Diagram and Basic Operation: The block diagram of our voltage modulation sensor is given in Fig. 5. We start with a frequency to voltage converter (FVC) [31] as our foundation. As the name implies, an FVC generates an output voltage V_{out} which depends on the frequency of

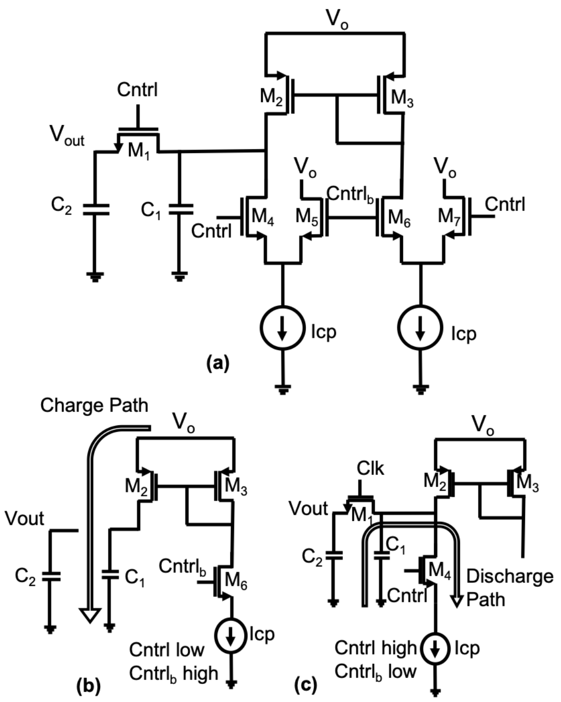


Fig. 6: (a) Frequency to voltage converter (FVC) circuit; (b) Charging cycle when $Cntrl$ and $Cntrl_b$ inputs are low and high, respectively; (c) Discharging cycle when $Cntrl$ and $Cntrl_b$ signals are high and low, respectively.

the input voltage V_{in}. Since a typical FVC circuit has certain requirements for its inputs, we add preprocessing elements to it. First, a high pass filter is used to extract only the modulation above 20kHz from the voltage supply (V_{in}). Then the modulation, which can be as high as 0.7V p-p, is amplified to a voltage close to V_{dd}. This produces an oscillating signal that we refer to as $Cntrl$ and its inverse $Cntrl_b$, which are given as inputs to the FVC circuit. Second, the FVC circuit needs a V_{dd} which is constant. In order to supply a constant voltage V_o to the FVC from the supply V_{in} which may be experiencing modulation during an LLSI attack, we also preprocess V_{in} using a rectifier and low dropout regulator (LDO). The rectifier converts the modulated signal to a DC reference signal while the LDO smooths V_{in} out to make it a constant V_o for the sensor's voltage supply.

The FVC circuit behaves as follows. In the absence of voltage modulation in the supply line, the output of the FVC is a constant known value V_{static} which depends on the technology node, temperature, and process variation. If a modulation is applied to V_{in}, the voltage output of the FVC decreases to a value less than V_{static}. Assuming that one wants to detect modulation frequencies above a certain value, e.g., $f_{mod} = 20KHz$, there is an associated output voltage V_{mod}. By comparing $V_{out} < V_{mod}$ using a well-designed comparator, any modulation in supply voltage above f_{mod} can be detected.

2) Frequency to Voltage Converter (FVC) Design and Operation: The FVC circuit and its operation are shown in Fig. 6. The FVC generates a voltage output which changes with the presence of voltage modulation due to the charge sharing between capacitors C_1 and C_2 followed by discharging of capacitor C_1 over a certain period of time. The $Cntrl$ input of the FVC, which controls the charging/discharging cycles, will have the same frequency as the modulation in supply voltage.

In the presence of modulation, the FVC goes through charging and discharging cycles as follows.

- During the charging cycle, $Cntrl$ is low and $Cntrl_b$ is high. The capacitor C_1 is charged to voltage V_o through the charge path shown in Fig. 6(a).
- During the charge sharing and discharging cycle, $Cntrl$ is high and $Cntrl_b$ is low. The voltage across C_1, V_{C1} is discharged through the discharge path shown in Fig. 6(b). When $Cntrl$ goes high enough to turn on the NMOS switch M_1, charge sharing occurs and the voltage across C_2, V_{out}, follows V_{C1}.
- After a few consecutive cycles, both the voltages V_{C1} and V_{out} settle at value which depends on the modulation frequency. If $V_{out} < V_{mod}$ then the attack will be detected by the sensor.

In the absence of any modulation, the $Cntrl$ signal is always high. Thus, C_1 and C_2 are both being charged simultaneously and V_{out} assumes the value V_{static} which is well above the aforementioned threshold V_{mod}.

3) Comparator Design: We also propose a Schmitt trigger comparator which compares the output voltage of FVC, V_{out}, with the threshold V_{mod} to check whether it dropped below the threshold or not. When there is modulation in supply line, V_{out} goes below the threshold and the Schmitt trigger comparator detects it and raises the flag. The output of the FVC, V_{out} has spikes at the edges where switching occurs. As a result, a comparator is needed that will detect and raise a flag when V_{out} settles below the chosen threshold, V_{mod}, and keep the flag risen even if the spikes cause V_{out} to go slightly above V_{mod}. It can be accomplished through a Schmitt trigger comparator. The Schmitt trigger raises the flag when V_{out} goes below V_{mod} but it keeps the flag high until V_{out} goes above a voltage which is much higher than V_{mod} which accommodates the spikes in V_{out} and fits in nicely with our comparator design. The operation region of Schmitt trigger is shown in Fig. 7. In the figure, we see the change in flag with V_{out}. As V_{out} decreases and goes below V_{mod} of about 390mV flag goes from logic low to logic high and it stays at logic high as long as V_{out} does not increase and go above 700mV which is much higher than the threshold V_{mod} creating a hysteresis loop of operation.

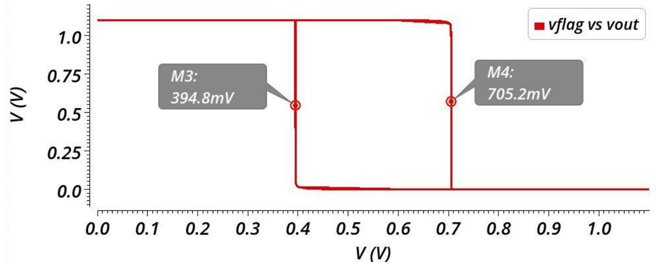
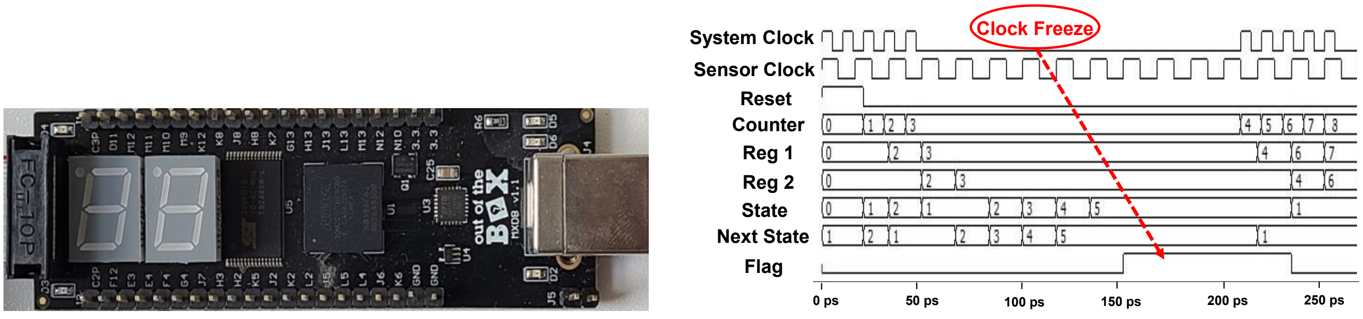


Fig. 7: Schmitt trigger raises flag to logic high when V_{out} goes below 390mV but does not lower flag to logic low as long as V_{out} does not go above 700mV.



(a) (b)

Fig. 8: (a) Altera Max 10 FPGA platform to demonstrate the sensor in silicon and (b) chronograph of the sensor simulation. The clock is frozen from 50ps to 200ps. The attack is detected at 150ps where the $Alarm/Flag$ is set high.

4) Sensitivity to Temperature and Process Variations: The reliability of voltage modulation sensor depends on the comparator's ability to distinguish whether the output of FVC V_{out} settles below a chosen threshold V_{mod}. To understand the robustness of the sensor it is imperative to study the effect of process variation and temperature on V_{out}. We did Monte Carlo simulation to study the process variation effect at different temperatures and found out that at higher temperatures and frequencies V_{out} increases and comes closer and closer to V_{mod}. As a result, at higher temperatures and modulation frequencies, the detection accuracy of the sensor decreases. However, under practical attack scenario the sensor is able to detect modulation with 100% confidence.

C. Twofold Detection Method

The clock freeze detection sensor and voltage modulation detection sensor can work as standalone detectors to detect LLSI attack independent of each other. The clock freeze detection sensor can be used not only to detect LLSI attack but also to detect other static attacks where attacker needs to freeze the clock for μs or longer time span. The former sensor can be implemented in an FPGA or ASIC while the latter sensor can only be implemented in an ASIC.

In an ASIC design, the sensors can be used together to detect LLSI attack with higher confidence. For example, their output flags can be combined using a logical OR for a more conservative detection or using a logical AND for a less conservative detection.

D. Security Analysis

The success of proposed countermeasure depends on the security against other attacks. A fault injection attack involves the adversary tampering with the operation of the device to gain access to sensitive information. The adversary uses a high-powered laser or alters the clock and power supply lines to cause a fault in the device [32]. When injected carefully, these faults corrupt the output. On the other hand, a fully invasive attack Focused Ion Beam, or FIB circuit edit, allows an attacker to cut traces or add metal connections within a chip [33].

The attacker could, in principle, inject faults at specific locations to disable the sensor or do FIB circuit editing to cut the sensor output line. However, it would not be easier for the attacker to disrupt the sensor by the attacks mentioned above. As a FIB-based invasive attack at the sensor output involves painstaking reverse engineering, it is costly to perform, making it unadoptable in the first place. Also, it is easy to find the external clock and edit it even before it enters the chip. However, in the case of our sensor, the clock is generated internally, making the attacks more challenging. The attacker needs to apply a more sophisticated method to tamper with the clock. Suppose the target is an FPGA (SRAM-based). In that case, an attacker can try to perform fault injection to manipulate/stop the clock source configuration (e.g., ring oscillator-based) or its routing configuration. However, fault injection before LLSI does not help to defeat the sensor since only transient faults can be injected, which is usually not sufficient to halt the internal clock permanently. Fault injection and optical probing also cannot be done simultaneously as they are not part of the same setup making the attacker's job extremely difficult in defeating the sensors.

IV. Experimental Setup and Results

A. Clock Freeze Detection Sensor

In this section, we examine the effectiveness of our sensor in silicon and simulation.

1) Experimental Platforms: The device under test (DUT) on which the effectiveness of our proposed sensor is tested is the Altera Max 10 FPGA (10M02SCU169C8G). This FPGA is built on 55 nm TSMC embedded flash (flash + SRAM) process technology and is shown in Fig. 8a. Simulations are performed in the ModelSim tool and Cadence Virtuoso to verify the operation of our proposed sensor before testing it on the FPGA. The FSM of the sensor is set to output an alarm after 5 sensor clock cycles with a frozen system clock.

2) Results and Discussion: Fig. 8b shows the simulation results of the LLSI clock freeze detection sensor. In this example, the system clock is functioning normally for five pulses and then is frozen to simulate the attack. The counter begins counting after the system reset signal goes low and samples the system clock at the rate of the sensor clock. The current counter value is stored in $Reg1$ while the previous counter value is stored in $Reg2$ with respect to the sensor clock. At around 70 ps, the counter stops counting because the system clock is frozen. Thus, the values in $Reg1$ and $Reg2$ are equal beyond this point. The FSM transitions from state

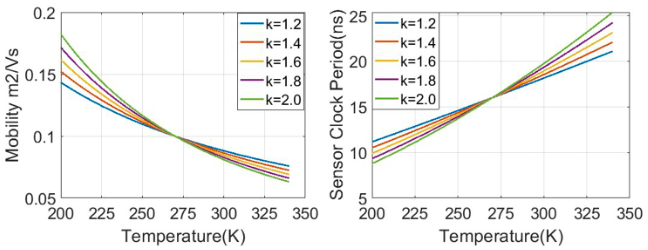


Fig. 9: Relation of mobility and sensor clock period with temperature.

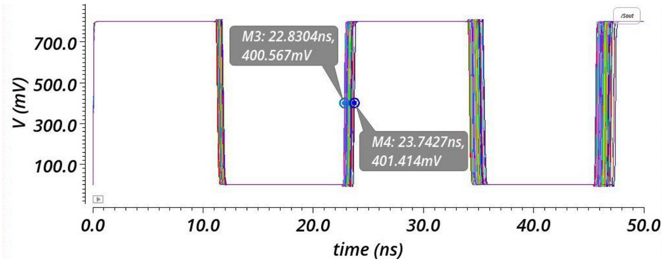


Fig. 10: Monte Carlo simulation of 300 random process variations on sensor clock consisting of 81 delay stages at supply voltage of 0.8V.

1 to state 5, and then raises the alarm flag high. Thus, it has correctly detected that the system clock is frozen. The attack stops (i.e., the system clock is unfrozen) at around 200ps. Thus, the counter begins counting again, $Reg1$ and $Reg2$ have different values once again, and the FSM transitions back to its initial state. The attack flag therefore transitions back to logic 0.As demonstrated in [3], a real LLSI attack is executed on an Altera board with 60 nm process technology. A scan of 16 bits of registers took 2.7 minutes, or 10.12 seconds per bit. The above information indicates that a real LLSI attack would require freezing the clock for at least a thousand clock cycles, varying according to the design between seconds and hours [5]. Therefore, a five-state FSM is more than sufficient to capture the clock freezing by our proposed sensor.

We also simulated the temperature and process variation effect on the sensor. In this example, we assume that there are 40 delay stages and each delay stage has a delay of about 0.2ns. The sensor period is twice the delay of each stage, i.e., 16ns at room temperature. The effect of temperature on V_t is ignored as $V_d \gg V_t$. At room temperature, electron mobility of NMOS devices is about 700 cm^2/Vs [34] and process dependent parameter k_μ may vary between 1.2 and 2. Fig. 9 shows the relation of mobility with temperature and how the sensor clock period increases with temperature. For process variation, we used Monte Carlo simulation on 45nm process node using Cadence Virtuoso. Our simulation consisted of 81 delay stages for sensor clock generation. At lowered supply voltage of 0.8V, we achieved sensor clock frequency that varies between 42MHz to 44MHz with 300 Monte Carlo test points, which is slow enough compared to modern FPGA system clock speed to detect clock freeze. The simulations results are shown in Fig. 10.

As a silicon demonstration, the Altera Max 10 is used where the proposed sensor has been implemented. The sizes of the counter and comparator were fixed to 4-bit, and different lengths of the sensing delay chain were used to ensure that the sensor clock is slower than the system clock. Each stage in the delay chain is constructed utilizing both LUT and latch pairs available in the board. The number of stages used in the sensor clock generation will vary board to board as the system clock and internal delay are different for each case. The system clock frequency of our prototype board is 4 MHz. To generate the sensor clock which is at least two times slower than the system clock, we used 127 delay stages and a frequency divider. Then, the system clock was frozen with an external pin and wire connecting it with the system clock to check whether our sensor can detect that or not. Our sensor's behavior matched the simulations and successfully detected the attack.

TABLE I: Resource utilization by the clock-based sensor on Altera Max10M02SCU169C8G implementation

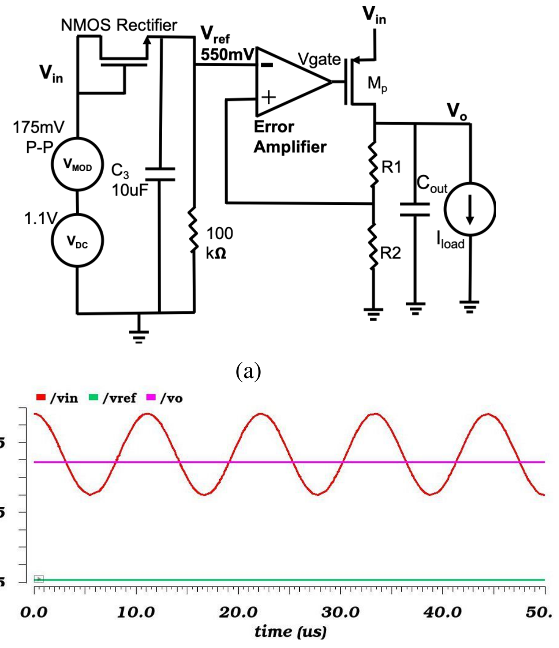
Resource Utilization by Entity		
Entity	Resources	
	LUT	Register
Counter	4	4
FSM	18	15
Sensor clock generation circuit	224	132

3) Overhead Analysis: We evaluated the overhead incurred by clock-based sensor: counter, FSM and clock generation circuit on Altera Max10M02SCU169C8G featuring 2304 LUTs. Each circuit in verilog format was synthesized and implemented using the Quartus 18.1 on the Altera Max10 FPGA. Table I gives the synthesis summary featuring the resource utilization by the components of the sensor. We can see from the table that the resource overhead is very low for the counter and FSM, where as high for the sensor clock generation circuit. The later circuit resource will vary from board to board depending on the system clock. The average resource overhead for current implementation board is 10% for LUTs. However, for the larger FPGA board with thousands of available resources the overhead may be less than 1%, e.g., Xilinx Virtex5 FPGA XC5VLX50T featuring 28800 LUTs [35]. Our sensor is also independent of the design. So, the area overhead should be same for the study on various selected benchmarks.

B. Voltage Modulation Detection Sensor

In this section, we discuss our sensor implementation and provide simulations results to verify its effectiveness.

1) Simulation Setup: We carried out the simulation in Cadence Virtuoso version IC6.1.7 with 45nm process library with model library set up to `tt` (i.e., typical typical). All the transistors in the design have nominal threshold voltage V_{th}. At first, we simulated the behavior of the pre-processing circuit, i.e., the output of constant voltage generation LDO and control signal generation circuit for the frequency to voltage converter (FVC) circuit. After that, we simulated the output voltage of FVC circuit at different modulation frequencies and simulated the behavior of Schmitt trigger comparator. Finally, we simulated the process and temperature variation effect on the output of FVC circuit to understand the detection accuracy of the sensor.



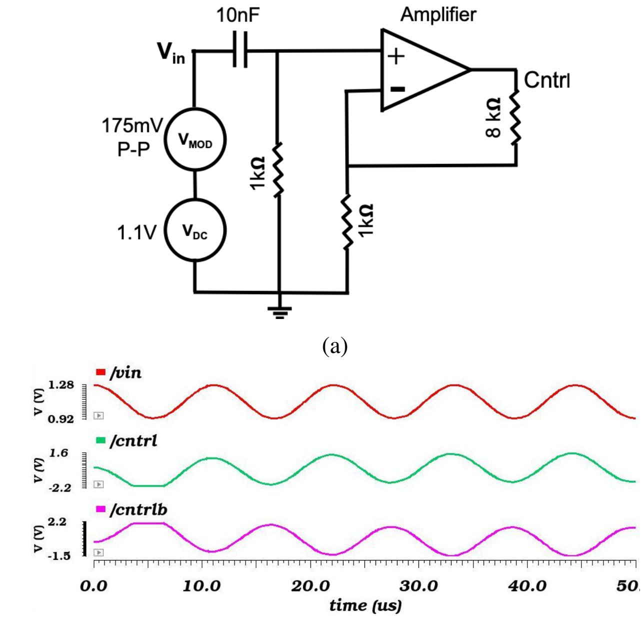
(a)

(b)

Fig. 11: (a) LDO circuit along with NMOS rectifier to generate constant voltage for FVC and (b) output of the LDO circuit.

2) Result and Discussion: We designed a generic LDO along with a NMOS rectifier to generate constant voltage V_o. The LDO circuit is shown in Fig. 11a. The NMOS rectifier along with the resistor and capacitor produces the constant reference voltage V_{ref} for the LDO. LDO takes the modulated signal V_{in} as input at the source of the pass element M_p, takes reference voltage V_{ref} and produces constant output voltage V_o. The output of the LDO circuit is shown in Fig. 11b where the reference voltage V_{ref} is about 0.55V and the input voltage is 1.1V with a modulation of 175mV p-p. The LDO output is a constant 1.1V which remains constant with modulation level change and also with FVC and comparator as added load. The $Cntrl$ signal is generated using a high pass filter and an amplifier. The high pass filter filters out the dc voltage of 1.1V and also any frequencies lower than 20kHz, so that only the modulation frequency of 175mV p-p is sustained. The amplifier amplifies the modulation so that the peak value is above the threshold voltage of NMOS for proper switching operation. The $Cntrl$ signal generator circuit is shown in Fig. 12a. $Cntrl_b$ signal is simulated as a 180^o phase shifted version of $Cntrl$ signal. The waveform showing the $Cntrl$ and $Cntrl_b$ signals are given by Fig. 12b.

In the absence of supply voltage modulation, the output of FVC is a constant voltage (i.e., V_{static}) of about 470 mV. When there is presence of modulation above 20KHz in the supply line, the switching activity occurs in FVC and through charging and discharging cycles, the output of FVC V_{out} settles at a value lower than a threshold V_{mod} of 390mV at nominal operating temperature. We use a Schmitt trigger comparator to detect whether the output V_{out} dropped below the set threshold V_{mod} and raise a flag to logic high. Schmitt trigger keeps the flag at logic high as long as V_{out} is below 700mV thus resisting the spikes present in V_{out} to change the flag value to logic low in the presence of modulation.



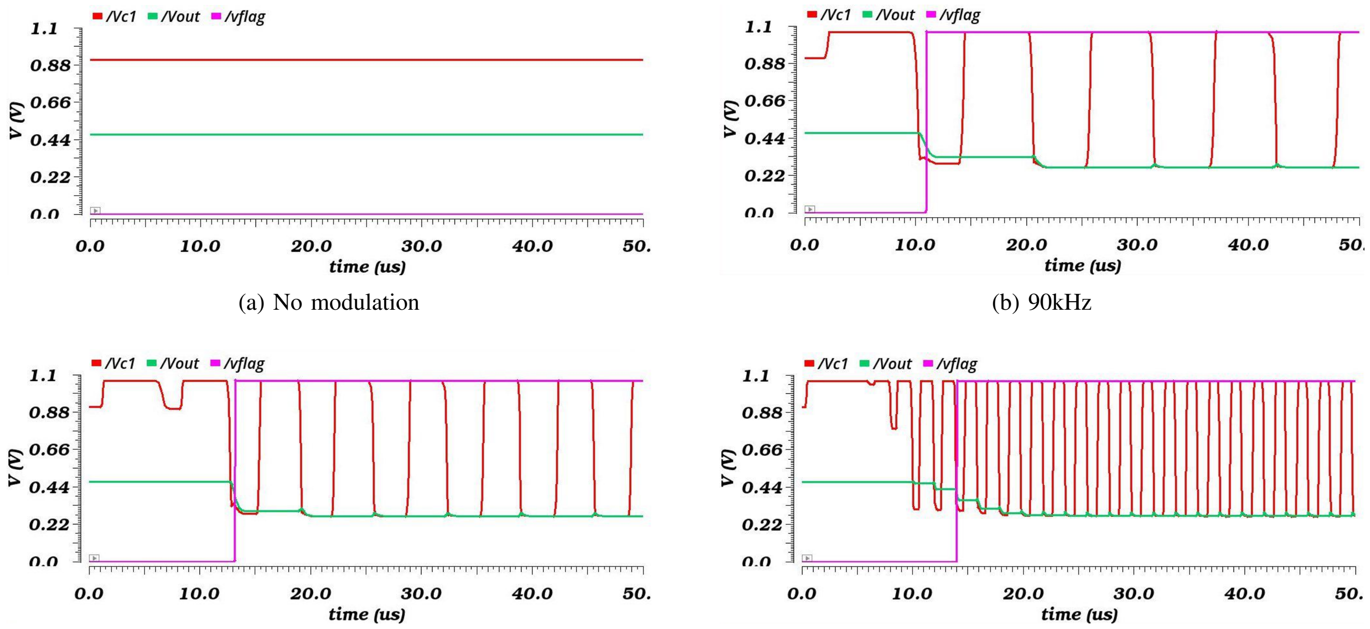
(a)

(b)

Fig. 12: (a) High-pass filter in combination with an amplifier to generate $Cntrl$ signal and (b) output of the $Cntrl$ signal generation circuit. Note that $Cntrl_b$ signal has a 180 degree phase shift.

In Fig. 13a we see that no flag is raised if there is no modulation in supply line, i.e., the flag stays at logic low. In Figs. 13b, 13c, and 13d we see that flag is raised to logic high at the presence of voltage modulation as in all these cases the output of FVC, V_{out} went below set threshold V_{mod} of 390mV. We see that, the sensor is able to detect modulation above 20KHz. In previous works [3], LLSI attack was conducted at 90KHz and it is difficult for attacker to achieve higher frequencies due to the decoupling capacitors present in modern ICs. In our work we see that, at ideal operating condition the sensor functions very well even at frequencies as high as 1MHz. This sensor can detect modulation as low as 50mV peak to peak as shown in Fig. 14a.

In order to simulate the temperature and process variation effect on the voltage modulation sensor we did Monte Carlo simulation at different frequencies. We varied the temperature from 0^oC to 90^oC and included the effect of process variation on the transistors in the design. The detection rate and time to raise the flag at different frequencies are simulated with 300 random Monte Carlo simulations at different temperatures and the results are summarized in the Table II. At nominal temperature of 27^oC and 60^oC the sensor can detect presence of modulation successfully even for frequencies as high as 2MHz. But at 90^oC accuracy drops as modulation frequency increases. We observed that, at higher temperatures, as frequency increases the output voltage of FVC V_{out} settles at even higher voltages compared to the case at nominal temperature, which becomes closer to our chosen threshold of V_{mod} of 390mV. As a result for worst case process variations, there lies a possibility that V_{out} settles higher than V_{mod} and modulation cannot be detected. The practical LLSI attack is done at a



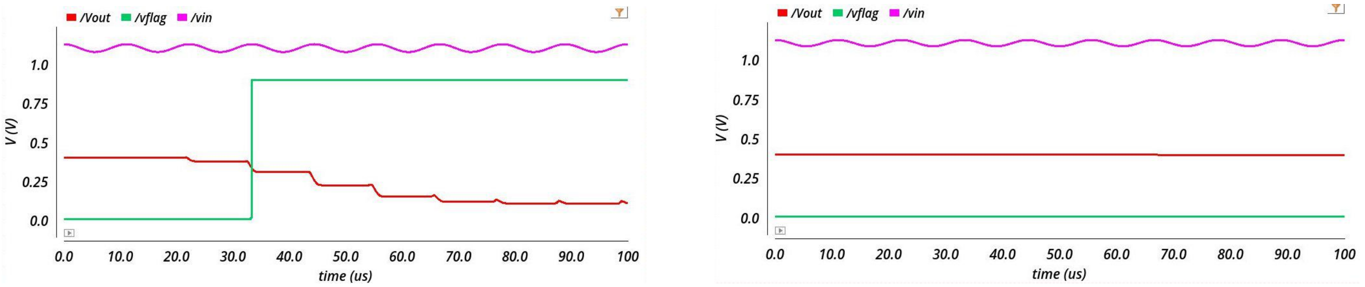
(a) No modulation

(b) 90kHz

(c) 150kHz

(d) 500kHz

Fig. 13: Voltages of internal nets and outputs of the voltage modulation sensor over time for 4 cases: (a) no modulation and voltage modulation of (b) 90kHz, (c) 150kHz, and (d) 500 kHz. The voltage on capacitor 1, voltage at FVC output, and alarm flag which are labeled $Vc1$, $Vout$, and $Vflag$ and shown in red, green, and magenta, respectively.The sensor flag is not raised when no modulation is present on the supply line in (a) but is raised in (b-d) at different modulation frequencies.



(a) Flag raises to high at 50mV peak to peak modulation at 90KHz

(b) Flag stays at zero at 40mV peak to peak modulation at 90KHz

Fig. 14: Voltage modulation detection as low as 50mV peak to peak at 90KHz

frequency of about 100 KHz. 90°C and the frequency of 2MHz represents very extreme condition and understandably our sensor is not supposed to work at that condition. However, we would like to mention that our sensor even works at 500KHz which is enough to detect LLSI attack. Monte Carlo analysis at 90^{o}C using 300 simulations at 90kHz and 500kHz are shown in Fig 15a and 15b respectively which shows the phenomena described earlier.

We see that as temperature increases the time needed to raise the flag also increases. At all temperatures, time needed to raise the flag is the minimum for 90kHz modulation and it increases for both lower and higher frequencies. At lower frequencies V_{out} settles slowly thus comparator needs more time to raise the flag and at higher frequencies V_{out} settles closer to V_{mod} so that comparator needs more cycles to successfully detect the settling voltage. In all cases, time needed to raise the flag is in μs range which is fast enough to detect LLSI attack as LLSI attack takes hours to perform.

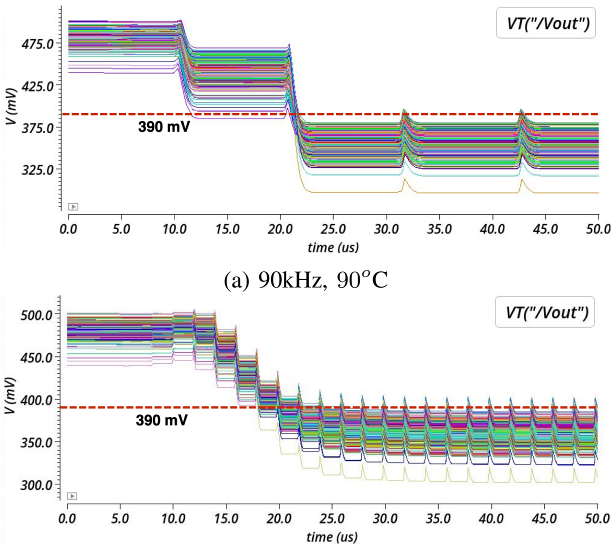
As long as the output voltage V_{out} settles below V_{mod} at the presence of supply modulation, it is possible to detect the modulation, but at higher frequency and at extreme temperatures the comparator may not be able to detect the modulation considering the worst case of process variation. But such situation is highly unlikely as it is difficult for attacker to modulate the supply line at frequencies above 100kHz because of the decoupling capacitors that restricts high frequency modulation from reaching the intended target. Under the practical frequency of supply modulation, even at extreme temperatures of 90^{o}C and worst case process variation, the sensor is able to detect modulation in supply line. From these results, it is apparent that under practical attack scenario, the voltage modulation sensor will be able to detect the presence of modulation in the supply line.

V. Applications

Our clock-based sensor was specially conceived and demonstrated for protection against LLSI attacks in this paper. However, we believe that our sensor is not only limited to LLSI

TABLE II: Detection accuracy and time needed to raise the flag in 300 random Monte Carlo simulations.

Temperature Frequency (Hz)	27^0C		60^0C		90^0C	
	Accuracy	Time (us)	Accuracy	Time (us)	Accuracy	Time (us)
25K	100%	33	100%	34	99%	35
60K	100%	15	100%	16	99%	17
90K	100%	12	100%	12	99%	12
500K	100%	16	100%	20	98%	37
700K	100%	17	100%	21	97%	43
1M	100%	20	100%	25	91%	55
2M	100%	27	97%	62	58%	77



(a) 90kHz, 90^{o}C

(b) 500kHz, 90^{o}C

Fig. 15: (a) Output of FVC considering process variation at 90kHz modulation at 90^{o}C; (b) Output of FVC considering process variation at 500KHz modulation at 90^{o}C.

attack but also effective against other attacks, e.g., static power side channel attack [36], [37], and static photon emission analysis [38]. These side channels can only be captured when the clock is halted. Some other attacks, e.g, laser stimulation, e.g., PLS, TLS [39], [5] can be carried out without clock freezing condition. The lists of side channel attacks that may be detected with our proposed clock-based sensor are depicted in Fig. 16. All these attacks require seconds to minutes to execute. Thus, the proposed sensor which is capable of operating on the order of picoseconds is more than sufficient.

Several countermeasures have been proposed over the years to defeat SCA attacks. There can be three types of comparing the existing countermeasures: algorithmic countermeasure, device-level protection schemes, and clock-based countermeasure: Phase Locked Loop (PLL). All these countermeasures are assumed to be protected against LLSI attack, static power side-channel attack, laser stimulation, and static photon emission. However, in literature, it is shown that some of these schemes are breakable by these attacks or not suitable enough to adopt due to high cost and complex fabrication steps [15], [16]. In this section, we have compared all these countermeasures and proposed our sensor as an overall protection scheme for all the attacks above-mentioned.

Masking has become the most prominent application to protect cryptographic implementations against physical side-channel attacks. According to the literature, the algorithmic countermeasures, e.g., masking schemes based on randomness, work for static power and static photon emission analysis; however, they do not protect against LLSI attack and PLS/TLS. Therefore, protection schemes at the circuit or device level are required to avert these attacks. Our proposed sensor is effective against all these attacks. Moreover, masking has tremendous overhead compared to ours, making it unsuitable to adopt in the first place unless the designers also want protection against side-channel attacks based on dynamic power consumption, timing, etc. [10].

There are also very few physical countermeasures existing to detect or prevent these attacks. The countermeasures that have been proposed, [14], [15], [16] focus more on the optical environment rather than the circuit environment of the attack. They try to detect/ prevent sample preparation steps or laser propagation. As a result, they have complex fabrication steps, additional silicon area, and nontrivial optimization. As a result, they are less natural to adopt, including complex fabrication steps, additional silicon area, CMOS incompatibility, and nontrivial optimization. We want to mention that the above-mentioned physical countermeasures do not help to protect against static power and photon emission analysis. Also, the PUFmon countermeasure needs a clock to work; if the clock is halted, which is the primary attack requirement, it will not work for any of the mentioned attacks. As a matter of fact, these countermeasures do not apply to detecting clock freezing conditions, so they are not adoptable otherwise.

If we compare the available countermeasure concerning the clock, a widespread assumption is that using an internal Phase Locked Loop (PLL) is sufficient to counter attacks via the clock. The PLL processes the signal from the external clock source and thus detaches it from the internal system clock; hence a glitch does not directly affect the system. However, even though the system clock is derived from the external clock signal by a PLL, fault injection by manipulation of the external clock signal is yet feasible [40]. Also, this countermeasure is mainly focused on clock glitching, whereas the attacks we mention have the clock freezing requirement in the range of seconds to hours. So, let us compare this PLL-based sensor with our one concerning fault injection; in our case, fault injection does not help defeat the sensor since only transient faults can be injected, which is usually insufficient to halt the internal clock permanently.

Based on the above comparison of all the countermeasures available, according to our knowledge, our proposed sensor

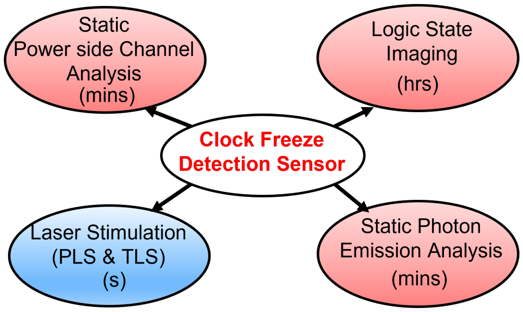


Fig. 16: List of side channel attacks with required clock freezing time that our proposed sensor can detect. Among these attacks some need always clock freezing (red) and some can be done in both conditions (blue).

is the first circuit-based countermeasure that gives protection against all the attacks mentioned above as a whole.

Although our voltage-based sensor was also conceived for protection against LLSI attacks, it may have possible application as a countermeasure against frequency injection attack such as frequency injection attack on ring oscillator (RO) based true random number generator (TRNG) [41]. This attack injects frequency of 1.8MHz in supply line of a secure microcontroller which has been used in ATMs. The frequency injection destroys the source of entropy of RO based TRNG in the secure microcontroller destroying the security in the process. Our sensor is able to detect modulation frequencies as high as 2MHz at room temperature and has the potential to detect such frequency injection attack. Another attack that our voltage-based sensor may detect is the pulse attack on voltage-based intrusion detection systems in controller area networks [42]. The objective of such attack is to block message transmission using a pulse width modulated signal of frequency less than 1.5 MHz. Our sensor is able to detect modulation at this frequency at nominal temperature. Even at higher temperature, our sensor has the potential to detect such attack if it is modified to work at a higher threshold at high temperatures.

VI. Conclusion and Future Work

In this paper, we developed a twofold detection approach to mitigate LLSI attacks. Our silicon and simulation results show that our clock freeze and voltage modulations sensors can detect attacks even in the presence of environmental noise and process variations. We also discussed the applicability of our sensors to other static SCA attacks. In future work, we aim to lower the overhead of both sensors, develop a simpler voltage modulation sensor, and create a voltage modulation sensor suitable for FPGAs.

VII. Acknowledgements

This effort was sponsored in part by NSF under grant number 2117349 and by the U.S. Government under Other Transaction number W9124P-18-9-0001 between AMTC and the Government. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the U.S. Government.

References

[1] 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.

[2] S. Tajik, H. Lohrke, J.-P. Seifert, and C. Boit, *On the Power of Optical Contactless Probing: Attacking Bitstream Encryption of FPGAs*. ACM, 2017, p. 1661–1674.

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

[4] H. Lohrke, S. Tajik, T. Krachenfels, C. Boit, and J.-P. Seifert, "Key extraction using thermal laser stimulation: A case study on xilinx ultrascale fpgas," p. 573–595, 2018.

[5] T. Krachenfels, T. Kiyan, S. Tajik, and J.-P. Seifert, "Automatic extraction of secrets from the transistor jungle using laser-assisted side-channel attacks," in *30th USENIX Security Symposium*, 2021.

[6] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Annual international cryptology conference*. Springer, 1999, pp. 388–397.

[7] F.-X. Standaert, "Introduction to side-channel attacks," in *Secure integrated circuits and systems*. Springer, 2010, pp. 27–42.

[8] H. Wang, D. Forte, M. M. Tehranipoor, and Q. Shi, "Probing attacks on integrated circuits: Challenges and research opportunities," *IEEE Design & Test*, vol. 34, no. 5, pp. 63–71, 2017.

[9] S. Chari, C. S. Jutla, J. R. Rao, and P. Rohatgi, "Towards sound approaches to counteract power-analysis attacks," in *Annual International Cryptology Conference*. Springer, 1999, pp. 398–412.

[10] E. Prouff and M. Rivain, "Masking against side-channel attacks: A formal security proof," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2013, pp. 142–159.

[11] B. Niu, G. M. E. Khoo, Y.-C. S. Chen, F. Chapman, D. Bockelman, and T. Tong, "Laser logic state imaging (llsi)," in *Proceedings from the 40th International Symposium for Testing and Failure Analysis (ISTFA 2014)*, 2014, p. 65.

[12] C. Boit, T. Kiyan, T. Krachenfels, and J.-P. Seifert, "Logic state imaging from fa techniques for special applications to one of the most powerful hardware security side-channel threats," in *2020 IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA)*. IEEE, 2020, pp. 1–7.

[13] T. Krachenfels, J.-P. Seifert, and S. Tajik, "Trojan awakener: Detecting dormant malicious hardware using laser logic state imaging," *arXiv preprint arXiv:2107.10147*, 2021.

[14] 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 *2016 IEEE 23rd International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA)*. IEEE, 2016, pp. 365–369.

[15] H. Shen, N. Asadizanjani, M. Tehranipoor, and D. Forte, "Nanopyramid: An optical scrambler against backside probing attacks," in *ISTFA 2018: Proceedings from the 44th International Symposium for Testing and Failure Analysis*. ASM International, 2018, p. 280.

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

[17] S. Roy, T. Farheen, S. Tajik, and D. Forte, "Self-timed sensors for detecting static optical side channel attacks."

[18] N. Vashistha, M. T. Rahman, O. P. Paradis, and N. Asadizanjani, "Is backside the new backdoor in modern socs?: Invited paper," in *2019 IEEE International Test Conference (ITC)*, 2019, pp. 1–10.

[19] A. Schlösser, D. Nedospasov, J. Krämer, S. Orlic, and J.-P. Seifert, "Simple photonic emission analysis of aes," in *Cryptographic Hardware and Embedded Systems – CHES 2012*. Springer, 2012, pp. 41–57.

[20] J. Couch, N. Whewell, A. Monica, and S. Papadakis, "Direct read of idle block ram from fpgas utilizing photon emission microscopy," in *2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, 2018, pp. 41–48.

[21] T. Krachenfels, H. Lohrke, J.-P. Seifert, E. Dietz, S. Frohmann, and H.-W. Hübers, "Evaluation of low-cost thermal laser stimulation for data extraction and key readout," *Journal of Hardware and Systems Security*, vol. 4, no. 1, p. 24–33, Nov 2019. [Online]. Available: http://dx.doi.org/10.1007/s41635-019-00083-9

[22] U. Kindereit, G. Woods, J. Tian, U. Kerst, R. Leihkauf, and C. Boit, "Quantitative investigation of laser beam modulation in electrically active devices as used in laser voltage probing," pp. 19–30, 2007.

[23] S. Chef, C. Chua, J. Tay, Y. Siah, S. Bhasin, J. Breier, and C. Gan, "Descrambling of embedded sram using a laser probe," in *2018 IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA)*. IEEE, 2018, pp. 1–6.

[24] S. Tada, Y. Yamashita, K. Matsuda, M. Nagata, K. Sakiyama, and N. Miura, "Design and concept proof of an inductive impulse self-destructor in sense-and-react countermeasure against physical attacks," *Japanese Journal of Applied Physics*, vol. 60, no. SB, p. SBBL01, 2021.

[25] A. Srivastava and P. Ghosh, "An efficient memory zeroization technique under side-channel attacks," in *2019 32nd International Conference on VLSI Design and 2019 18th International Conference on Embedded Systems (VLSID)*. IEEE, 2019, pp. 76–81.

[26] E. Hung, S. J. Wilton, H. Yu, T. C. Chau, and P. H. Leong, "A detailed delay path model for fpgas," in *2009 International Conference on Field-Programmable Technology*. IEEE, 2009, pp. 96–103.

[27] R. Newcomb, "Digital integrated circuits analysis and design-book reviews," *IEEE Circuits and Systems Magazine*, vol. 4, no. 4, pp. 34–40, 2004.

[28] I. P. . L.-V. M. Osuna, C. G., "A self-timed multipurpose delay sensor for field programmable gate arrays (fpgas)," *Sensors*, vol. 14, no. 1, pp. 129–143, 2013.

[29] R. R. Rao, A. Devgan, D. Blaauw, and D. Sylvester, "Parametric yield estimation considering leakage variability," in *Proceedings of the 41st Annual Design Automation Conference*, 2004, pp. 442–447.

[30] H.-Y. Wong, L. Cheng, Y. Lin, and L. He, "Fpga device and architecture evaluation considering process variations," in *ICCAD-2005. IEEE/ACM International Conference on Computer-Aided Design, 2005.* IEEE, 2005, pp. 19–24.

[31] H. T. Bui and Y. Savaria, "Design of a high-speed differential frequency-to-voltage converter and its application in a 5-ghz frequency-locked loop," pp. 766–774, 2008.

[32] S. P. Skorobogatov and R. J. Anderson, "Optical fault induction attacks," in *International workshop on cryptographic hardware and embedded systems*. Springer, 2002, pp. 2–12.

[33] C. Helfmeier, D. Nedospasov, C. Tarnovsky, J. S. Krissler, C. Boit, and J.-P. Seifert, "Breaking and entering through the silicon," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, 2013, pp. 733–744.

[34] D. S. Wolpert, *Managing temperature effects in nanoscale adaptive systems*. University of Rochester, 2011.

[35] J. Zhang, Y. Lin, Y. Lyu, and G. Qu, "A puf-fsm binding scheme for fpga ip protection and pay-per-device licensing," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 6, pp. 1137–1150, 2015.

[36] A. Moradi, "Side-channel leakage through static power," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2014, pp. 562–579.

[37] J. Ferrigno and M. Hlaváč, "When aes blinks: introducing optical side channel," *IET Information Security*, vol. 2, no. 3, pp. 94–98, 2008.

[38] J. Couch, N. Whewell, A. Monica, and S. Papadakis, "Direct read of idle block ram from fpgas utilizing photon emission microscopy," in *2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. IEEE, 2018, pp. 41–48.

[39] D. Nedospasov, J.-P. Seifert, C. Helfmeier, and C. Boit, "Invasive puf analysis," in *2013 Workshop on Fault Diagnosis and Tolerance in Cryptography*. IEEE, 2013, pp. 30–38.

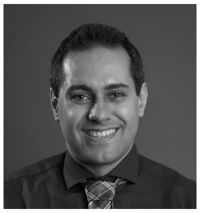
[40] B. Selmke, F. Hauschild, and J. Obermaier, "Peak clock: Fault injection into pll-based systems via clock manipulation," in *Proceedings of the 3rd ACM Workshop on Attacks and Solutions in Hardware Security Workshop*, 2019, pp. 85–94.

[41] A. T. Markettos and S. W. Moore, "The frequency injection attack on ring-oscillator-based true random number generators," in *Cryptographic Hardware and Embedded Systems - CHES 2009*, C. Clavier and K. Gaj, Eds., pp. 317–331.

[42] S. U. Sagong, R. Poovendran, and L. Bushnell, "Mitigating vulnerabilities of voltage-based intrusion detection systems in controller area networks," 2019.

TASNUVA FARHEEN received the B.S. degree in chemical engineering from the Bangladesh University of Engineering and Technology, Dhaka, Bangladesh in 2018. Currently she is a Ph.D. student in the Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL. Her research interests focus on the domain of hardware security, including physical backside attacks prevention and detection, anti-reverse engineering, SEM image analysis, FPGA implementation, simulation modeling and device fabrication.

SOURAV ROY received a B.S. degree in electrical and electronics engineering from the Bangladesh University of Engineering and Technology, Dhaka, Bangladesh with honors in 2011, and the M.S. degree in electrical, electronics and communication engineering from the Osaka University, Osaka, Japan in 2015. Currently he is pursuing Ph.D. in the Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL. His research interest include hardware security, including chip backside attack detection and prevention, hardware analog trojan detection and prevention and chip counterfeit detection and prevention.



SHAHIN TAJIK received the B.S. degree in electrical engineering from the K. N. Toosi University of Technology in 2010, and the M.S. and Ph.D. degrees in electrical engineering from the University of Berlin, in 2013 and 2017, respectively. He is currently an Assistant Professor with the Electrical and Computer Engineering Department of Worcester Polytechnic Institute (WPI), Worcester, MA. His field of research mainly includes non-invasive and semi-invasive side-channel analysis, Physically Unclonable Functions (PUFs), machine learning, FPGA security, and designing anti-tamper mechanisms against physical attacks. He has served as a reviewer for IEEE and ACM journals as well as a technical program committee member of many hardware security conferences, including Conference on Cryptographic Hardware and Embedded Systems (CHES), Symposium on Hardware Oriented Security and Trust (HOST), and Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC).

DOMENIC FORTE received the B.S. degree from the Manhattan College, Riverdale, NY, USA, in 2006, and the M.S. and Ph.D. degrees from the University of Maryland at College Park, College Park, MD, USA, in 2010 and 2013, respectively, all in electrical engineering. He is currently an Associate Professor with the Electrical and Computer Engineering Department, University of Florida, Gainesville, FL, USA. His research interests include the domain of hardware security, including the investigation of hardware security primitives, hardware Trojan detection and prevention, electronics supplychain security, and anti-reverse engineering. He was a recipient of the Presidential Early Career Award for Scientists and Engineers (PECASE), the Early Career Award for Scientists and Engineers (ECASE) by the Army Research Office (ARO), the NSF Faculty Early Career Development Program (CAREER) Award, and the ARO Young Investigator Award. His research has also been recognized through multiple best paper awards and nominations.