Self-timed Sensors for Detecting Static Optical Side Channel Attacks

Sourav Roy[1], Tasnuva Farheen[1], Shahin Tajik[2], and Domenic Forte[1]
[1]Department of Electrical and Computer Engineering, University of Florida
[2]Department of Electrical and Computer Engineering, Worcester Polytechnic Institute

***Abstract*—Sophisticated optical side-channel attacks such as Laser Logic State Imaging (LLSI) can destroy an entire system's security by extracting static signals. LLSI is based on chip failure analysis (FA) techniques and is conducted from the backside of an IC. It provides unlimited number of probes to observe static signals in the hands of an attacker. Several countermeasures have been proposed to prevent optical probing techniques like LLSI, but they have limitations such as complex fabrication steps, large area, etc. which makes them difficult to verify and implement. In this paper, we propose self-timed, CMOS-compatible sensors for easy-to-implement countermeasures to thwart LLSI attack. To conduct LLSI attack, the attacker needs to freeze the clock at a point of interest and modulate the voltage supply line at a known frequency. With these two attack surfaces in mind, we design and simulate clock freeze and voltage modulation detection sensors that can detect LLSI attacks with very high confidence.**[1]

I. Introduction

In recent years, embedded electronic devices are designed with strong cryptographic primitives and side channel attack resistant schemes. Despite such efforts, the security of deployed devices can still be compromised by attackers, who gain access to them in hostile environments and launch physical attacks. Side-channel analysis (SCA) attacks such as timing [1], electromagnetic emanation [2], power consumption [3], FIB-based probing [4], and optical probing [5] are examples of such threats. It has become apparent in recent years that laser-assisted optical probing attacks are very dangerous.

Optical probing was originally developed as a failure analysis (FA) technique. With increasing complexity to do FA from chip frontside due to increasing metal layer, analysis from chip backside provides more flexibility since the silicon substrate does not contain any impediments [6]. Optical FA techniques such as photon emission (PE) analysis [7], [8], thermal laser stimulation (TLS) [9], [10], and optical probing [11], [12], [13] 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 contactless manner.

Unfortunately, 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 in some cases logic gates. In 2021, the contactless nature of optical probing was exploited with great success where a technique called Laser Logic State Imaging (LLSI) bypassed randomness based on the most prominent side-channel countermeasure, e.g., masking schemes [14], [15], [16]. To launch an LLSI attack, the attacker needs access to FA equipment which can be rented hourly at low cost. In addition, the attacker needs to have control of the target chip's system clock and supply voltage. These are often easily accessible as external pins for popular targets such as smart cards. Its worth noting that an attacker need not even know other important information such as layout or location of assets to successfully attack the target chip [14]. Thus, LLSI is a practical attack that incurs little investment and time.

The optical probing countermeasures that have been proposed [17], [18], [19] focus more on optical environment rather than the circuit environment of the attack. That is, 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. In addition, some are only applicable to ASICs, not FPGAs. Thus, LLSI, remain a significant threat.

Contributions. In this paper, we propose low-cost, circuit-based self-timed sensors that are specifically designed to detect critical steps taken by attackers when performing LLSI attacks. To be more specific, our approach targets the two main attack surfaces of LLSI – system clock (freezing) and supply voltage (modulation). Using a twofold detection countermeasure, we can detect the LLSI attacks. To do so, our sensors must be self-timed since the block is frozen during an LLSI attack. Our main contributions in this paper are summarized as follows:

- To the best of our knowledge, this is the first circuit-based detection countermeasure for LLSI attack. Our sensors are low-cost, easy to parameterize, and verifiable during design.
- 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 clock freezing during attacks.
- 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.

The rest of the paper is organized as follows. In Section II, we introduce the background of laser logic state imaging (LLSI) and describe related works on optical probing countermeasures. In Section III, we propose and describe two detection-based countermeasures, clock freeze sensor and voltage modulation sensor. Then in Section IV, we discuss the simulation results. Finally, the conclusion is given in Section V.

[1]Distribution Statement A: Approved for Public Release

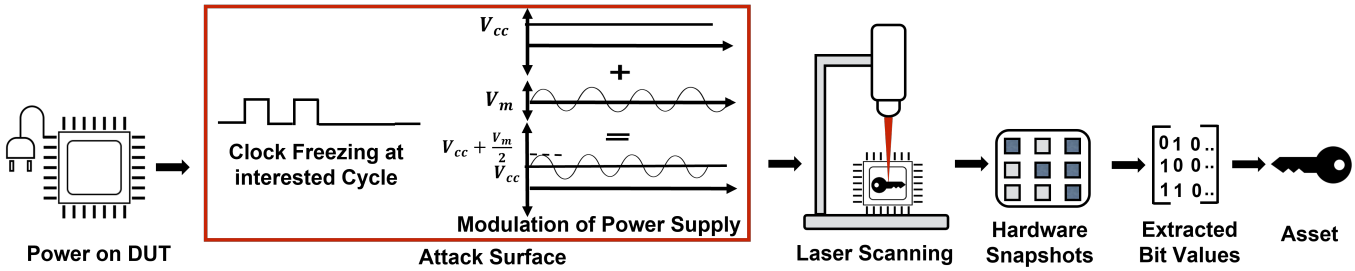


Fig. 1: The LLSI attack involves taking a hardware snapshots with a laser scanner while halting the clock and modulating the supply voltage to extract the bit values.

II. Background and Related Work

A. Laser Logic State Imaging (LLSI)

LLSI [20], [21] is a single trace optical probing technique that operates on static data and does not require repeated measurements of computations. In contrast, most of the conventional SCA attacks only operate with dynamic data (i.e., transistor and state transitions from '0' to '1' or vice versa) and require multiple measurements to achieve high signal-to-noise ratio (SNR). An illustration of steps taken in an LLSI attack is depicted in Fig. 1. A potential attacker should have access to a live device under test (DUT). The attack is then performed in three steps.

- Freezing the system clock to keep the IC logic and memory elements in a static state.
- Modulating the supply voltage so that the reflection of on vs. off transistors can be distinguished. 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.
- Creating an LLSI image by scanning the IC through its backside with a laser. In some cases, i.e., for certain wavelengths, this may require thinning the IC substrate first.

Fig. 2 depicts an image resulting from 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 in the 'ON' state at any given time. LLSI imaging shows a signature (bright white spots) on the locations where transistors are on. In the figure, the inverter on the right and left are producing logic 0 and logic 1, respectively. If the opposite PMOS and NMOS transistors were on, they would appear as bright spots instead. Thus, from this image, an attacker can determine data stored in the SRAM cell.

LLSI can compromise randomness based countermeasure by breaking its core assumption – that the adversary is limited in the number of simultaneous probes available to analyze all the distributed shares within a single clock cycle. Therefore, the employed randomness does not provide any protection against LLSI. In addition, static and on-die secrets in unmasked circuits, such as physically unclonable function (PUF) responses, true random number generator (TRNG) outputs, and combinational and sequential logic gates [22] can also be extracted by LLSI. Recent work also shows that deep learning can be used to extract sensitive key automatically [23] without

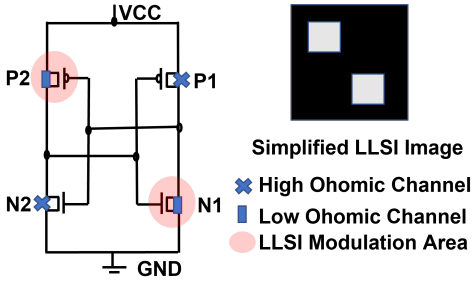


Fig. 2: An SRAM cell with transistors P2 and N1 in 'ON' state and associated LLSI image with bright spots at P2 and N1.

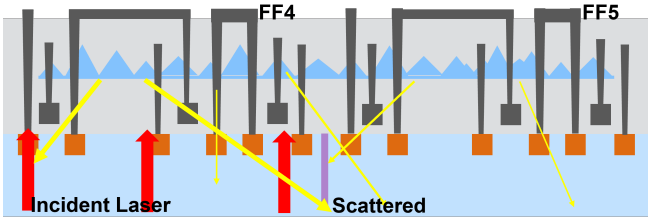


Fig. 3: Incident laser is scattered so reflection includes light from not only illuminated flip-flop (FF4) but also the neighbor ones (FF5).

even knowing the design and what regions of the IC contain sensitive information.

B. Related Work

Two countermeasures against optical probing attacks have been proposed. First, 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 [17]. 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. However, the distribution of photo detectors need to be optimized for best results and the protective layer comes with extra non standard fabrication and verification steps.

In another countermeasure, nanopyramid structures were built into an IC to randomly scramble the measurements reflected by laser irradiation [18]. This technique provides protection against optical probing by preventing unscrambled

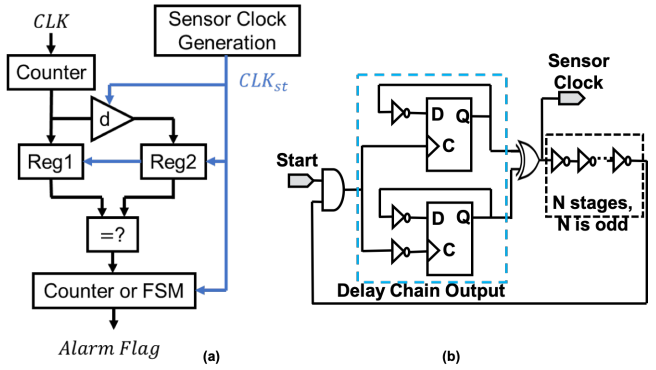


Fig. 4: (a) Architectural diagram of clock freeze sensor; (b) Self-timed sensor clock generation circuit.

signals from being captured by the detector as shown in Fig. 3. 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.

Compared to both photon detectors and nanopyramid approach, our sensor does not need any additional fabrication steps making it easier to implement with existing fabrication technology.

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[2]. It is worth mentioning that realistic LLSI attacks [23], [14], [20] 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 where black and blue lines represent data and sensor clock signals, respectively. 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 $Reg2$ store the count values taken with respect to the current and previous sensor clock cycles. A comparator compares 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 ensures that the sensor clock is at least two times slower than the system clock 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. In the next subsection, 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 flip flops (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 internal RO, and the other one by its falling edge. The number of inverters can be designed based on frequency of the system clock as long as sensor clock period is at least two times larger than the system clock period. 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. Another critical aspect 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 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 number 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 its first state. The FSM will check this condition for, e.g., five consecutive states. 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.

B. Voltage Modulation Sensor

As discussed in Section II-A, the attacker modulates the voltage supply during an LLSI attack. In order to thwart this, we propose a sensor that detects this modulation. According to the literature [14], voltage modulation as high as 0.7V peak to peak (p-p) with frequency of 90KHz is used to execute the LLSI attack. Note that modulation cannot reach the intended target due to the bypass capacitor on-chip at higher modulation frequencies and modulation voltage cannot be increased without hampering normal circuit behavior.

1) Architectural Diagram and Basic Operation: The block diagram of our voltage modulation sensor is given in Fig. 5(a). We start with a frequency to voltage converter (FVC) [24] as our foundation. FVC generates an output voltage V_{out} which depends on the frequency of the modulated input voltage V_{in}. Since a typical FVC circuit has certain requirements for its

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

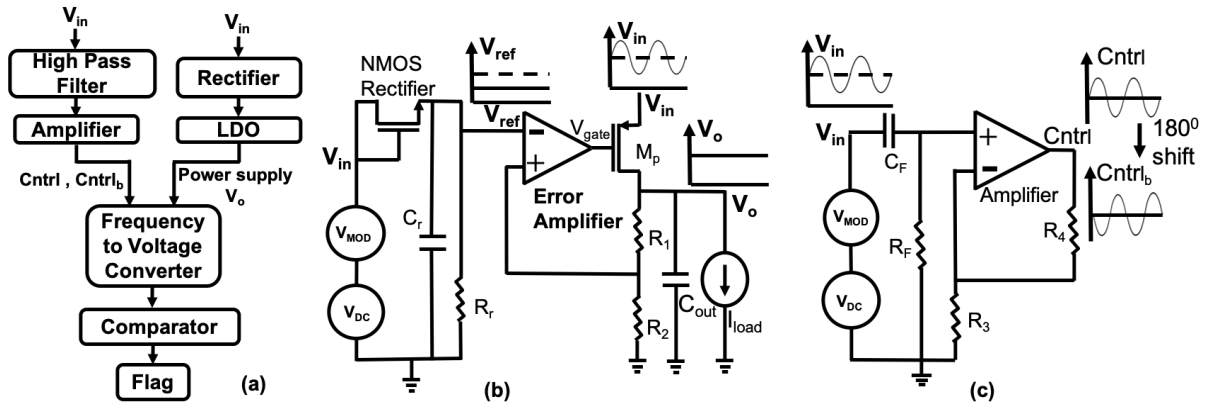


Fig. 5: (a) High-level block diagram of voltage modulation sensor; (b) LDO circuit along with NMOS rectifier to generate constant voltage for FVC and output of the LDO circuit (c) High-pass filter in combination with an amplifier to generate $Cntrl$ signal. Note that $Cntrl_b$ signal has a 180 degree phase shift.

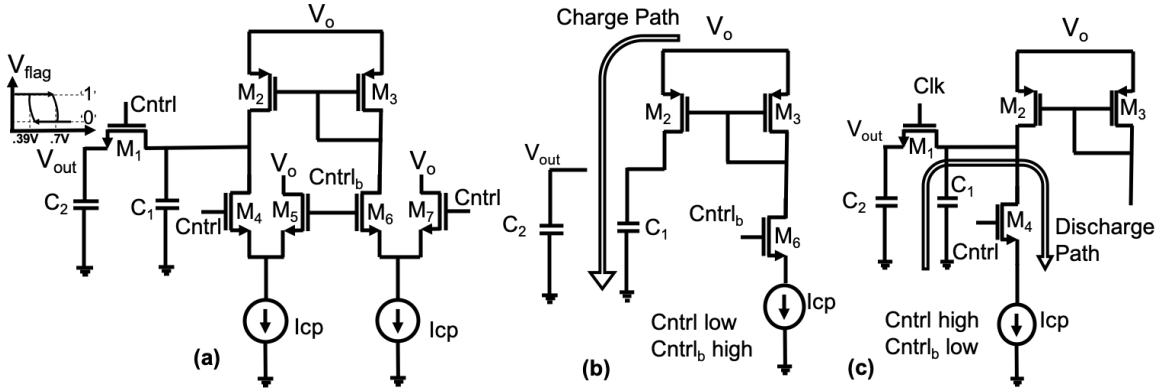


Fig. 6: (a) Frequency to voltage converter (FVC) circuit; (b) Charging cycle when $Cntrl$ and $Cntrl_b$ inputs are low and high, respectively; (c) Discharging cycle when $Cntrl$ and $Cntrl_b$ signals are high and low, respectively.

inputs (e.g., constant V_{dd}), we add preprocessing elements to it. First, a high-pass filter is used to extract only the modulation above 20kHz from the modulated voltage supply (V_{in}). Then the modulation is amplified to a voltage close to V_{dd}. This produces an oscillating signal that we refer to as $Cntrl$ and its inverse $Cntrl_b$ as shown in Fig. 5(c), 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 as shown in Fig. 5(b).

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 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(b).
- 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(c). 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.

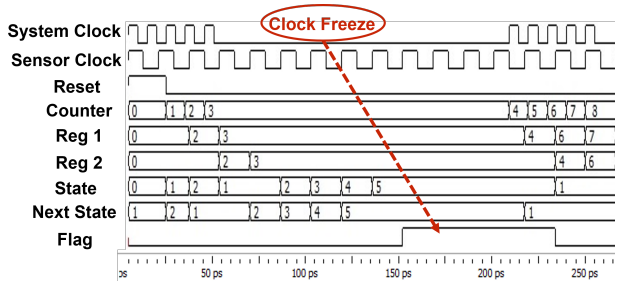


Fig. 7: Chronograph of the sensor simulation. The clock is frozen from 50ps to 200ps. The attack is detected at 150ps where the $Alarm/Flag$ is set high.

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 checks whether the output of FVC, V_{out} dropped below a set threshold V_{mod} or not. When there is modulation in supply line, V_{out} settles below V_{mod} and the Schmitt trigger comparator detects it and raises the flag. The flag 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 which accommodates the spikes present in V_{out} at the edges where switching occurs.

C. Twofold Detection Method

For LLSI attack, clock must be frozen and supply voltage must be modulated simultaneously. LLSI attack has to be carried out for at least one modulation period to get the state information. As a result, we designed our clock freeze sensor to detect clock freeze much faster than one modulation period so that it can detect even the fastest LLSI attack. The clock freeze detection sensor and voltage modulation detection sensor can work as standalone detectors to detect LLSI attack independent of each other. 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.

IV. Experimental Setup and Results

A. Clock Freeze Detection Sensor

In this section, we examine the effectiveness of our first sensor through simulations in ModelSim. The FSM of the sensor is set to output an alarm after 5 sensor clock cycles with a frozen system clock.

Fig. 7 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 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 [14], 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 [23]. Therefore, a five-state FSM is more than sufficient to capture the clock freezing by our proposed sensor.

B. Voltage Modulation Detection Sensor

In this section, we discuss our second sensor's implementation and provide simulations results to verify its effectiveness. We carried out the simulations 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 with modulation and simulated the behavior of Schmitt trigger comparator. We considered a input modulation of 175mV p-p at 90kHz frequency.

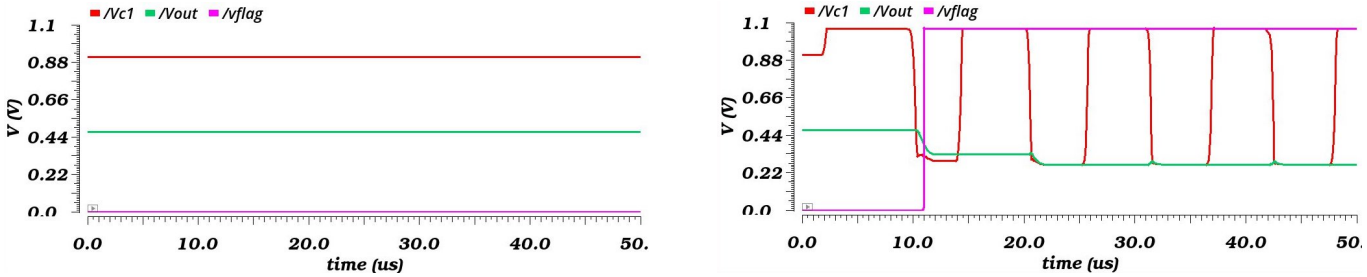
In the LDO circuit, The NMOS rectifier along with the resistor and capacitor produced the constant reference voltage V_{ref} of 550mV. LDO takes the modulated signal V_{in} as input at the source of the pass element M_p and produces constant output voltage V_o of 1.1V. The LDO output remains constant with modulation level change and also with FVC and comparator as added load. The $Cntrl$ and $Cntrl_b$ signals are fed into FVC circuit to control switching operations. $Cntrl_b$ signal is simulated as a 180^o phase shifted version of $Cntrl$ signal.

In the absence of supply voltage modulation, the output of FVC is a constant voltage (i.e., V_{static}) of about 470 mV. In Fig. 8a we see that no flag is raised if there is no modulation in supply line, i.e., the flag stays at logic low. 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. 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. In Fig. 8b, we see that flag is raised to logic high at the presence of voltage modulation at 90kHz as the output of FVC, V_{out}, went below set threshold V_{mod} of 390mV.

From these results, it is apparent that our sensor is able to detect modulation in supply line during an LLSI attack.

V. Conclusion and Future Work

While optical attacks are dangerous in general, the LLSI attack gives an attacker unlimited number of probes to attack



(a) No modulation

(b) 90kHz

Fig. 8: Voltages of internal nets and outputs of the voltage modulation sensor over time for 2 cases: (a) no modulation and voltage modulation of (b) 90kHz. 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) at 90kHz modulation frequency.

a chip and extract sensitive information. It is imperative that countermeasures be developed to prevent such powerful attacks and our circuit-based detection approach is a step in that direction. Our simulation results show that our clock freeze and voltage modulations sensors can detect attacks with a very high confidence. Although we expect our detection approach to thwart LLSI attacks, further improvements can be made. In future work, we aim to investigate the impacts of process and temperature variations on our sensors, lower the overhead of both sensors, develop a simpler voltage modulation sensor, and create a voltage modulation sensor suitable for FPGAs.

VI. 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] P. C. Kocher, "Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems," in *Annual International Cryptology Conference*. Springer, 1996, pp. 104–113.

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

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

[4] 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.

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

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] 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.