Polymorphic Sensor to Detect Laser Logic State Imaging Attack

Sourav Roy[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*—Laser Logic State Imaging (LLSI) is a failure analysis (FA) technique which is conducted from the chip backside. LLSI provides an unlimited number of contactless probes to observe static signals, such as security critical assets, which in the hand of an attacker poses a significant threat. Countermeasures that have been proposed so far to prevent backside optical attacks have limitations, such as additional fabrication steps, large area overhead, incompatibility with digital circuits, which makes their implementation challenging. In this paper, we propose all-digital polymorphic gate sensors for the first time in hardware security to detect LLSI attacks. Polymorphic gates change their behavior depending on environmental conditions, e.g., variations in supply voltage and temperature. Freezing the system clock and modulation of supply voltage are the main requirements of mounting an LLSI attack. With these two attack requirements in mind, we design and simulate a polymorphic gate-based sensor that behaves as a NOR gate when there is no supply voltage modulation and switches behavior between NAND gate and NOR gate in the presence of modulation. The sensor is able to detect LLSI attacks 100% of the time at room temperature even considering manufacturing variation and with a detection rate of more than98% for a temperature range of 0^oC to 85^oC.**

I. Introduction

Cryptographic primitives, such as symmetric key ciphers, public key ciphers, hash functions, and pseudorandom number generators are the basic building blocks of secure computing systems. Despite advancements in development of various countermeasures, attackers continue to explore novel methods to break the hardware implementations of such cryptographic primitives using physical attacks. These attacks enable adversaries, who have access to the device in a hostile environment, to extract secret keys and other assets from integrated circuits (ICs). Optical probing is one of such physical attacks, which is performed from the IC backside, and is capable of bypassing the most advanced protection schemes. Among the optical probing techniques, laser logic state imaging (LLSI) [1], [2], [3], [4] is a powerful method that can extract on-die static signals, and thus, break the most prominent side-channel security countermeasures, such as masking. What makes LLSI extremely powerful is that it provides an attacker with an unlimited number of probes and does not require repeated measurements unlike other optical attacks, e.g., photon emission (PE) analysis [5], [6] and laser voltage probing (LVP) [7], [8].

Unfortunately, there are not so many countermeasure options to mitigate the IC vulnerability to LLSI attacks. The existing device and package-level IC backside countermeasures against optical attacks [9], [10], [11] require additional non-standard fabrication steps. On the other hand, more recent circuit-level [12], [13] countermeasures impose high overhead and power consumption. Therefore, it remains an open question whether one can develop a low-overhead circuit-level countermeasure to avert LLSI attacks.

Virtually all the proposed countermeasures against laser-assisted SCA attacks focus on preventing the laser beam from entering the chip package, scattering the laser beam, or detecting the thermal variations caused by the thermal laser. However, there are other requirements for mounting successful LLSI attacks. To execute an LLSI attack, one needs to simultaneously freeze the system clock and provide a small peak-to-peak modulation to the victim chip's supply voltage. Both conditions can easily met in many real-world scenarios [3]. Similar to the sensor proposed in [13], we shift our focus from laser beam detection to detecting another attack requirement, namely the voltage modulation. However, in contrast to the analog sensor in [13], in this work, we make *novel use of polymorphic circuits* to detect changes to the circuit supply voltage using a CMOS-compatible all-digital circuit.

Polymorphic circuits change their behavior depending on external environment such as supply voltage, temperature, illumination, etc. Polymorphic circuits can be embedded into circuit functionality and designed to provide obfuscation under attack conditions. These circuits are digital, have low overhead and if embedded in functionality can potentially be very difficult to localize and remove by an attacker. Such circuits have tremendous potential to be used in hardware security, verification, and smart systems, but so far they have largely been limited to logic locking, camouflaging, and watermarking [14], [15], [16]. However, polymorphic circuits could be promising sensor candidates as well. In particular, polymorphic circuits that change behavior based on supply voltage can be applied for voltage modulation detection during an LLSI attack. Our main contributions in this work are summarized as follows:

- To the best of our knowledge, this is the first polymorphic circuit-based detection countermeasure proposed in the field of hardware security. Our sensor is low-cost, easy to parameterize, and compatible with digital design flow.
- We describe how to convert a voltage-sensitive NAND-NOR polymorphic gate to a supply voltage modulation sensor through proper transistor sizing. We also make adjustments to deal with practical challenges to the poly-

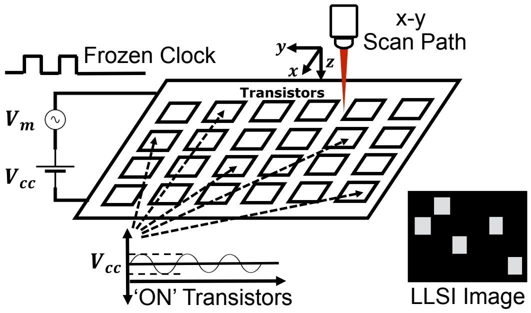


Fig. 1: LLSI image with modulation in supply line at frozen clock showing bright spot at the location of 'ON' transistors.

morphic sensor such as on-chip temperature variation.

- We integrate the output of our polymorphic voltage modulation sensor with a clock freeze sensor to detect LLSI.
- We perform an analysis of the proposed sensor and validate its behavior with aging analytically and across process variation and environmental variations via simulations.

The rest of the paper is organized as follows. In Section II, we introduce the background of LLSI, the LLSI attack model, existing LLSI countermeasures, polymorphic gates and synthesis of polymorphic gates. In Section III, we propose and describe the polymorphic sensor-based countermeasure. Then in Section IV, we discuss the simulation results. Finally, we draw conclusions and discuss future work in Section V.

II. Background and Related Work

A. Laser Logic State Imaging (LLSI)

As shown in Figure 1, a 2D pattern generated by LLSI for an IC gives the location of all 'ON' transistors by scanning a laser across the chip's backside. This breaks the main premise of randomness-based countermeasures such as masking schemes because it provides an attacker with an unlimited number of simultaneous probes to evaluate all the dispersed shares within a single clock cycle. LLSI can also be used to extract static signals in unmasked circuits, such as physically unclonable function (PUF) responses, true random number generator (TRNG) outputs, and the input/output of combinational and sequential logic gates [17]. In other words, LLSI can extract volatile secrets and reverse engineer circuits, provided enough measurement resolution. Recent research also reveals that deep learning on LLSI images can break sensitive keys [4] without even understanding the design or which sections of the IC contain sensitive data.

B. LLSI Attack Model

To carry out an LLSI attack, the attacker needs access to a live device under test (DUT) and then performs three steps:

1) *Freezing the system clock* which causes the IC memory and logic elements to be stuck in a static state.
2) *Modulating the supply voltage* at a known frequency to detect the reflected laser based on that frequency.
3) *Constructing an LLSI image* by scanning the IC backside with a infrared laser.[1] The modulation of the electric field of the on-state transistors due to the supply voltage modulation gives clear signatures on LLSI image. Thus, high and low logic signals can be differentiated in a non-invasive manner.

C. Existing Countermeasures

Countermeasures proposed against optical probing attacks, including LLSI, can be categorized into backside protection and circuit-based detection approaches.

In one of the backside protection approaches, light emitting diodes (LEDs) and photon detectors were fabricated in the active layer [9] while a protective optical layer was placed on the chip backside. The light from the LEDs was reflected by the protective layer, which was monitored by photon detectors. Any silicon thinning required for optical attacks on the chip backside will damage the layer and modify the reflection, allowing the detector to detect it. In another approach, backside buried metal (BBM) structure was used to detect backside thinning [18]. Again, metal serpentine-like structures at chip backside were proposed to prevent laser illumination-based fault injection along with weakening structures to detect backside thinning [19].

In a prevention approach, reflected laser irradiation were randomly scrambled using nanopyramid structures fabricated inside the IC [11]. By preventing unscrambled signals from being collected by the detector, this approach protects against all kinds of optical probing.

In a circuit based detection approach, self-timed ring oscillator and frequency-to-voltage converters circuits were used to detect the two major attack surfaces of LLSI attack, namely clock freeze and supply voltage modulation [13].

The comparison between our proposed polymorphic sensor and other countermeasures proposed in literature so far is summarized in Table I. The main advantage of ours compared to other countermeasures are the ease of integration into standard processes. Compared to the previous circuit-based approach, the proposed one is digital and much lower in overhead.

D. Polymorphic Electronics and Gates

Polymorphic electronics (or polytronics for short) were first introduced by Stoica et al. in 2001 [20]. In polymorphic electronics, changes in functionality do not depend on control signals but from changes in circuit characteristics and environmental conditions [21], [22], [23], [24]. For example, a NAND-NOR polymorphic gate was designed such that the gate changes behavior from NOR gate to NAND gate if supply voltage goes above a certain threshold [25] – this threshold can be controlled by proper sizing of particular transistors. Over the years different kinds of polymorphic gates have been

[1] In some cases, thinning of IC backside may be needed depending on the packaging. For modern flip-chip devices, thinning is not required.

TABLE I: Comparison among previous countermeasures and proposed polymorphic detection sensor.

	IC Backside-based Laser Detection Countermeasure [9], [10], [11]	**Circuit-based Countermeasure [12], [13]**	**Polymorphic Detection [This Paper]**
Extra fabrication and verification	Required	Not required	Not required
Application	Detects optical probing attacks that require backside thinning or scrambles signals collected during optical probing attacks	Detects LLSI attack	Detects LLSI attack
Type of structure or circuitry	LEDs or metal current paths or Silicon nanopyramids	Mixed signal circuits	Digital circuits
Area coverage	Covers the entire chip backside	Uses large area – requires ROs, amplifier, LDO, etc.	Uses the smallest area – no amplifier, LDO, etc.

developed including but not limited to NAND-NOR, AND-OR, NAND-XOR, and AND-OR-XOR where the polymorphic behavior was controlled by supply voltage, temperature or external signals [26]. The reconfigurable nature of the polymorphic circuits ensures a single circuit can implement multiple functionalities in a resource-efficient manner. The majority of the polymorphic gates were designed using conventional MOSFETs, but much of the recent work in hardware security has relied on beyond CMOS devices [14], [15].

E. Design of Polymorphic Circuits

Polymorphic circuits can be designed by hand or by using evolutionary algorithms [21]. For the latter, they can be evolved by connecting transistors freely in any arrangement deemed necessary with multiple requirements that has to be satisfied by the circuit. A generative process proposes candidate solutions that are evaluated against a fitness function incorporating desired criteria. The best candidates are chosen for reproduction, and the process repeats until an acceptable solution is found or after a specified number of generations. Cartesian Genetic Programming (GCP) has been used extensively in designing polymorphic circuits [27]. Polymorphic multiplexing [28] was also used to generate polymorphic circuits where conventional digital circuitry are developed for required functionalities and polymorphic multiplexing is used to choose among those functionalities. Currently, there is no established synthesis method that facilitates the design of polymorphic gates which makes the design of polymorphic circuit a highly customized endeavor.

Figure 2 shows a NAND-NOR polymorphic circuit where the output V_0 depends on the power supply level. As shown in Table II, the circuit behaves like a NAND gate at higher power supply level ($V_{DD} > V_*$). Otherwise, it behaves like a NOR gate. The power supply threshold at which the polymorphic circuit switches behavior depends on the sizing of the transistors, especially M7 and M8:

- When both inputs are low, output V_0 becomes high through M1 irrespective of power supply level.

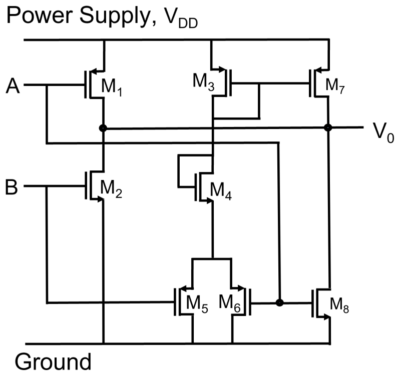


Fig. 2: V_{DD}-controlled polymorphic NAND-NOR gate.

- When both inputs are high, the output V_0 becomes low through M2 irrespective of power supply level.
- When the inputs are different, transistors M7 and M8 come into consideration. If A is low and B is high, V_0 can be high through M7 and M1 or low through M8 and M2. The pair that wins the battle depends on the power supply level. The transistors are sized in such a way that M7 and M1 wins at high power supply making output V_0 high. At low power supply M8 and M2 wins, making output V_0 low. Similarly, when A is high and B is low, output V_0 can be high through M7 or low through M8 under proper transistor sizing.

III. Proposed LLSI Attack Sensor

In order to detect the supply voltage modulation during LLSI attack, we design a polymorphic voltage modulation detection sensor according to this specification: It produces a logic '0' output if there is no modulation in the supply line; If there is modulation in the supply line (a condition of an LLSI attack), it produces a full rail-to-rail pulsating output at the same frequency as the supply voltage modulation. We then use the pulsating output of voltage modulation detection

TABLE II: Truth table of V_{DD}-controlled polymorphic NAND-NOR gate along with transistors impacting the output.

A	B	$V_{DD} > V_*$ V_0 (NAND)	$V_{DD} < V_*$ V_0 (NOR)	Regulating Transistors
0	0	1	1	M1, M7
0	1	1	0	M1, M7, M2, M8
1	0	1	0	M7, M8
1	1	0	0	M2, M8

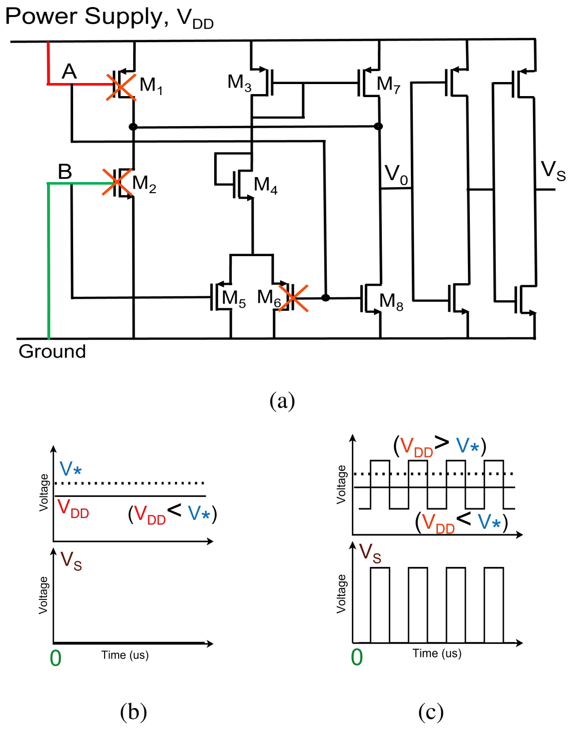
sensor to sense clock freeze and raise a flag when the clock is frozen – the other condition required by an LLSI attack.

A. Polymorphic Gate Voltage Modulation Detection Sensor

The circuit for polymorphic voltage modulation detection sensor is shown in Figure 3a. It is designed by modifying the circuit shown in Figure 2. Note that the transistors M1, M2, and M6 can be removed as shown with red cross in the figure. The input A is connected to the power supply and the input B is connected to ground making the output V_0 dependent on variation in supply voltage. To make the output rail-to-rail, two inverters are added at V_0. The sensor output after the inverters, V_s is shown in Figure 3b with no modulation and in Figure 3c with modulation at supply line. The chief considerations are (1) transistor sizing to get the desired behavior and (2) effects of temperature and process variation on the circuits' polymorphic behavior.

1) Basic Operation: The transistors in Figure 3a are sized in such a way that when there is no modulation in supply line, output V_s is 0. In other words, the polymorphic sensor works as a NOR gate at normal operating condition. The polymorphic sensor shows polymorphic behavior when there is modulation in supply line. The threshold V_* at which the polymorphic sensor changes behavior is chosen based on typical peak-to-peak voltage of about $400mV$ used during LLSI attack[2]. One example of successful LLSI attack with peak-to-peak modulation of $640mV$ can be found in [3]. The supply threshold, V_* is chosen about $100mV$ above the normal supply voltage V_{DD}. When the supply voltage is below the threshold, V_*, i.e., the low voltage cycle of the modulation or normal supply voltage, the sensor works as a NOR gate leading to a zero output at V_s and when the supply voltage is above V_*, i.e., the high voltage cycle of the modulation or more than $100mV$ of normal supply voltage, the sensor works as a NAND gate leading to V_{DD} at V_s. The operation can be summarized as follows:

- During no modulation, it works as a NOR gate and always outputs a logic 0.
- During low voltage cycle of modulation, it works as a NOR gate.
- During high voltage cycle of modulation, it works as a NAND gate.



(a)

(b)

(c)

Fig. 3: (a) NAND-NOR polymorphic gate-based voltage modulation sensor where the red crosses on M1, M2 and M6 indicate that they can be removed for sensor operation; (b) Sensor output with no modulation at supply line; (c) Sensor output with modulation at supply line.

At no modulation or at low voltage cycle of modulation when there is modulation in supply line, the transistor M8 has stronger effect than M7 which makes the output zero at V_s. At the high voltage cycle of modulation, M7 has stronger effect than M8 and output becomes V_{DD} at V_s. Thus, the output of the polymorphic circuit oscillates when there is a voltage modulation present in the supply line.

2) Impact of Aging and Process Variations: Aging and manufacturing process variation can alter the power supply threshold level V_* at which polymorphism occurs. As a result, during design, special care needs to be taken so that the sensor is able to detect LLSI even considering aging and process variation. With respect to process variation, we did Monte Carlo analysis to observe the effect of mismatch and process variation on the sensor and observed that the sensor is able to detect LLSI in a fairly accurate manner.

As transistors age due to negative bias temperature instability (NBTI), positive bias temperature instability (PBTI), and hot carrier injection (HCI), threshold voltage increases and they become slower. HCI occurs due to impact ionization while transistors are switching. In case of our sensor, if there is no modulation in supply line (the typical situation for the chip) we do not expect any switching and *thus the effects of HCI are negligible* at no modulation. As for NBTI in PMOS, the gate voltage has to be low with both source and drain voltage

[2] Note that the sensor can be designed to accommodate other values.

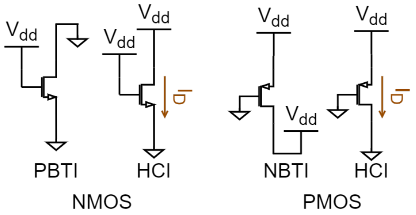


Fig. 4: Aging conditions in NMOS and PMOS.

high and for PBTI in NMOS, gate voltage has to be high with both source and drain voltage low as shown in Figure. 4. None of the transistors from M1 to M7 experience such conditions. M8 may experience partial PBTI as the drain voltage V_0 is close to zero. Nevertheless, full recovery from PBTI is possible when the stress is removed, i.e., when there is modulation in supply voltage. The other elements that may experience aging due to NBTI and PBTI are the inverters to the right but they will only introduce minor latency and *will not hamper the sensor's functionality.*. We have artificially increased the threshold voltage of M8 to mimic aging up to a year and the sensor is able to detect LLSI attack at room temperature with 100% accuracy.

3) Temperature Effects and Mitigation: Successful operation of the sensor depends on the change of polymorphic behavior at specific supply voltage threshold V_* determined by the voltage modulation during an LLSI attack. V_* also depends on temperature, as the mobility and threshold voltage of transistors change with the increase of temperature. The mobility degradation has a larger impact at high supply voltage compared to lower supply voltage which makes reliable operation of our sensor over broad temperature range a challenging prospect while keeping the sizes of the transistors within reasonable limits. As a result, we propose two separate sensors sized to reliably operate in two temperature ranges below and above 30^oC as shown in Figure 5. 30^oC is selected as a representative of room temperature and the two ranges represent temperatures below and above room temperature. V_{30} is the on-chip temperature sensor output at 30^oC which is stored using a voltage divider. Both the inputs to the comparator are affected similarly by any voltage modulation that may be present in the supply line. Let V_{s0} and V_{s1} represent the output V_s of the polymorphic voltage detection sensors properly sized to operate in the temperature ranges of 0^oC to 30^oC and above 30^oC respectively. A multiplexer with an on-chip temperature sensor along with the comparator is used to control its select line and thus choose which sensor output to use.

B. Polymorphic Gate Integrated with Clock Freeze Sensor

1) Architectural Diagram and Basic Operation: Figure 6 shows the architectural diagram of the LLSI detection sensor which integrates the polymorphic gate discussed above with a clock freeze sensor. The sensor inputs are a self-timed ring oscillator based clock Clk_{ro}, system clock Clk and the polymorphic gate output V_s. The sensor output $Alarm$ is only

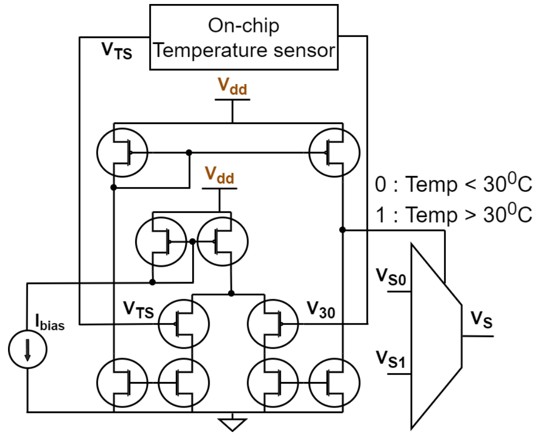


Fig. 5: Multiplexing sensor output for reliable operation over a broad temperature range. During an attack, both inputs to the comparator experience similar voltage modulation and select the appropriate sensor for detection.

1 when there is supply voltage modulation and Clk is frozen. Otherwise $Alarm$ is 0 indicating that an LLSI attack is not taking place. Note that we assume that $Alarm = 1$ will trigger a response from the chip such as zeroization, self-destruction, or hard reset to protect sensitive assets from recovery by LLSI. *However, the response itself is outside the scope of this paper.*

The LLSI attack sensor consists of a counter, the polymorphic gate, a comparator, a D-type flip flop and a ring-oscillator-based clock. Clk_{ro} is used to enable the counter and the D-flip flop at positive and negative cycles, respectively. The frequency of Clk_{ro} should be less than half the frequency of the expected modulation frequency. The counter is used to count up whenever there is positive edge on the system clock. That is, it will increase its value as long as the system clock Clk is not frozen to 0 or 1. The count value resets when Clk_{ro} goes to negative cycle.

As an example, let us assume there are four clock edges of Clk at positive cycle of Clk_{ro} as shown in Figure 6. At the end of the positive cycle of Clk_{ro} the Cnt value will be 4. The comparator will check whether the count value is greater than a threshold which is synthesized in the design, e.g., $Cnt_{th} = 3$. If the condition is satisfied then $Alarm = 0$ indicating normal operating condition. In case there is no voltage modulation, V_s will have no positive edge and $Alarm = 0$. While there is voltage modulation and also clock is frozen at either 0 or 1, the Cnt value will be stuck below Cnt_{th} and at the next negative cycle of Clk_{ro} and positive edge of V_s, the $Alarm$ will rise to 1 indicating that an LLSI attack is occurring.

2) Salient Point on Duration of LLSI Attack: The modulation frequency used during LLSI attack typically is in the few hundred KHz range as higher frequencies are usually filtered out by the decoupling capacitors present in modern chips. As a result, modulation frequency at V_s is much lower compared to frequency of system clock CLK. In order to carry out a successful LLSI attack, the clock must be frozen and supply voltage must be modulated for hours, which gives our sensor

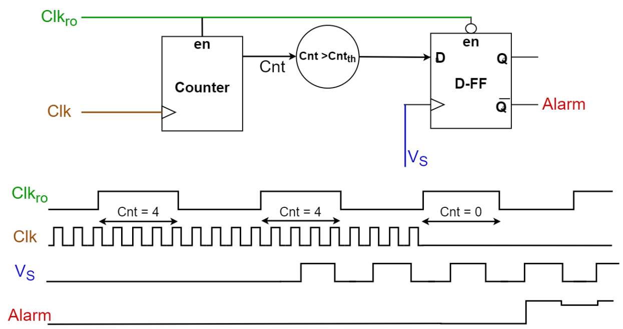


Fig. 6: Polymorphic voltage modulation sensor integrated with clock freeze sensor.

more than enough time to detect voltage modulation and clock freeze, Thus, an LLSI attack is sure to be detected.

C. Comparison to Circuit-level Sensor from [13]

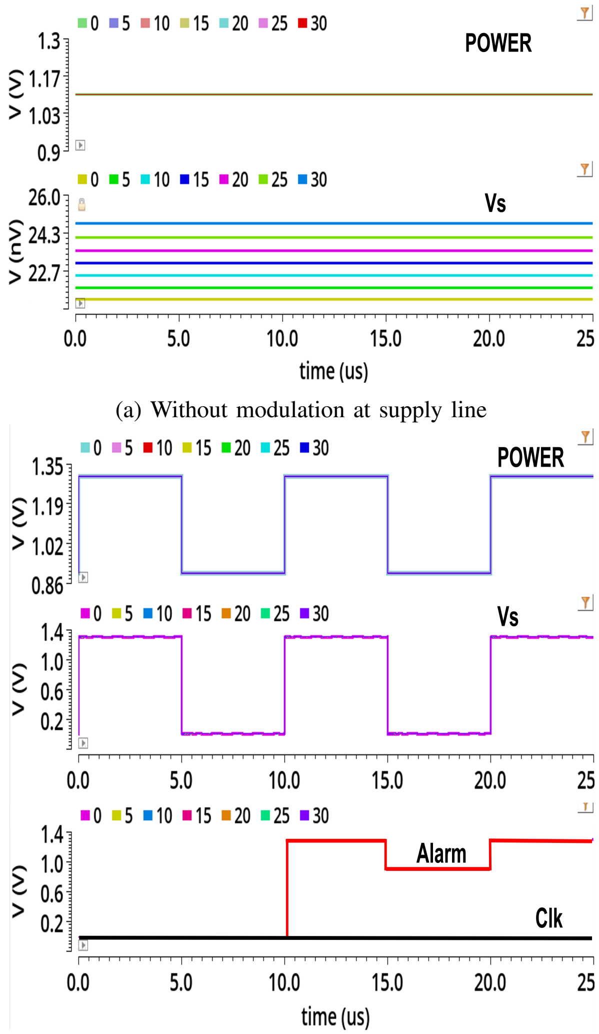
The voltage modulation and clock freeze sensors from [13] can operate independently of each other whereas the polymorphic sensor integrates the two to detect LLSI where clock freeze detection depends on voltage modulation detection. The area of the sensor from [13] is also much larger than the proposed digital, polymorphic sensor (see Section IV-D).

IV. Simulation Setup and Results

A. Simulation Setup

All the simulations were done in Cadence Virtuoso version IC6.1.7 with 45nm technology node. The model library was set to `tt` (i.e., typical typical). The transistors are designed to have nominal threshold voltage V_{th}. Transistor sizing used for different temperature ranges are given in Table III where units n indicates nanometer and μ indicates micrometer respectively. For all temperature ranges, a supply voltage modulation of 400mV peak to peak at a frequency of 100kHz was used.

At nominal temperature the sensor can detect modulation as low as 100mV peak to peak. But in that case, sensor fails to detect modulation at temperatures below 20^{o}C and temperatures above 30^{o}C. As a result, multiple sensors with modified transistor sizing are needed both in the case of low temperature and high temperature operations. Even lower peak to peak modulation can be detected by carefully sizing the transistors of multiple sensors to operate in different temperature ranges. It is a challenging prospect to detect lower voltage modulation at all temperature ranges keeping the number of sensors minimum and the transistor sizing within reasonable limit. At lower amplitude modulation, it is difficult to get clear signature from LLSI image and at higher frequency modulation larger than 100kHz may be obstructed by the decoupling capacitors present in modern ICs. As a result, 400mV peak to peak modulation at 100kHz was chosen as a practical representative stimulus which may be used during LLSI attack. For this work, we report the results with two sensors for two temperature ranges 0^{o}C to 30^{o}C and 30^{o}C to 85^{o}C to detect LLSI while clock is frozen and supply voltage is modulated at 400mV peak to peak.



(a) Without modulation at supply line

(b) With modulation at supply line

Fig. 7: Voltage modulation sensor output at temperatures 0^{o}C to 30^{o}C with and without supply voltage modulation of 400mV peak to peak.

B. Simulation Results Across Temperature Range

The simulation result for the temperature range of 0^{o}C to 30^{o}C is shown in Figure 7. Note that a similar result is found for the temperature range of 30^{o}C to 85^{o}C. In the figure, 'POWER' represents the supply voltage and V_s represents the polymorphic voltage modulation sensor output. Figure 7a represents absence of modulation with supply voltage (static $1.1V$) and Figure 7b shows the output when modulation is 400mV peak to peak. When there is no modulation at supply the sensor output V_s is logic low for all temperatures as shown in Figure 7a and $Alarm$ is also logic low (not shown). When there is modulation in supply voltage, at low cycle of modulation the supply voltage is $0.9V$ and high cycle of modulation supply voltage is $1.3V$. The output V_s of the sensor follows the supply voltage modulation at the same frequency when there is modulation, as shown in Figure 7b, but with a

TABLE III: Sizing of transistors at different temperature ranges.

Transistor Sizing / Temperature Range		M3	M4	M5	M7	M8
0^0C to 30^0C	Width	430n	1μ	4μ	8.5μ	120n
	Length	60n	250n	100n	75n	4.5μ
30^0C to 85^0C	Width	870n	2μ	8μ	10μ	450n
	Length	125n	500n	200n	145n	4u

rail-to-rail voltage. Consequently it results in a logic high for $Alarm$ for all temperatures when Clk is frozen (At logic low as shown in bottom figure in the Figure 7b).

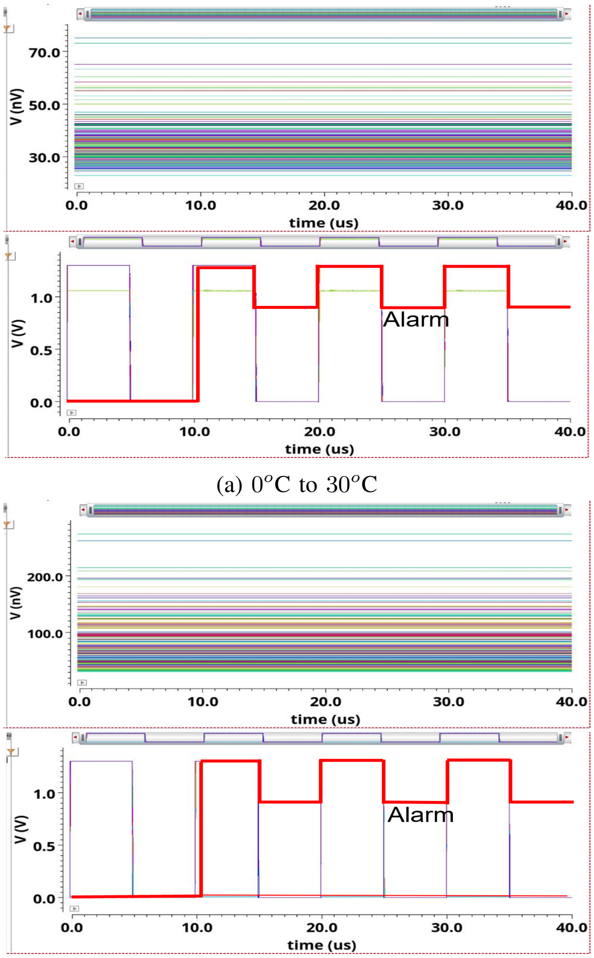
As explained in Section III-B the voltage modulation sensor output V_s can be used to raise the Alarm Flag shown in Figure 6. When there is voltage modulation with the clock frozen with a ring oscillator frequency, Clk_{ro} of 25KHz the Cnt value gets stuck at less than the threshold and $Alarm$ signal goes high at next positive edge of supply voltage modulation. The setup should work as long as the Clk_{ro} frequency is less than half of clock frequency of 100KHz. The $Alarm$ signal also experiences modulation of 400mV peak to peak as observed in Figure 7b but remains logic high for all intent and purposes which can be used to decide that LLSI attack is taking place.

C. Accuracy Across Process Variations and Aging

Extensive Monte Carlo simulation with 300 random simulation points was done on Cadence Virtuoso to explore the mismatch and manufacturing process variation effect on the sensor for both temperature ranges. At a temperature range of 0^oC to 30^oC, 300 out of 300 simulation points were successful to detect supply voltage modulation and $Alarm$ goes high leading to detection accuracy of 100%. At the temperature range of 30^oC to 85^oC, 294 out of 300 simulation points were able to detect supply voltage modulation contributing to a detection accuracy of 98%. The simulation results are shown in Figures 8a and 8b corresponding to temperature ranges 0^oC to 30^oC and 30^oC to 85^oC, respectively. At nominal temperature, the accuracy of detection is 100% considering both aging and process variation, which means the sensor is able to detect an LLSI attack with high confidence.

D. LLSI Sensor Overhead

Due to the presence of analog parts especially the capacitors in the voltage modulation sensor from [13], the area overhead of our proposed polymorphic sensor is about million times smaller. The comparison is shown in Table IV. We consider the multiplexer and comparator to select the appropriate sensor in the area overhead calculation of the voltage modulation part and ring oscillator, counter in area overhead calculation of the clock freeze sensor part, However, we assume that the on-chip temperature sensor is already available and do not consider it in the area overhead. The primary source of overhead in the voltage modulation sensor from [13] is the six capacitors present in the design that constitutes 99.99% of the area requirement of $56mm^2$.



(a) 0^oC to 30^oC

(b) 30^oC to 85^oC

Fig. 8: Monte Carlo simulation with 300 random simulations with 100% and 98% accuracy of detection at temperature ranges 0^oC to 30^oC and 30^oC to 85^oC respectively where top figure indicates output at no modulation and bottom figure indicates output at supply voltage modulation of 400mV peak to peak.

V. Conclusion and Future Work

We developed an all-digital, polymorphic sensor to detect LLSI attacks with high confidence. This circuit does not need additional complex fabrication steps like photodiodes, nanopyramids, and other backside structures. At the same time, compared to the previous analog sensor, this circuit has low overhead. On top of that all-digital nature of this sensor makes

TABLE IV: Area overhead comparison.

	Voltage Modulation Sensor	Clock Freeze Sensor	Total Area
Sensor from [13]	56 mm^2	13 μm^2	56 mm^2
Proposed Sensor	8 μm^2	10 μm^2	18 μm^2

it compatible with digital design flow. Although compared to previous analog circuit-based voltage modulation sensor which can detect modulation as low as 50mV, this circuit is less precise with detection ability of modulation as low as $100mV$ at room temperature, for all practical intents and purposes, this circuit is suitable to detect LLSI attack while being low cost and digital design compatible. In future, we will work on designing a single sensor that will be able to detect modulation at a broad temperature range using evolutionary methodologies and a self-sufficient, low-overhead clock freeze detection sensor that may be able to work independently of the voltage modulation sensor.

VI. Acknowledgements

This effort was sponsored in part by NSF under grant numbers 2117349, 2150122, and 2150123. 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] 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.

[2] 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.

[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] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] E. Amini, T. Kiyan, N. Herfurth, A. Beyreuther, C. Boit, and J.-P. Seifert, "Second generation of optical ic-backside protection structure," in *2020 IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA)*. IEEE, 2020, pp. 1–5.

[11] 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.

[12] 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.

[13] S. Roy, T. Farheen, S. Tajik, and D. Forte, "Self-timed sensors for detecting static optical side channel attacks," in *2022 23rd International Symposium on Quality Electronic Design (ISQED)*, 2022, pp. 1–6.

[14] S. Patnaik, N. Rangarajan, J. Knechtel, O. Sinanoglu, and S. Rakheja, "Advancing hardware security using polymorphic and stochastic spin-hall effect devices," in *2018 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 2018, pp. 97–102.

[15] N. Rangarajan, S. Patnaik, J. Knechtel, R. Karri, O. Sinanoglu, and S. Rakheja, "Opening the doors to dynamic camouflaging: Harnessing the power of polymorphic devices," *IEEE Transactions on Emerging Topics in Computing*, 2020.

[16] T. Wang, X. Cui, D. Yu, O. Aramoon, T. Dunlap, G. Qu, and X. Cui, "Polymorphic gate based ic watermarking techniques," in *2018 23rd Asia and South Pacific Design Automation Conference (ASP-DAC)*. IEEE, 2018, pp. 90–96.

[17] 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.

[18] T. Miki, M. Nagata, H. Sonoda, N. Miura, T. Okidono, Y. Araga, N. Watanabe, H. Shimamoto, and K. Kikuchi, "Si-backside protection circuits against physical security attacks on flip-chip devices," *IEEE Journal of Solid-State Circuits*, vol. 55, no. 10, pp. 2747–2755, 2020.

[19] S. Borel, L. Duperrex, E. Deschaseaux, J. Charbonnier, J. Cledière, R. Wacquez, J. Fournier, J.-C. Souriau, G. Simon, and A. Merle, "A novel structure for backside protection against physical attacks on secure chips or sip," in *2018 IEEE 68th Electronic Components and Technology Conference (ECTC)*, 2018, pp. 515–520.

[20] A. Stoica, R. Zebulum, and D. Keymeulen, "Polymorphic electronics," in *ICES2001 4th International Conference on Evolvable Systems: From Biology to Hardware*, 2001, pp. 291–301.

[21] A. Stoica, R. Zebulum, X. Guo, D. Keymeulen, M.-I. Ferguson, and V. Duong, "Taking evolutionary circuit design from experimentation to implementation: some useful techniques and a silicon demonstration," *IEE Proceedings - Computers and Digital Techniques*, vol. 151, pp. 295–300(5), July 2004.

[22] R. Ruzicka and V. Simek, "Nand/nor gate polymorphism in low temperature environment," in *2012 IEEE 15th International Symposium on Design and Diagnostics of Electronic Circuits Systems (DDECS)*, 2012, pp. 34–37.

[23] F. Parveen, Z. He, S. Angizi, and D. Fan, "Hybrid polymorphic logic gate with 5-terminal magnetic domain wall motion device," in *2017 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2017, pp. 152–157.

[24] A. Rezaei, J. Gu, and H. Zhou, "Hybrid memristor-cmos obfuscation against untrusted foundries," in *2019 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2019, pp. 535–540.

[25] R. Ruzicka, L. Sekanina, and R. Prokop, "Physical demonstration of polymorphic self-checking circuits," in *2008 14th IEEE International On-Line Testing Symposium*, 2008, pp. 31–36.

[26] R. Tesař, V. Šimek, R. Růžička, and A. Crha, "Design of polymorphic operators for efficient synthesis of multifunctional circuits," *Journal of Computer and Communication*, vol. 4, pp. 151–159, 2016.

[27] J. Miller and A. Turner, "Cartesian genetic programming," in *Proceedings of the Companion Publication of the 2015 Annual Conference on Genetic and Evolutionary Computation*, ser. GECCO Companion '15. New York, NY, USA: Association for Computing Machinery, 2015, p. 179–198. [Online]. Available: https://doi.org/10.1145/2739482.2756571

[28] Z. Gajda and L. Sekanina, "On evolutionary synthesis of compact polymorphic combinational circuits," *J. Multiple Valued Log. Soft Comput.*, vol. 17, pp. 607–631, 2011.