2023 IEEE Computer Society Annual Symposium on VLSI (ISVLSI) | 979-8-3503-2769-4/23/$31.00 ©2023 IEEE | DOI: 10.1109/ISVLSI59464.2023.10238545

LAT-UP: Exposing Layout-Level Analog Hardware Trojans Using Contactless Optical Probing

Sajjad Parvin[𝕌], Mehran Goli[𝕌,†], Thilo Krachenfels[◇], Shahin Tajik[⋆], Jean-Pierre Seifert[◇,⋇],
Frank Sill Torres[‡], and Rolf Drechsler[𝕌,†]

[𝕌] Institute of Computer Science, University of Bremen, Germany
[†] Cyber-Physical Systems, DFKI GmbH, Germany
[◇]Chair of Security in Telecommunications, Technische Universität Berlin, Germany
[⋆]Department of Electrical and Computer Engineering, Worcester Polytechnique Institute, USA
[‡] Institute for the Protection of Maritime Infrastructures, German Aerospace Center, Germany
[⋇]Fraunhofer SIT, Germany
{parvin, mehran, drechsler}@uni-bremen.de, frank.silltorres@dlr.de, {tkrachenfels,jpseifert}@sect.tu-berlin.de, stajik@wpi.edu

***Abstract*—The insertion of a *Hardware Trojan (HT)* into a chip after the in-house layout design is outsourced to a chip manufacturer for fabrication is a major concern, especially for mission-critical applications. While several HT detection methods have been developed based on side-channel analysis and physical measurements to overcome this problem, there exist stealthy analog HTs, i.e., capacitive and dopant-level HTs, which have negligible or even zero overhead on the chip. Thus, these stealthy HTs cannot be detected using the aforementioned methods. In this work, we propose a novel analytical approach to detect these *Layout-level Analog Trojans (LAT)*. Our proposed method uses an extension of Optical Probing (OP) for LAT detection, namely, the *Laser Logic State Imaging (LLSI)* technique. In principle, to detect LATs using LLSI, we only need the golden design and not a golden chip, which is not typically available. As we take advantage of LLSI to detect HTs, our approach is non-invasive, less costly, and scalable to larger designs. We report experimental results on a malicious RISC-V to demonstrate the effectiveness of our approach in detecting LATs.**

***Index Terms*—Optical Probing, LLSI, Hardware Trojan, Layout-level Analog Trojan, RISC-V, Hardware Security.**

I. Introduction

Due to the high cost of building a semiconductor manufacturing facility, many companies outsource their in-house design to a third-party company (usually abroad) to fabricate their design. Outsourced manufacturing raises a major concern about the integrity of the manufactured integrated circuit (IC), particularly design alteration through *Hardware Trojan (HT)* insertion. In general, HTs can be inserted into a chip as extra logic gates, also known as *Layout-level Digital Trojan (LDT)*, during the fabrication process in an untrusted foundry [1]. The inserted logic gates can act as a backdoor for an adversary to exploit secret data or make the chip perform maliciously. For example, a LDT inserted into a cryptographic core during fabrication can result in leaking the key when applying specific input values to the core. Hence, an adversary can manipulate the input and infiltrate the chip.

Several methods have been proposed in the literature to expose HTs [2], [3]. These methods rely on side-channel analysis such as EM analysis [4], power analysis [5], and leakage current analysis [6] of a chip to detect whether there exists a HT or not. However, there are two problems associated with these techniques. First, a HT can be designed in a way to have an infinitesimal area and power consumption that does not appear in the side-channel analysis. For example, in [7], an analog capacitive HT named "A2" is proposed, which has negligible power consumption and occupies only a small area on a chip. Fig. 1 shows the working principle of the "A2" HT, which works based on the gradual increase in charge of a capacitor. "A2" triggers a malicious functionality in a chip upon storing enough charge in the capacitor. Moreover, in [8], another analog HT is proposed that it is created by only altering the doping polarity in a single transistor. Consequently, this alteration in the doping polarity introduces an HT to the IC. A dopant swapping HT results in a node to stuck-at "0/1". Fig. 2 illustrates the stealthy dopant effect. Another example of such a HT can be created by a slight change in a transistor's length of a logic gate which results in an extra delay. We call these types of HTs *Layout-level Analog Trojan (LAT)*. They can be inserted at the layout level as an analog block and cannot be detected by conventional HT detection methods. The second problem with existing HT detection techniques is the requirement of a golden chip to detect LATs, which typically is not available. To the best of our knowledge, [9] is the only method that can detect the doping polarity type of LATs in a logic gate based on delayering a chip and using a scanning electron microscope. While this method does not require a golden chip to perform security validation, it destroys the chip when performing this analysis. Besides, this process needs high effort and cost.

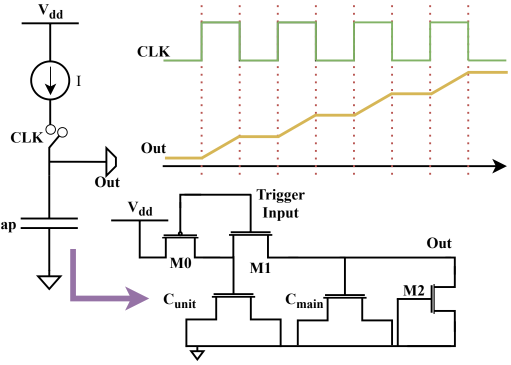
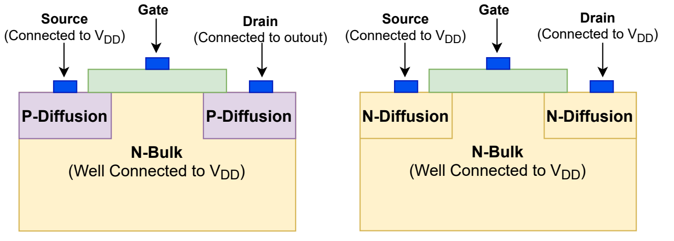


Fig. 1: Operation principle of A2 trojan.

The *Laser Logic State Imaging (LLSI)* technique is a subset of *Optical Probing (OP)* techniques, which have been shown as a promising solution to detect HTs (that are based on adding extra logic gates) on FPGAs [10], [11]. They work based on a comparison between snapshots of the reference and a given FPGA's configurable logic blocks (CLBs). In case of difference, the given FPGA's CLB is suspected of containing a HT. In this work, we adopt the LLSI technique for ASIC designs to detect the pattern difference between the in-house layout and the fabricated chip with respect to LATs.

The **main contributions** of this paper can be summarized

979-8-3503-2769-4/23/$31.00 ©2023 IEEE



(a) Standard PMOS. (b) Trojan-infected PMOS.

Fig. 2: Standard PMOS transistor vs. PMOS with doping-level trojan

as follows:

- Simulation of reflected light due to OP, when doping polarity of a transistor is swapped to act as a LAT.
- Performing LLSI simulation on several gates infected with LATs. When having LATs, we show that the LLSI images of the non-modified and modified designs differ significantly. Thus, our proposed approach can precisely localize the LATs on a chip.
- Inserting a LAT into a single-cycle RISC-V [12] design. This experiment demonstrates the scalability of our proposed approach using LLSI to detect LATs.

II. Contactless Optical Probing

In this section, we explain the necessary background and formulation for OP to be used for the rest of the paper.

A. Methodology and Setup

OP capabilities are usually embedded into a Laser Scanning microscopes (LSMs), in which a focused laser beam is scanned using galvanometric mirrors or statically pointed at a single point on a chip. At the same time, a detector collects the reflected light. Since silicon is transparent to light in the *Near-InfraRed (NIR)* spectrum, probing an IC through its backside is possible without thinning or preparation of the chip. As shown in Fig. 3, the laser light focused on a region of the die area of IC passes the bulk silicon and travels through the active areas of transistors. A portion of the incident light is reflected; for instance, when the incident light hits the first metal layer. It then travels back through the silicon into the microscope lens. Afterward, the beam splitter directs the reflected light to an optical detector, which converts its intensity into voltage.

B. Origin of the Signal

At a wavelength of around 1300 nanometers, a change in absorption and refraction of the laser beam interacting with a device occurs mainly due to free carriers. The number of free carriers varies according to the voltage present at the device [13], [14]. In this case, the change in the absorption coefficient α and the index of refraction n for wavelength λ due to the number of free carriers are defined as follows [13]:

$$\Delta\alpha = \frac{\lambda^2 q^3}{4\pi^2 c_0^3 \epsilon_0 n_0}\left[\frac{\Delta N_e}{m_e^2 \mu_e} + \frac{\Delta N_h}{m_h^2 \mu_h}\right] \tag{1}$$

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

where n_0, q, ϵ_0, c_0, μ, m, and ΔN denote the index of refraction of un-doped silicon, electron charge, the permittivity of free space, speed of light in vacuum, mobility, effective mass, and changes in charge carrier density, respectively. The parameters h and e stand for holes and electrons, respectively. By changing the present voltage at the semiconductor interface, the charge carrier density N (i.e., the number of free carriers in the signal path) changes. The maximum amplitude of ΔN highly depends on the doping concentration [14]. It has been shown in [14] that next to the well doping concentration, also the diffusion doping impacts $\Delta\alpha$ and Δn.

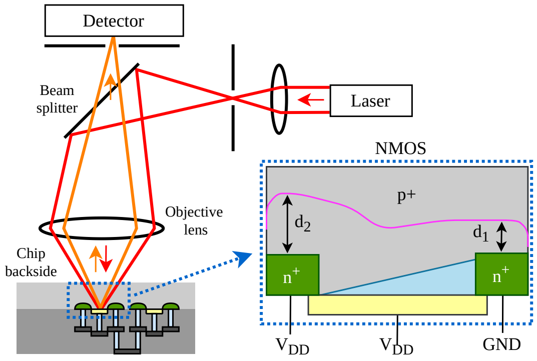


Fig. 3: Illustration of an optical probing setup when the laser is focused on an NMOS biased in saturation region.

C. Optical Probing for Data Extraction

As voltage differences applied to a transistor can be detected using OP, data stored or processed on an IC can be extracted as well. The probing technique where the laser is parked at a certain location of the chip is called *Electro-Optical Probing (EOP)*[1]. Using EOP, sensitive data processed by the IC can be extracted [15], [16]. Due to having a weak modulation of the reflected optical beam, the chip needs to be run in a loop, and the captured signal needs to be integrated to achieve a decent *Signal-to-Noise Ratio (SNR)*.

In order to localize the paths carrying periodic signals on the chip, the laser can be scanned over the chip while feeding the detector's output into a narrow-width bandpass filter set to the frequency of interest. Consequently, a gray-scale encoded image of the scanned area is obtained where bright spots indicate areas with switching activity. This technique is called Electro-Optical Frequency Mapping (EOFM)[1]. By injecting a periodic pattern into the data processed by the device, all potential locations on the chip that may carry data of interest can be identified using EOFM and later probed using EOP [15]–[17].

Since the device has to be operated in a loop for this approach, single-trace measurements, i.e., where the data of interest is only present once on the chip, are impossible. An extension to EOFM, called LLSI, allows such single-trace measurements by modulating the power supply of the device during operation and conducting EOFM. In this way, the charge carrier density of transistors is modulated, and transistors in the on- and off-states can be distinguished. Therefore, LLSI allows the extraction of data from on-chip memories, such as flip-flops and SRAM cells [18], [19] and the detection of malicious modifications on FPGAs [10].

D. Optical Resolution and Technology Size

Even though there are different ways to define the spatial resolution R of optical probing, the most common definition is

[1] In the case of using a coherent light source, EOP is typically called *Laser Voltage Probing (LVP)*, and EOFM is called *Laser Voltage Imaging (LVI)*.

defined in the form of Fourier optics and Abbe's criterion [20] as $R = 0.5\lambda/NA$ where λ is the wavelength of the light and NA is the *Numerical Aperture* of the microscope system. The parameter R can be seen as the minimum distance between resolvable two-point sources [20]. The intensity of the laser spot can be described as Gaussian distribution [20] with

$$p(r) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{\frac{-(r)^2}{2\sigma^2}} \tag{3}$$

where r is the distance from the center of the beam and σ is the standard deviation which can be calculated as $\sigma = 0.37\lambda/NA$ for a confocal microscope [20].

Based on the resolution definition, the optical resolution can be enhanced either by using a light with a lower wavelength or by increasing the NA. However, the opaqueness of silicon to the wavelength λbelow 1100 nm increases the challenges for sample preparation. Interested readers can refer to the work of Boit et al. [21] for a study on probing using visible light. Alternatively, the theoretical maximum NA achievable by a classical microscope lens, i.e., through air, is 1. However, existing high-end lenses achieve an NA of only around 0.75, resulting in a maximum possible resolution between 733 nm and 866 nm for a λ of 1100 nm and 1300 nm, respectively. A *Solid Immersion Lens (SIL)* can increase the NA up to around 3.5, increasing the resolution to around 200 nm, allowing Failure Analysis (FA) of single transistors down to 10 nm technologies [22].

E. Multilayer Reflection Formulation of Optical Probing

Optical probing's reflected signal can be studied using Fresnel's equation [23]. Using this equation, we can find the interference of light in a medium composed of several layers. At each medium's interface, due to changes in refraction and absorption coefficients of a medium, some part of the light gets absorbed and some other parts of the incident light passes through. In Fig. 4, we have a three interface medium (mediums i, j, and k) where the **H** matrices are called transfer matrix, and the **L** matrix is called propagation matrix. The parameters ρ, τ, and β are related complex refraction index of the two interfaces and the distance between two interfaces [14], respectively. The system matrix (**S**) of the reflected signal can be calculated using matrix multiplication as follows:

$$H_{ij} L_j H_{jk} = S = \begin{pmatrix} S_{11} & S_{12} \\ S_{21} & S_{22} \end{pmatrix}, \tag{4}$$

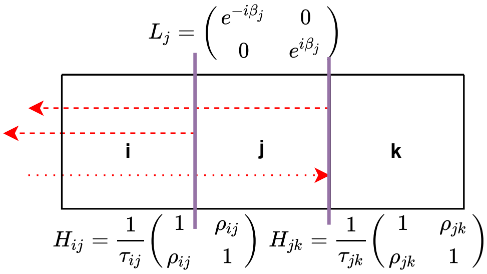
where the value of reflected light is $R = |\frac{S_{12}}{S_{22}}|^2$.

In [23], it has been shown how reflected light of a MOSFET's drain biased in reverse (PN junction) and a MOSFET biased as a varactor looks like using this formulation.

F. Reflection Caliber Value (RCV)

In [24], a simple-to-use model is proposed for the reflection of a transistor under OP. This model, which is called, RCV, approximates the reflected light from a transistor's active region as a linear function of the applied voltage to the transistor's terminals (V), amplification constant of transistor K ($K_{PMOS} = 1.3K_{NMOS}$), transistor's fabrication related parameter (β), the power of incident laser light (P_L), and the area of transistor's active region. The RCV value can be expressed as follow:

$$RCV = V \times K \times \beta \times P_L \int_0^{2\pi} \int_0^{r_{spot}} p(r) \times A(r, \theta)\, dr d\theta, \tag{5}$$



$L_j = \begin{pmatrix} e^{-i\beta_j} & 0 \\ 0 & e^{i\beta_j} \end{pmatrix}$
i
j
k
$H_{ij} = \frac{1}{\tau_{ij}} \begin{pmatrix} 1 & \rho_{ij} \\ \rho_{ij} & 1 \end{pmatrix}$
$H_{jk} = \frac{1}{\tau_{jk}} \begin{pmatrix} 1 & \rho_{jk} \\ \rho_{jk} & 1 \end{pmatrix}$

Fig. 4: Matrix formulation of reflected light in a multi-layer medium.

where $p(r)$ and $A(r, \theta)$ are the laser's power Gaussian distribution and the area of the active region under the laser spot in polar coordinates, respectively. Furthermore, (5) can be expanded to be applicable for a FET which has Drain (D), Gate (G), and Source (S) regions. The RCV of a single transistor is the sum of all the active regions of a transistor (R) light under OP, which is shown below:

$$RCV_{FET} = \sum_{\forall R \in FET\{D,S,G\}} RCV_R. \tag{6}$$

Since, in real designs, we have standard logic gates, we can expand the RCV equation furthermore to simulate probing a logic gate cell. The RCV of a logic gate cell is the sum of RCV_{FET} for all the transistors (t) in a logic gate cell. RCV_{Cell} is represented as follows:

$$RCV_{Cell} = \sum_{\forall t \in Cell} RCV_{FET_t}. \tag{7}$$

III. Reflection Matrix Formulation of Doping Level Trojan

When a doping level HT is implemented in a chip, the reflected light from drain/source to bulk of a transistor does not act as well-studied "PN" junction under OP [14]. As shown in Fig. 2 (b), when we have a stealthy doping LAT, we have a "$N^+ - N$" junction for a PMOS ("$P^+ - P$" junction for an NMOS) [8]. This homojunction has a partially depleted region. Thus, by applying a voltage, this partially depleted region's width can get modulated, as discussed in [25]. Since modulation of *Space Charge Region (SCR)* based on the applied voltage to a MOSFET's terminal plays a major role in modulation of OP light, we can probe the stealthy dopant using OP technique.

To analytically show how the reflected light from a junction with the same doping material but with different doping concentrations level under various applied voltages looks like, we performed the multilayer reflection formulation of OP, as discussed in Section II-E, on a"$N^+ - N$" region. The result of reflected light from the matrix formulation is shown in Fig. 5. In Fig. 5, $\frac{\Delta R}{R_0}$ is the change in reflection when no voltage is applied to the device. This simulation is done on several different well concentrations while the diffusion concentration of a modified NMOS is kept to 10^{21} for all the simulation runs. Moreover, this experiment is only done on the modified NMOS's bulk-to-diffusion path.

As shown in Fig. 5, when the homojunction is doped with a similar dopant though having a different doping concentration, the reflected light becomes weaker when the difference between bulk and diffusion doping concentration is smaller.

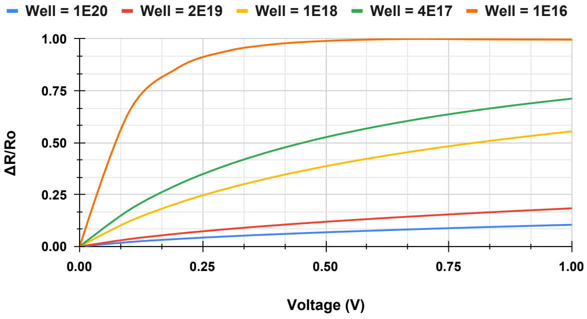


Fig. 5: Reflection simulation using Fresnel equations of a "$N^{+} - N$" junction with various doping concentrations of the N region ($N^{+} = 10^{21}$ for all cases) under various applied voltages.

Though OP measurements on a real transistor are different from the reflection simulation, as shown in [23], the simulation results of reflected light correctly show the trend and shape of the reflected light. It is worth mentioning that after changing the doping polarity, the bulk of a FET and the region under the GATE terminal act as a varactor [23]. This means that charges accumulate upon the applied voltage. Due to having a varactor, there exists a SCR, and a channel forms beneath the gate terminal. These two phenomena contribute to the modulation of incident light on a transistor.

IV. Performing LLSI on Layout

In this section we evaluate LATs under OP simulations. For this purpose, we use the LLSI technique and consider all regions that are modulated when V_{dd} is modulated. To facilitate the simulation of the reflected light for LLSI, we use equation (5) for each region of the transistors in the layout. The layout of each logic gate is drawn as polygon of active regions. Next, we convolve the cell's RCV (RCV_{Cell}) with the active region of the layout (M). The formulation of LLSI imaging can be summarized as follows:

$$LLSI_{image}[i,j] = \sum_{k=1}^{m}\sum_{l=1}^{n} M(i+k-1, j+l-1) RCV_{Cell}(k,l). \tag{8}$$

$$M_{(i,j)} = \begin{cases} 1 & \textit{if there is an active region at position } i \;\&\; j \\ 0 & \textit{otherwise} \end{cases} \tag{9}$$

For simplicity, we assumed the value for K and β for standard NMOS and PMOS to be 1 and 1.3 [23], [24], respectively. For stealthy dopant LATs, due to partially depleted SCRs, we took K and β for NMOS and PMOS to be 1 and 1.05, respectively. It is worth mentioning that this is just an assumption that we took to perform LLSI simulation analysis. For all our analyses we use a wavelength of $\lambda = 1.3\,\mu$m and an NA of 3.5.

A. Stealthy Dopant Level Trojan

Consider a modified AOI222 logic cell with stealthy dopant LAT, which is wired to function as a 3-input NOT-Majority logic cell [8], as shown in Fig. 6. In this logic cell, the topmost PMOS transistor's doping polarities are swapped (similar to Fig. 2). This dopant swapping causes these two transistors to be electrically connected to V_{dd}. For the rest of the PMOSes, the doping regions are shrunk to have a lower effective width.

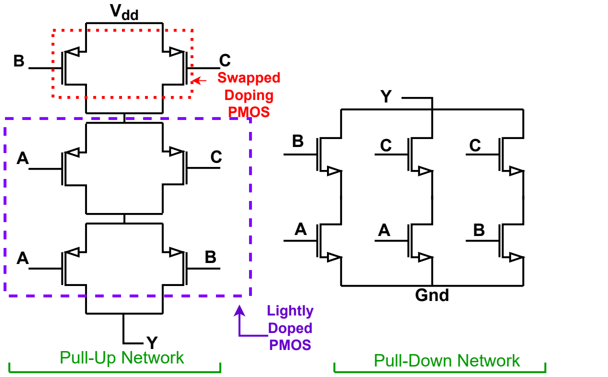
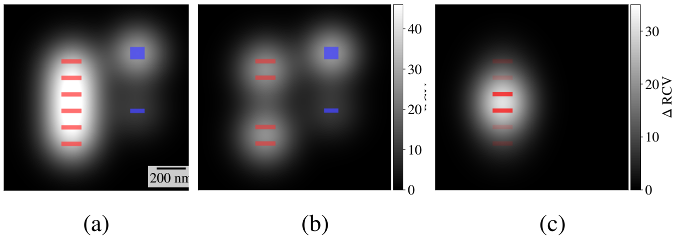


Fig. 6: Modified AOI222 logic cell which is wired up to function as 3-input NOT Majority logic cell.



(a) (b) (c)

Fig. 7: LLSI simulation images of AOI222 gate when all inputs are set to logic "0" with layout overlay (blue: NMOS, red: PMOS), λ = 1.3 µm, NA = 3.5 (SIL). (a) Standard AOI222 gate, (b) AOI222 with LAT, (c) Difference of (a) and (b).

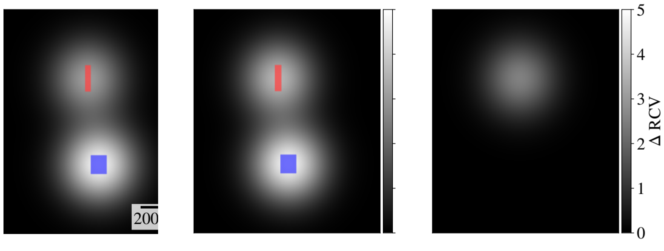
Lowering the effective width of transistors results in having a lower driving capability.

To see what the LLSI image of the malicious AOI222 logic cell with trojan looks like, we set all the input terminals to the logical value "0". Then, we performed the LLSI, and scanned the logic cell's active region using the laser. Figs. 7(a), 7(b), and 7(c) show the LLSI simulation of the unmodified AOI222 gate, the modified gate by changing the polarity of PMOS transistors' doping and shrinking the doped region of some PMOS transistors, and the difference between unmodified and modified LLSI images, respectively. It can be seen that LLSI simulation can reveal the insertion of the LAT in a logic cell. The difference is large as ΔRCV has a high intensity compared with the RCV values for the unmodified and modified gates.

B. Adding Trojan by Changing the Transistor's Length

To show how the LLSI image of a LAT that implements a slight modification in a transistor's length looks like, we use an INVERTER logic cell. For this INVERTER, we apply a logic value "0" as an input. Then we perform the LLSI simulation on an unmodified and a modified INVERTER cell, as shown in Fig. 8. The length of transistors is set to 28 nm in a standard INVERTER. For the modified INVERTER, the length of the PMOS is set to 32 nm while keeping the width of the transistors similar to the standard INVERTER's sizing.

According to equation (5), the RCV is proportional to the active area of a transistor. Consequently, an increase in the length of the transistor will cause in an increase in the RCV. The LLSI analysis of standard and modified INVERTER logic cell are shown in Fig. 8(a) and Fig. 8(b), respectively. From Fig. 8(c), it can be seen that LAT caused by a minimum allowable increase in the length of a transistor (in a 28nm



(a) (b) (c)

Fig. 8: LLSI simulation images of an INVERTER gate when its input is set to logic “0” with layout overlay (blue: NMOS, red: PMOS), λ = 1.3 µm, NA = 3.5 (SIL). (a) Standard INVERTER gate, (b) INVERTER with LAT, (c) Difference.

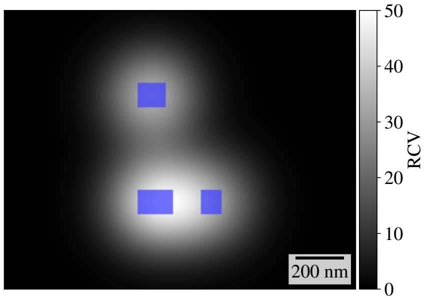


Fig. 9: A2 LAT under LLSI simulation with layout overlay, λ = 1.3 µm, NA = 3.5 (SIL).

technology) will appear in the LLSI images, just by taking the difference between images of the unmodified and LAT-infused logic cells. However, compared to the previous experiment, ΔRCV is rather low, meaning that the detection on a real device might be more challenging.

C. A2 Capacitive Trojan

Since an A2 LAT (shown in Fig. 1) is an extra circuitry added to the circuit, performing LLSI leads to the modulation of capacitances upon having a small charge on them. This means that the charge and the SCR underneath the channel of MOSFETs get modulated due to modulation in the power rail. As a result, the A2 as a capacitive LAT will show up during LLSI analysis, as shown in Fig. 9. It must be mentioned that this capacitive LAT is stealthy, and it is impossible to be detected using conventional HT detection methods. However, since A2 adds an extra circuitry, an extra pattern will be detected upon comparing the LLSI images of a LAT-free and LAT-inserted layout.

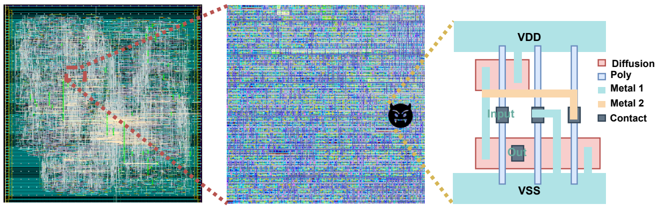
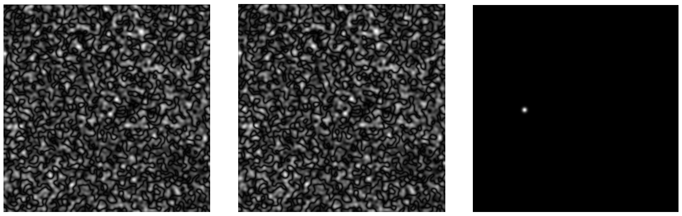


Fig. 10: A2 inserted into RV32IM core.



(a) (b) (c)

Fig. 11: LLSI simulation on RV32IM core. (a) RV32IM core's golden layout, (b) Infected layout, (c) Difference.

D. LAT Insertion in a RISC-V Core

As a show case of the LAT detection in a real case scenario, we inserted an A2 LAT into the layout of an in-house designed single-cycle RISC-V core's ALU (RV32IM), as shown in Fig. 10. Note that the RV32IM core is designed using a commercial 28 nm technology. Next, we applied a random input value to the RV32IM core and performed LLSI analysis on the layout (ALU and register bank). We are able to detect the existence of the LAT by comparing the LLSI simulation images of the LAT-free layout (golden layout), as shown in Fig. 11a, and the LAT-inserted layout, as shown in Fig. 11b. The difference between the two images is shown in Fig. 11c and illustrates that we can expose the LAT.

V. Integration and Discussion

In this section, we first explain how we can acquire RCV values for each transistor to load it into the golden layout model and then perform LLSI analysis. We also discuss a solution for potential limitations of the LLSI technique to detect LATs, namely analysis time and Process Variation (PV).

A. Obtaining Optical Reflection Properties for LLSI Simulations on the Golden Layout

In this work, we assumed that we know the RCVs of transistors under LLSI analysis. These values are the prerequisite for comparing the simulations on a golden layout with the measurements on the physical chip. Two possible approaches can be taken to acquire such information. First, one could ask the foundry to provide the fabrication parameters under the NDA. Based on the fabrication parameters of the transistors, the refraction and absorption of laser light passing through the semiconductor can be calculated [23]. Second, one could create a chip with single transistors of various sizes on it, and then perform LLSI measurements. Then, by loading the acquired values from a real test chip, we can perform LLSI in simulation. Both mentioned methods are not practical. For the first method, if a foundry is untrusted, the provided information from them can be assumed to be untrustworthy, or a foundry can refuse to provide such sensitive information to the customers. For the second method, fabricating a chip with single transistor structures is costly thus not practical for every design. However, this approach can be justified if a design house would like to use a specific technology node for multiple chips.

The more practical approach would be to distribute single transistors of various sizes around the chip when a design is sent for fabrication (or in empty spaces of the design by removing the filler cells), as shown in Fig. 12. After the chip is sent back to the design house, these distributed structures can be used as reference structures to retrieve the OP reflection of each transistor after performing OP analysis

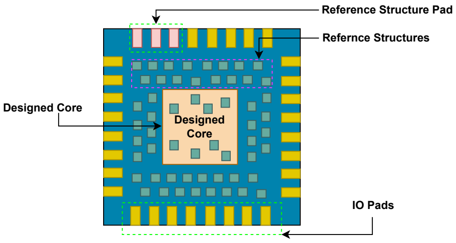


Fig. 12: Distribution of reference structures around the chip to retrieve reflection values under LLSI.

on the chip. Consequently, these reference reflection values from the reference structures can be used for LLSI simulations on the golden layout. It might also be possible to use the existing transistors in the design to retrieve the reflection values. This would require more effort and experiments to collect the reflection values of devices under LLSI.

B. Process Variation Effects on LLSI

A semiconductor's optical reflection depends on the transistors' fabrication parameters (e.g., doping and size), as investigated in [23], [24]. Therefore, PV can be considered as a potential limitation to our LLSI-based LAT detection method. Nonetheless, we can use the idea of placing some reference structures around the chip, as shown in Fig. 12, to have reference values for optical probing around the chip, to include the effect of PV in the reflected light from the transistors in various regions of the design. In other words, these reference structures will include the PV in OP reflection of transistors in those regions. Then, we can load this collection of reflection values to our golden layout simulator to decrease the false-negative detection when we compare the LLSI analysis of the fabricated chip and golden layout.

An important point to note is that, after a fabrication process, a fabricated chip is tested extensively for functional accuracy and PV detection. We assume that our fabricated chip has passed functional testing. Hence, the collected reflection values are from a functional chip.

C. Time as a Potential Limitation to LLSI Detection

In this work, we performed the LLSI analysis on the golden and modified layouts in simulation, as explained in section IV. However, in a real-world scenario, performing LLSI is time-consuming and requires hours to days, depending on the area of interest. The reason for that is the relatively low SNR due to the small modulated signal of 100 mV at 100 kHz on the transistor regions. It is possible to improve the timing of LLSI by increasing the steps that the laser moves over the chip, staying on each spot for a shorter time (i.e., decreasing the SNR of the overall image). There is a need to find an optimal point for good image SNR and LLSI analysis time. Another approach to decrease the required time for LLSI measurements is to limit the analysis to the most susceptible areas for LAT insertion, for example, crypto cores [16]. Nevertheless, the required time for such a critical analysis, which is performed offline, is reasonable and acceptable [15], [17].

VI. Conclusion and Future Work

In this work, we proposed a novel analytical approach to detect LATs – extremely stealthy HTs that can be inserted into a chip during the fabrication process. Our approach takes advantage of the LLSI technique. We first derived the necessary calculations for simulating LLSI and showed that it should be possible to detect LATs using LLSI. Then, we simulated the LLSI images of unmodified and modified logic gates. We showed that the images of modified and unmodified logic gates differ significantly under the existence of LATs. To show the applicability of our LAT detection scheme, we inserted a LAT into a RISC-V core, and then demonstrated the effectiveness of our detection scheme using LLSI simulations. For our future work, we will tape-out the discussed LATs in this work to perform LLSI analysis on a real chip with LATs. This will improve our LLSI simulator for a real technology and test the applicability of LAT detection using our non-invasive OP-based method.

Acknowledgment

The work described in this paper has been supported by the Deutsche Forschungsgemeinschaft (DFG – German Research Foundation) under the priority programme SPP 2253 – 439918011 in project DR 287/38-1, and in part by National Science Foundation (NSF) under the grant number 2150123.

References

[1] S. Parvin, M. Goli, F. Sill Torres, and R. Drechsler, "Trojan-D2: Post-layout design and detection of stealthy hardware trojans-a RISC-V case study," *ASP-DAC*, 2023.

[2] V. R. Surabhi and et al., "Hardware trojan detection using controlled circuit aging," *IEEE Access*, 2020.

[3] T.-T. Hoang, T.-H. Tran, V.-P. Hoang, X.-N. Tran, and C.-K. Pham, "Hardware trojan detection techniques using side-channel analysis," in *NICS*, 2019.

[4] O. Söll, T. Korak, M. Muehlberghuber, and M. Hutter, "Em-based detection of hardware trojans on fpgas," in *IEEE HOST*, 2014.

[5] S. Narasimhan and et al., "Hardware trojan detection by multiple-parameter side-channel analysis," *IEEE TC*, 2013.

[6] J. Aarestad, D. Acharyya, R. Rad, and J. Plusquellic, "Detecting trojans through leakage current analysis using multiple supply pad I_{ddq}s," 2010.

[7] K. Yang, M. Hicks, Q. Dong, T. Austin, and D. Sylvester, "A2: Analog Malicious Hardware," in *IEEE SP*, 2016.

[8] G. T. Becker, F. Regazzoni, C. Paar, and W. P. Burleson, "Stealthy dopant-level hardware Trojans: Extended version," *JCE*, 2014.

[9] T. Sugawara and et. al, "Reversing stealthy dopant-level circuits," in *CHES*, 2014.

[10] T. Krachenfels, J. Seifert, and S. Tajik, "Trojan awakener: Detecting dormant malicious hardware using laser logic state imaging," *CoRR*, 2021.

[11] A. Stern, D. Mehta, S. Tajik, F. Farahmandi, and M. Tehranipoor, "Sparta: A laser probing approach for trojan detection," in *ITC*, 2020.

[12] S. Bandara, A. Ehret, D. Kava, and M. A. Kinsy, "BRISC-V: an open-source architecture design space exploration toolbox," *CoRR*, 2019.

[13] R. Soref and B. Bennett, "Electrooptical effects in silicon," *IEEE JQE*, 1987.

[14] 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," *IEEE TDMR*, 2007.

[15] H. Lohrke, S. Tajik, C. Boit, and J.-P. Seifert, "No place to hide: Contactless probing of secret data on fpgas," in *CHES*, 2016.

[16] S. Tajik, H. Lohrke, J.-P. Seifert, and C. Boit, "On the power of optical contactless probing: Attacking bitstream encryption of fpgas," 2017.

[17] M. T. Rahman, S. Tajik, M. S. Rahman, M. Tehranipoor, and N. Asadizanjani, "The key is left under the mat: On the inappropriate security assumption of logic locking schemes," 2020.

[18] T. Krachenfels, F. Ganji, A. Moradi, S. Tajik, and J.-P. Seifert, "Real-world snapshots vs. theory: Questioning the t-probing security model," in *IEEE SP*, 2021.

[19] 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 *USENIX*, 2021.

[20] V. Ravikumar, G. Lim, J. Chin, K. Pey, and J. Yang, "Understanding spatial resolution of laser voltage imaging," *Microelectronics Reliability*, 2018.

[21] C. Boit and et al., "Contactless visible light probing for nanoscale ics through 10 um bulk silicon." INT, 2015.

[22] M. von Haartman and et. al., "Optical Fault Isolation and Nanoprobing Techniques for the 10 nm Technology Node and Beyond," 2015.

[23] U. Kindereit, "Investigation of laser-beam modulations induced by the operation of electronic devices," Doctoral Thesis, Technische Universität Berlin, Fakultät IV - Elektrotechnik und Informatik, 2009.

[24] S. Parvin and et al, "Toward optical probing resistant circuits: A comparison of logic styles and circuit design techniques," in *ASP-DAC*, 2022.

[25] V. Benda, D. A. Grant, and J. Gowar, *Discrete and Integrated Power Semiconductor Devices: Theory and Applications*. John Wiley & Sons, Ltd, 1999.