IACR Transactions on Cryptographic Hardware and Embedded Systems
ISSN 2569-2925, Vol. 2024, No. 4, pp. 541–568. DOI:10.46586/tches.v2024.i4.541-568

Through the Looking-Glass: Sensitive Data Extraction by Optical Probing of Scan Chains

Tuba Kiyan[1], Lars Renkes[1], Marvin Sass[1], Antonio Saavedra[1], Norbert Herfurth[2], Elham Amini[1] and Jean-Pierre Seifert[1]

[1] Technische Universität Berlin, Berlin, Germany, {firstname.lastname}@tu-berlin.de
[2] IHP - Leibniz-Institut für innovative Mikroelektronik, Frankfurt (Oder), Germany, herfurth@ihp-microelectronics.com

Abstract. There is an imminent trade-off between an Integrated Circuit (IC)'s testability and its physical security. While Design for Test (DfT) techniques, such as scan chains make the circuit's physical behavior at runtime observable and easy to control, these techniques form a lucrative class of attack vectors with the potential to compromise the entire security architecture of the Device under Test (DuT). Moreover, with the rapid development of more complex technologies, the need for integration of DfT techniques even intensifies due to the requirement for faster time-to-market of cutting-edge ICs. In this work, we demonstrate that sensitive data can be extracted from the registers once their locations on the chip are identified by exploiting DfT structures and optically probing them — in this case, scan chains, even after the access to test mode is restricted. Furthermore, we show that also an obfuscated scan chain architecture can be fully reconstructed by using tools and techniques encountered in the Failure Analysis (FA) domain.

Keywords: Hardware attacks · Design for Testing · Scan chains · Optical Probing

1 Introduction

In terms of competition, there is no second match for the semiconductor industry. In a world where competition between chip manufacturers heats up on a daily basis and a reduction in innovation implies high financial damage, the cost and time spent in production are of *significant* importance. Following the manufacturing process, the produced chips undergo packaging and testing to identify and segregate any non-functional units. This step is known as the "back-end" process and can be done either by the foundry itself or by Outsourced Semiconductor Assembly & Test (OSAT) companies. The economic dynamics of back-end manufacturing have driven a growing trend of outsourcing to China, Taiwan, and other countries in Southeast Asia [Ruh22]. As an example, AMD processors are designed by AMD, produced in TSMC's fabs, and then packaged and tested by OSAT company SPIL, both in Taiwan [KB20]. Moreover, OSAT companies have experienced significant growth in recent years. Their market expanded from $17 billion in 2009 to surpass $30 billion by 2019. Hence, Intellectual Property (IP) piracy during testing has been a growing concern due to the globalization of IC production and outsourcing [RKK14, BT18].

The post-production testing determines the yield of a batch of ICs, thus representing a major criterion affecting the total cost of manufacturing for semiconductor suppliers. This highlights the importance of DfT strategies, as they increase the observability and controllability of any DuT and thus drastically decrease the time spent on testing. If

Received: 2024-04-15 Accepted: 2024-06-15 Published: 2024-09-05

we consider the complexity of modern System-On-Chips (SOCs), the integration of DfT techniques is inevitable. Once a non-functional chip is detected by post-silicon testing techniques, FA methods can be used to narrow down the cause of the failure. Optical probing and laser stimulation have been very effective FA methods that have also been used in conjunction with DfT techniques to dissect the broken point of failure [KBB08, GPY+12, LCP+17, SDB+18].

The main representative of the class of DfT techniques are so-called scan chains, which are based on the reuse of existing logic. Scan chains enable access to the critical nodes deeply buried inside the IC as well as introduce a possibility to create snapshots of an IC's state at a given clock cycle. From a security point-of-view, however, this kind of DfT technique must be considered the most critical. At the downside of DfT techniques, these have the potential to form a back door in several ways. As an example, an adversary may abuse the scan chains to reverse engineer logic components, extract sensitive information, and steal a company's design IPs.

Previous research has shown that scan chain-based attacks can be used to target, e.g., cryptographic chips. In these so-called differential attacks, the adversary commonly operates the device in normal mode until a (partial) secret is loaded at runtime. Once the sensitive information is assumed to be available in the device's computational path, the operating mode is switched to test mode in order to shift out the test pattern. By repeating the switch between modes multiple times, various hardware implementations have been attacked. As examples, devices with various encryption standards, such as the Data Encryption Standard (DES), Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), Elliptic Curve Cryptography (ECC), NTRUEncrypt, and stream ciphers based on Linear Feedback Shift Registers (LFSR), have been attacked by exploiting the scan chain architecture [YWK04, YWK06, NSY+10, RNFR13, KY12, LWK11]. Even more critical than that, the information gained via scan chain architecture has shown to have the potential to be processed automatically in order to non-invasively reverse engineer and disclose a company's design IP. As an example a hardware implementation of AES has successfully been reconstructed, as highlighted in a study by Azriel et al [AGM17]. However, previous works on scan-based attacks targeting cryptographic chips assume that there is no protection mechanism that locks the scan path and that the transition between test and normal mode is not restricted.

To counter the aforementioned scan chain-based attack vectors, access to the test infrastructure might be physically disabled by blowing the fuses at either side of the scan path after testing has taken place [RAWT96]. By fusing out the scan chain signals, the internal scan chain logic remains fully functional, despite the fact that it cannot be accessed or activated anymore. However, completely deactivating the test mode is not a widely adopted practice due to potential consequences for on-site debugging and maintenance [LWN+22]. Although scan access can be restricted to prevent unauthorized access, for example, by detecting test access and withdrawing the test keys [LKK+21].

Apart from restricting the access to the scan architecture another type of countermeasure is resetting the Scan Flip-Flops (SFFs) content while switching between test mode and normal operation to avoid data leakage. However, it has been shown that test mode-only attacks are still feasible to squeeze out the sensitive information [SASK14]. Furthermore, advanced industrial application techniques like scan compression, masking, or dynamic scrambling of SFFs have shown to be broken [SASK14, DRDNFR12]. Another technique is referred to as logic locking which has been extensively researched in the last two decades [RKM08, KAFT22, YSN+17]. A locked scan chain obfuscates the scan chain's data in order to hide the chip's functionality during the testing phase. However, even when confronted with a locked scan chain, the adversary may still try to apply SAT attacks [SRM15], namely ScanSAT attack [AYS+19]. It reconstructs the correct key from an obfuscated design by modeling it as a boolean satisfiability problem and using heuristic-based algorithms to

reduce the key search space and solve it.

Powerful attacks on obfuscated scan chains as well as ScanSAT attack, require two pieces of information to retrieve the correct key [RPSK12]: 1) the locked netlist and 2) a functional IC with the embedded secret key with full scan access (oracle). The netlist of a chip can be obtained either by a malicious actor in the foundry or by reverse engineering techniques. The malicious actor at the foundry already possesses the GDSII file which can be converted into a gate-level netlist. Alternatively, the attacker can go through a time-consuming and expensive reverse engineering process, which requires a lot of expertise and sophisticated FA tools. Nonetheless, recent work has been shown to prevent oracle-based attacks by adding circuitry that detects test access in oracles and corrupts the chip's functionality [LKK+21].

Our Contributions. In this work, we leverage optical probing attacks and demonstrate that once the locations of target SFFs are identified, sensitive data can be extracted while the device is operating in normal mode.
In more detail, our contributions are as follows:

1. We introduce and describe our Tester design to be used on Field Programmable Gate Array (FPGA) to precisely interact with a scan chain, as to the best of our knowledge, no open source design exists.

2. We propose the use of scan chain side-channel for reverse engineering the physical position of target registers. Our approach distinguishes itself by not requiring a design netlist or GDSII file, setting it apart from most attacks documented in the literature.

3. We perform novel optical side-channel attacks based on Electro Optical Probing (EOP) and Electro Optical Frequency Mapping (EOFM) against SFFs to break locked scan chain obfuscation for the first time in literature.

4. Finally, we showcase the extraction of data from target SFFs in normal mode.

Unlike FA engineers, attackers typically lack access to the netlist, design schematic, or layout of the DuT in most attack scenarios. Consequently, parts of the chip have to be first reverse-engineered to detect the registers holding the secret data before they get optically probed. Due to the increased complexity and larger physical dimensions of modern ICs, the time and resources required to identify specific registers within the chip are substantial, particularly for Application Specific Integrated Circuits (ASICs). ASICs consist of various blocks dedicated to individual sub-functions and synthesized logic areas, resulting in a more irregular structure compared to FPGAs, CLBs or memories. Attackers may attempt to employ optical probing techniques for reverse engineering the registers. However, knowledge of the switching frequency of the transistors is necessary to conduct these types of attacks. Despite having this information, more logic blocks are identified than necessary. Moreover, for EOFM there exists a minimum switching frequency threshold for the transistors to be detectable that is technology-dependent. Registers that are active for only a short duration, have slow frequency or do not switch periodically are more challenging to locate. In such scenarios, attackers must devise solutions. For instance, in [KGM+21], the authors combine obtained LLSI snapshots with a SAT solver to identify unknown register locations, which requires having access to the netlist. In contrast, scan chain access provides full control over clock frequency and the scan data input, offering a great capability by simplifying tedious reverse engineering task by decreasing the search space for the target registers. For instance, scan chain can be exploited to differentiate between sequential and combinational logic. The complexity of finding the unknown register locations is elaborated more in detail in Subsection 9.3.

The remainder of this paper is structured as follows: In Section 2, we present the necessary background information to facilitate a comprehensive understanding of this

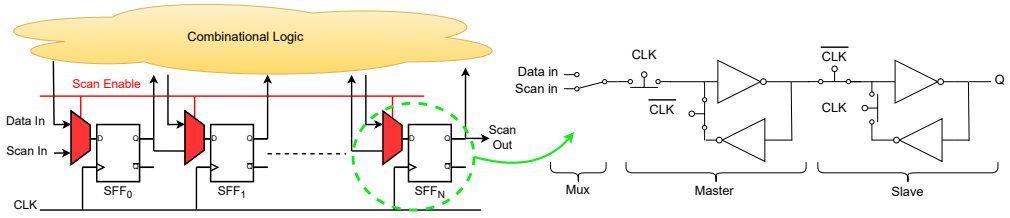


Figure 1: A scan chain consists of a certain number of SFFs which are interconnected to form a long shift register. The length of the scan chain is equal to the number of SFFs. Each SFF is preceded by a Multiplexer (MUX) which selects one of two inputs to the D-Flip-Flop (DFF). The DFF itself consists of a master and a slave stage.

study. We then briefly discuss the threat model in Section 3, setting the foundation for our novel attack approach, which is detailed in Section 4. In Section 5 and Section 6 we define the specific targets and outline the optical attack setup, respectively. To validate our attack approach, we introduce the verification methodology outlined in Section 7 which is employed to obtain the results presented in Section 8. Finally, in Section 9, we discuss the efficiency of our attack approach when faced with state-of-the-art countermeasures, as well as its performance for more complex devices in smaller technology nodes.

2 Background

2.1 Scan Chain Basics

DFT is a widely adopted industry practice, particularly in large-scale digital circuits and SoC designs where direct inputs and outputs offer limited insight into the internal logic operations. The combination of scan chains and automatic test pattern generation (ATPG) is extensively utilized due to its ability to achieve high fault coverage, low design costs, ease of implementation, and rapid testing speeds. Furthermore, commercial Electronic Design Automation (EDA) tools, such as DFT Compiler and Encounter DFT Architect, have been developed to automate the scan chain insertion process [Jin14, BT18].

A scan chain should not be confused with a boundary scan. While both techniques are crucial for ensuring the reliability and functionality of devices, they operate at different levels of the design and testing process. Boundary scan addresses the interconnections on a printed circuit board (PCB), and focuses on controlling the IO pins to allow testing interconnects between chips on a PCB. This technique is standardized by the IEEE 1149.1 Joint Test Action Group (JTAG) protocol. In contrast, such a standard does not exist for scan tests, and they focus on the internal logic of ICs, facilitating internal diagnostics and fault detection.

A scan chain consists of a configurable shift register, used in testing to control and observe the internal nodes of a chip by utilizing a minimal amount of external pins [WA73]. It can be either driven indirectly via JTAG interface or directly by the primary input and output pins. The scan chain does not only test the functionality of the sequential logic but also the combinational logic in between them.

In scan design, standard flip-flops in the circuit are replaced with SFFs. A single SFF is commonly implemented by preceding an existing DFF with a multiplexer which forwards different inputs depending on the mode of operation: test mode or normal mode. A simple scan chain structure is depicted in Figure 1. Here it is illustrated that regular DFFs are converted into SFFs by preceding a MUX, which selects between `Data In` and `Scan In` based on the `Scan Enable` signal. If test mode is activated, i.e., the Scan Enable signal is asserted high, the SFFs form a shift-register, defined as the scan chain. However, the

Table 1: The truth table of an SFF depicting its operation. (SE is Scan Enable, SI is Scan chain input in test mode, D is data input coming from the combinational logic in normal mode, CLK is the scan clock and Q is the output of the SFF).

SE	SI	D	CLK	Q	$\overline{Q}$
0	X	0	Rising Edge	0	1
0	X	1	Rising Edge	1	0
1	0	X	Rising Edge	0	1
1	1	X	Rising Edge	1	0
X	X	X	0	Last Q	Last $\overline{Q}$
X	X	X	1	Last Q	Last $\overline{Q}$

internal storage element of the SFF is still represented by an edge-triggered sequential DFF, which generally consists of a master and a slave stage. The complementary operation of these two stages ensures that the SFF is triggered at the rising edge of the clock. The truth table of a SFF is presented in Table 1.

The scan chain testing process can be summarized in three key steps:

1. Loading Known States: In the test mode, a known state is loaded into the scan chain by shifting the test pattern through the shift register. This step is quick and efficient, requiring significantly fewer clock cycles compared to traditional functional testing.

2. Operational Testing: Once the known state is loaded, the device switches to normal operational mode for one or two clock cycles. During this phase, the circuit processes the loaded state as it would during regular operation.

3. Shifting Out Patterns: After the operational testing phase, the device switches back to test mode. The resulting states are then shifted out through the scan chain for analysis. This back-and-forth switching ensures that both the loading of test states and the observation of resulting states are efficiently managed.

This method not only enhances test coverage but also dramatically reduces testing time, addressing key challenges in the testing process. The challenge of conventional functional testing is that setting the device to a known state is often a complex and time-consuming task. This process requires numerous clock cycles to manipulate the circuit into the desired state, which can be highly inefficient, especially for large-scale digital circuits and SoC designs. The limited ability to control and observe the internal logic states during functional testing further complicates achieving comprehensive test coverage. Scan chain testing overcomes these challenges by introducing a streamlined and efficient method for testing ICs, which significantly simplifies the process of setting known states and observing internal logic. During the test mode, configuring a serial shift register allows for a known state to be easily loaded into the registers through the scan path. Shifting the input vector through the scan path coerces linear complexity w.r.t. the length of the scan chain's architecture. Doing so drastically increases the throughput of test cases at a post-silicon testing stage.

In most modern ICs, test compression design technique is now extensively utilized in the semiconductor industry instead of using one single long scan chain with millions of SFFs [LH07, DEG+13]. It further reduces test data volume, test time and therefore test cost. Here, instead of a single scan chain, multiple scan chains are implemented in parallel with two new components added: a decompressor and a compactor. The decompressor takes a stimulus from one or a small number of `Scan In` pins and feeds a large number of scan chains. Similarly, the compactor takes the responses of all scan chains and compacts

them to a few or a single output. Figure 2 shows a compressed scan architecture with m scan chains, each of length n.

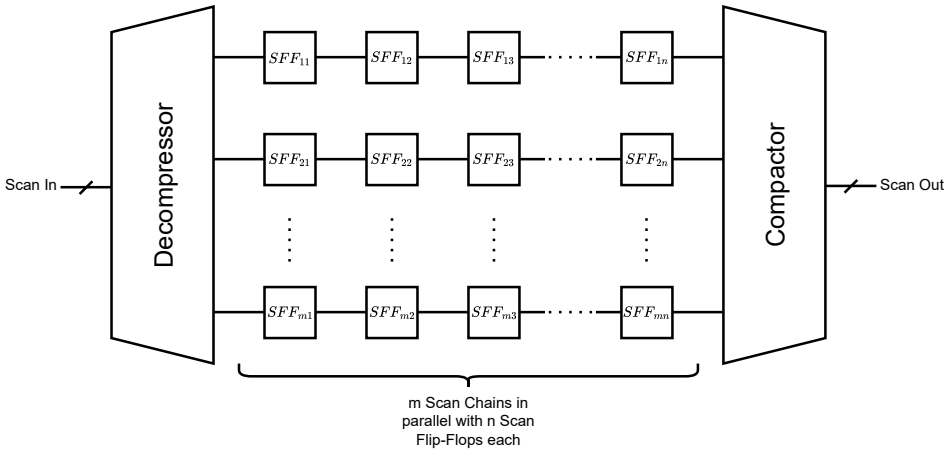


Figure 2: Scan compression architecture with m scan chains, each of length n

2.2 Scan Chain Obfuscation

Logic locking has attracted significant interest, resulting in extensive research over the past two decades. This has led to the development of a wide range of logic-locking techniques in both academia [RKM08, KAFT22, YSN+17] and the semiconductor industry. For instance, Mentor Graphics introduced the TrustChain framework, aimed at supporting logic locking and camouflaging capabilities in their CAD tools [Lee17]. Scan chain locking, in particular, aims to ensure the safety of the outsourced testing process by obfuscating the circuit's design and by this, protecting against a malicious actor in the manufacturing foundry or tester company. In scan chain-locking the obfuscation of the scan path is achieved by inserting a specific amount of key gates in between the SFFs. The corresponding key bits to the gates are assumed to be stored inside tamper-proof memory. The key gates inserted between the SFFs transform the `Scan In` and `Scan Out` data, such that the input and output pattern differs from the actual pattern, thereby concealing the functionality of the IC. The design house provides the outsourced testing company transformed test pattern which avoids revealing the real functionality of the device. After the testing is completed, the tested chips are returned to the design house where they are unlocked by using the correct key.

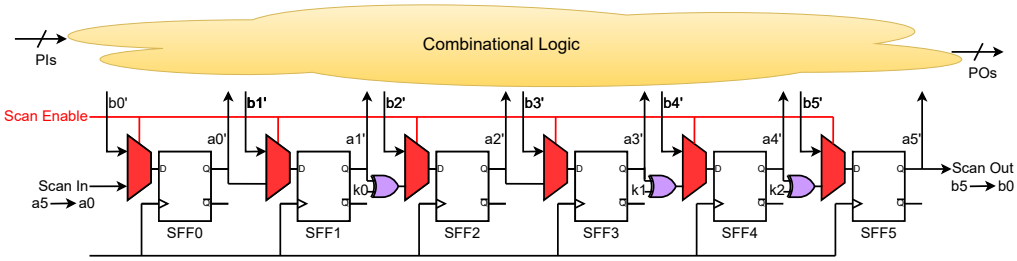


Figure 3: Implementation of an obfuscated scan chain (s386 benchmark). Three `XOR` gates with key bits are used for obfuscation

To address the risks associated with scan chain-based attacks, various secure scan designs have been suggested. While some of these methods restrict access to the scan chain [LKK+21], others use obfuscation. Different configurations are employed in the literature to obscure the scan path. They employ logic primitives such as MUXs [KCK18], latches [ASYT12], XOR-Gates [RKM08], dummy flip-flops [LTP06], or inverters [SMC07] to counteract scan chain based attacks.

By exploiting the side-channel opened by scan chains, an attacker can retrieve security-critical information and break locked circuits that aim to prevent IP theft of a locked design. If the secret key is updated periodically, it is referred to as dynamic scan obfuscation [KCK20, KKC21]. If it remains constant, the obfuscation is classified as being static instead [KCK18]. The investigated scan chain consists of six scan flip-flops that are locked with three XOR gates and three key bits as illustrated in Figure 3. However, we discuss the efficiency of our technique in Section 9 when state-of-the-art countermeasures are integrated into the target DuT.

2.3 In-Circuit Test Systems

In-Circuit Test Systems, also known as Testers, are expensive machines used by semiconductor fabrication plants as well as testing companies to quickly and fully automatically test the functionality of a set of ICs[1]. Given a specific batch of logically equivalent ICs, the tester is provided a vast amount of test cases, where each test case is represented as a pair of input and output scan patterns. During operation, the tester then shifts in the test input pattern, operates the DuT for a single clock cycle in normal mode and shifts out the corresponding test output pattern in a fully automated fashion. If a test case fails, such when an expected output pattern is not equal to the actual output pattern, the IC will be marked non-functional. Afterwards, further failure analysis might be employed in order to determine the cause of the test case failure.

2.4 Optical Probing

Optical techniques that are known from FA domain are widely adapted to assess the vulnerabilities of ICs for security reasons. They offer significant advantages over other side-channel methods in terms of signal tracking and data extraction from the chips. For instance, power analysis side-channel techniques leverage power consumption to extract confidential data from registers. However, they are assumed to leak Hamming weight rather than exact data. Additionally, power consumption traces are susceptible to noise. In the context of masked implementations, using a sufficiently large number of shares can mitigate power analysis attacks, especially in the presence of noise. On the other hand, in [KGM+21], the authors demonstrate that LLSI can be successfully used to attack masking implementations.

Due to the stacking of several metal layers on the front side of ICs, fault isolation techniques commonly apply to the backside [BTS+16]. The increasing adoption of advanced packaging technologies, such as flip-chip, facilitates backside access to chips by simplifying the chip preparation process. Optical contactless fault isolation techniques, among other methods, have proven highly effective in precisely debugging faults from the backside. They exploit the fact that Silicon (Si) is transparent to near-infrared light. Nevertheless, it is crucial to acknowledge that the utilization of these techniques may inadvertently introduce potential security vulnerabilities. Given the extensive prevalence of these techniques in FA laboratories globally, related methods such as Photon Emission Microscopy (PEM) [NSSO12], Thermal Laser Stimulation (TLS) [LTK+18a], and optical probing [TLSB17] have been adopted to attack secure ICs. PEM localizes all the switching

[1] https://www.teradyne.com/semiconductor-testing/

transistors. If the switching frequency and the supply voltage level are high enough, the photon emission intensity of said transistors becomes substantial enough to manifest in the PEM measurements. However, the photon emission method lacks the capability to distinguish the paths switching with different frequencies. As an alternative optical technique, TLS requires low noise on the power line. Due to other operations on the IC, the current consumption of the device is highly fluctuating negatively influencing the TLS recording's Signal-to-Noise-Ratio (SNR).

Optical probing, on the other hand, offers exceptional capabilities over the other optical methods mentioned above in precisely tracking signals on the chip when the switching frequency of the target is known or can be estimated. It's essential to highlight that for EOFM to function optimally, the target frequency should be periodic, and the duty cycle needs to be set at 50%. Any deviation from this 50% mark will lead to a decrease in the SNR. Additionally, the signal frequency and supply voltage level should be high enough for an acceptable SNR that is specific to each technology node [SG19]. Optical probing uses three techniques based on the same phenomena: 1) EOFM is used to identify logic switching at a particular frequency, 2) EOP scopes the signal at a particular point on a transistor or cluster of transistors [KWT+07] and 3) Laser Logic State Imaging (LLSI), is used to extract logical states of the gates. As a result, EOFM and LLSI create two-dimensional maps of an area of interest while EOP recovers the signals similar to an oscilloscope of a single specific location. The underlying principle of optical probing is based on photon-semiconductor interaction. Si-based semiconductors are transparent to infrared light. The infrared light beam passes through the backside Si (also known as Bulk-Silicon), interacts with the active devices on the front side, and reflects back through the backside. The interaction with the Si modulates the reflected light beam depending on whether the exposed active device is on or off. On a physical level, the absorption and refraction index of Si is modified during optical probing due to the charge carrier density alteration during the transistors' switching activity, which in turn causes a change in the reflectivity of Si [SB87]. The weak modulation in the returned light is detected and converted into an electrical signal by a very sensitive light detector, which is capable of measuring photon count changes in the parts-per-million (ppm) range.

EOFM can be performed either in amplitude or phase mode. In amplitude mode, locations switching at a target frequency are gray-scale encoded w.r.t. the signals' strength. In phase mode, they are color-coded depending on the phase between the detected signal and an external reference signal fed into the tool. As a result, we can derive more information about the device's functionality in the phase mode. Because we acquire a 2D activity map at a target frequency as well as the detected signals' phase information. Phase mode is very helpful in reverse engineering a single SFF cell. Alternatively, one can distinguish between master and slave stages under the EOP prober, as the signal reaches the slave stage half a clock cycle later than the master stage.

LLSI represents an extension of EOFM, aimed at generating comprehensive 2-D maps determining logic states of the gates across specified areas [NKC+14]. During LLSI, the core voltage of the DuT undergoes modulation at a predetermined frequency, while the clock signal is halted. Subsequently, EOFM operations are executed at the specified modulation frequency, facilitating the capture of internal node signal snapshots for a desired clock cycle. LLSI proves particularly advantageous in scenarios where the switching frequencies of transistors remain undetermined. Modulating the supply voltage induces variations in the electric field within the transistor channels. Consequently, on-state transistors exhibit distinct signatures within the LLSI image, unlike their off-state counterparts. Leveraging this observation allows for the extraction of logical gate states [KLB18, KGM+21].

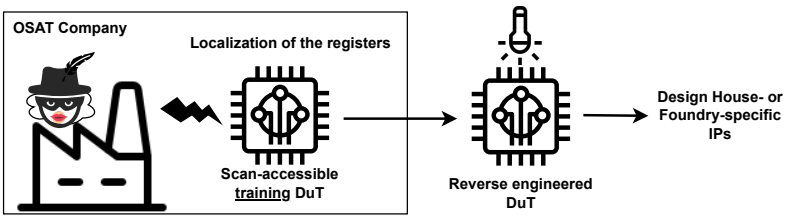


Figure 4: Threat model. The scan path of the training DuT is obfuscated during testing. Before the produced devices are distributed in the market, they are unlocked by entering the correct key.

3 Threat Model

The potential attacker is a malicious actor in an OSAT company who targets devices protected by restricting the scan access and by a scan chain-locking obfuscation. The threat model is illustrated in Figure 4. The attacker's motivation is to exploit the scan path, thereby compromising sensitive data such as design house's IPs. The utilization of scan chain side-channel facilitates the challenging task of reverse-engineering target registers. Locating registers through EOFM relies on knowledge of the switching frequency of transistors, a piece of information that may not be readily available or estimable in certain applications. Even if the switching frequency is known, more logic blocks will be visible and it will be hard to pinpoint the target registers among them. This becomes particularly daunting in modern chips containing billions of transistors, rendering reverse engineering a formidable task. However, the scan test mode presents an advantageous scenario for attackers. Here, the attackers have complete control over the scan chain clock and data input, creating an ideal setting for conducting optical probing attacks.

The emergence of a globalized, horizontal semiconductor business model also affected IC testing. There has been a consistent shift away from conducting IC testing in-house to outsourcing this process [RKK14, Pan21, Ruh22, KB20]. While numerous papers delve into methodologies for breaking encryption algorithms by scan chain side channel, the concern spans a broader spectrum. Leakage via scan path during testing poses a risk of compromising any kind of IP, such as reverse engineering the hardware implementation of an AES core crafted by the design house [AGM16]. In our attack scenario, we assume that the attacker aims to obtain company-specific assets such as design IPs. Furthermore, we assume that the scan chain access of the DuT is either restricted or even disabled post-testing before they are distributed in the market. It can be achieved, for instance, by blowing the fuses or corrupting the scan access. In this case, the attack has to be executed while the scan chain is still accessible. A malicious actor within a testing company already possesses access to the scan chain due to her involvement in the testing task. Furthermore, optical probing equipment is typically found in FA laboratories of manufacturing or testing companies. In cases where such equipment is not readily available, the necessary FA tools for conducting this specific analysis are available for rent at a rate of a few hundred euros per hour.

The attacker de-packages the DuT exposing its backside to facilitate the attack. By toggling between test and normal modes, she can decipher the semantics of the scan path, even if the scan chain is obfuscated. It is important to note that obfuscation does not impede the determination of the index of SFFs within the scan chain. Subsequently, she proceeds to the next step, she determines the spatial locations of the SFFs. She can then break the scan obfuscation. Such an attack has the potential to reverse engineer the device and compromise the security of a design house's IP to produce unauthorized copy of the design.

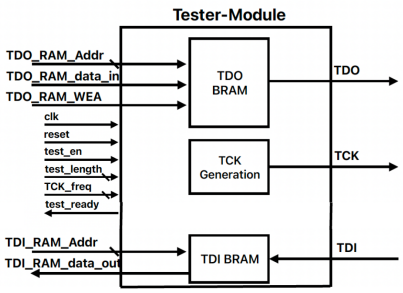


Figure 5: Block diagramm of our Tester HDL Design

Alternatively, since the necessary information about the chip is collected i.e. the locations of the critical SFFs on the device, the attacker is able to later launch attacks even on a scan-access-restricted device. After the testing is completed, the devices return to the design house, where they are activated with the correct keys to become functional and then they are distributed. With the all information gathered during the testing phase, she can now use optical probing to extract secure data from the DuT, even in normal mode, without relying on the scan chain test interface. These attacks could include secret information leakage residing inside the chip to compromise the security or privacy of the chips' users.

4 Attacker's Approach

Our attacker's approach is split into two parts. First, as testers come at very high costs we describe how we designed and implemented our own tester circuitry on FPGA. In the second part, we elaborate on how to use our tester design as well as methods originating from IC failure analysis, to mount a novel attack.

4.1 Tester Design

In order to be able to communicate with the scan chain in the most accurate manner, we had to develop the Tester first, as to the best of our knowledge no open-source design exists for such a purpose. In the following, we would like to elaborate on how we implement a tester on FPGA. The block diagram of our design is depicted in Figure 5. This shows that the tester consists of several sub-components: 1) Test Data Out (TDO) Block Random Access Memory (BRAM), 2) Test Data In (TDI) BRAM and 3) Test Clock (TCK) generation. The naming scheme is from the perspective of the FPGA platform, i.e TDO BRAM stores the IC's test input pattern and TDI BRAM stores the IC's test output pattern. Each BRAM instance exhibits a single read and a single write port. For TDO BRAM, the read port is used internally by the Tester to read the test input pattern, while the actual pattern is written externally, specifically via TDO-Signals. For TDI BRAM, the situation is reversed: the write port is internal to the Tester while the read port is external (i.e. via TDI-Signals).

By utilizing multiple BRAM instances we address multiple issues. For once, there manifests an issue with multiple clock domains when utilizing an internal clock as well as an additional scan clock (i.e. TCK). By using multiple BRAM instances, they act as buffers between the two domains. Moreover, DFFs represent a limited resource in FPGAs, which makes them unsuitable for implementing large memories. Scan chain lengths on the other hand can easily exceed multiple thousand SFFs in the real world. Hence, a straightforward FPGA implementation utilizing a vast amount of DFFs would result in non-implementable and inefficient logic.

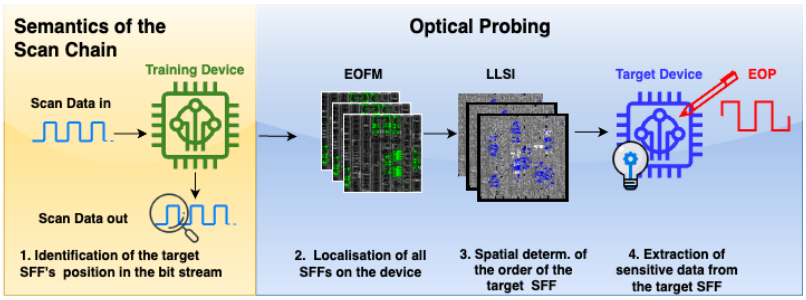


Figure 6: Attack approach

The TCK generation component takes care of generating a matching TCK signal, i.e. a synchronizing scan chain input signal, which exhibits a configurable, much slower frequency than the FPGA's clock itself. It is further worth noting that the TCK generation module generates a dynamic amount of clock cycles, which are determined by the `test_length` input of the Tester. By this, the test length can be configured. Once the TDO BRAM has been filled with a specific test input pattern, the `test_en` signal initiates shifting-in the test pattern into the scan chain while also recording the scan chains output and storing the results inside the TDI BRAM. After `test_en` has been asserted, `test_ready` goes low. Once `test_ready` is reasserted, the test has successfully been completed and the corresponding output pattern is stored within the TDI BRAM. Finally, the `TCK_freq` input determines the frequency of the TCK signal.

4.2 Novel Attack Design

By designing and implementing a Tester module on FPGA we gained the ability to control the scan chain. Proper interaction with the scan chain architecture opens the possibility for our novel attack design, which consists of several steps, i.e. 1) Determine the index of the SFFs of interest in the scan chain, 2) Localize the set of all the SFFs on the IC, 3) Localization of the SFFs which store information of interest, 4) Disclosing sensitive data from the SFF of interest. The attack approach is further depicted in Figure 6. In the following, we are going to elaborate on each of the aforementioned steps.

Determining the index of an SFF of interest inside the scan chain is the first challenging part. Here, the attacker does not know yet which SFFs on the chip holds the sensitive information, so she can analyze the scan chain's scan pattern to determine its index in the shift register. This step can be skipped when the location of the target SFF is known in advance to the adversary. By switching the DuT between normal mode and test mode, we are able to locate the SFFs of interest in the test pattern. For this, a series of measurements must be performed, similar to differential attacks. A single measurement always consists of the following points: 1) Reset the DuT into its initial State and operate it in normal mode in order to store a known byte into an unknown set of Flip-Flops. These Flip-Flops are assumed to be structured as SFFs as depicted in Figure 1. 2) Switch to test mode and shift out all the Scan-Bits (i.e. scan pattern) information. A test mode scan pattern is stored along with its normal mode input data.

After at least two measurements have taken place, the adversary is able to `XOR` two scan patterns as well as their corresponding data inputs. By this, changes in scan pattern are directly restated to a change in input data. Moreover, if an adversary is interested in reverse engineering the semantics of n bits of the scan chain, n inputs have to be chosen such that a single input uniquely determines the position of one bit of the scan pattern.

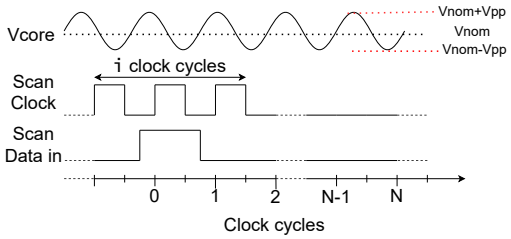


Figure 7: Input pattern for LLSI experiments, a logic high is fed into the scan-in and shifted through the scan chain for a defined number of clock cycles

The spatial localization of all SFFs is performed by utilizing EOFM. First, we alternate the scan chains data input line given at a specific frequency. The Scan-Clock signal is asserted to be twice that frequency, which results in an alternating input sampling inside the scan chain. Afterwards, EOFM is performed on both, the scan chain's input data as well as the scan chain's input clock frequency sequentially. To attain an adequate SNR, the chip needs to be operated in a loop to integrate captured signals over time, as the modulation in the reflected optical beam appeared to be very weak. By conducting EOFM on the scan chain clock frequency, we can localize all the SFFs as well as clock buffers. However, given their physical attributes, they become immediately distinguishable. When performing EOFM at the scan chain data input signal's frequency, the SFFs, as well as the combinational logic in between, can be localized. Finally, by subtracting both the previously mentioned measurements from each other, it is possible to localize the set of all the SFFs. Exemplary results are shown in Figure 10.

To determine the position of the target SFFs we use the LLSI technique. The identification based on LLSI works in four steps: 1) The core voltage is modulated with a sinusoidal signal 2) The scan chain is initialized such that every SFF holds a logic low. The clock is stopped and LLSI measurement is conducted. 3) The scan chain input is initialized with a single logic high signal, which propagates through the scan chain for a specified number of clock cycles, as shown in Figure 7. The number of the clock cycles should correspond to the index of the target SFF, ensuring that only the target SFF maintains a logic high state while the remaining hold a logic low state. Subsequently, the clock signal is halted, and another LLSI measurement is performed. 4) These two maps are subtracted. The resulting image reveals the location of the target SFF.

Disclosure of sensitive data directly follows from the previous steps. At this point, we know the semantics of a subset of SFFs we are interested in. We further reverse-engineered their positions by using LLSI. We can also now easily break the scan locking and finally disclose sensitive information in normal mode by using EOP. For EOP measurements, the laser beam is parked at a position of interest on the IC, where the electrical signal is recovered from the reflected optical signal. As an additional point, if the masking countermeasure is implemented, the LLSI method can be utilized instead of EOP to read out the register states. Unlike EOP, LLSI does not require repeated measurements with identical data. Therefore, the inherent randomness in masking schemes doesn't offer any protective effect.

5 Target Devices

We chose two different DuTs manufactured in different technology sizes. The first one being an Application Specific Integrated Circuit (ASIC) implementation while the second

one is an FPGA on which an obfuscated scan chain is implemented.

5.1 IHP UlpiSPI Chip

The first DuT represents a USB-to-SPI bridge ASIC provided by Innovations for High Performance Microelectronics (IHP). It is manufactured in 0.25μm Complementary Metal-Oxide-Semiconductor (CMOS) technology and it operates at a core voltage of 2.5V. This IC is operating as a SPI master which can serve 8 SPI slaves, connecting them to any computer via USB. It contains a scan chain consisting of 2100 SFFs spread over the whole die area without any further protection against hardware-based attacks. On this DuT there exist four scan chain related pins, which are 1) `scan enable`, 2) `scan mode`, 3) `scan in` and 4) `scan out`. When `scan enable` and `scan mode` pins are asserted, the SFFs enter the scan test mode and stitch together to form a single large shift register. The input of the shift register is represented by `scan in`, whereas the output of the shift register can be observed at `scan out`. To gain access to the backside of the IC the plastic package was opened. The backside silicon (bulk silicon) thickness was measured to be approx. 300μm. The DuT did not require any thinning of the bulk silicon for mounting the attacks.

Since the UlpiSPI IC does not incorporate any scan chain obfuscation and its scan path is accessible, we use it as a Proof-of-Concept (POC) to showcase the practical potential of our approach.

5.2 Intel Cyclone IV

The Cyclone IV FPGA is manufactured in a 60nm technology and it has a 144-pin TQFP package. It contains 6272 Logic Array Blocks (LABs), each one consisting of 16 Logic Elements (LEs). Each LE includes a 4-input Lookup-Table (LUT) and a single register cell. The nominal core voltage level is 1.2V. In order to gain access to the chip's backside, the package of the FPGA was opened and the prepared samples were soldered in an inverted fashion onto a custom-printed circuit board (PCB). We have chosen Cyclone IV FPGA to demonstrate the success of our attack approach in breaking scan chain obfuscation. We implemented a scan chain on Cyclone IV, consisting of six SFFs with an additional scan chain-locking scheme. We used three `XOR` gates to obfuscate the scan chain data as illustrated in Figure 3. One input to the `XOR` gate is the key bit and the other input is connected to the previous SFF's output.

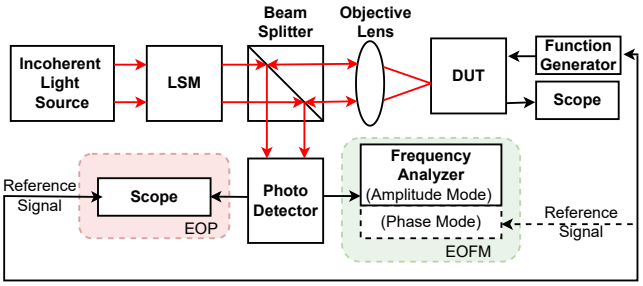
We have chosen Cyclone IV to evaluate the success of our approach on a locked scan chain.

6 Experimental Setup

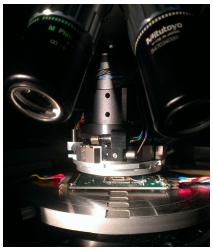
We used the PHEMOS 1000 Failure Analysis tool by Hamamatsu Photonics[2] to perform EOP as well as EOFM measurements. It is equipped with an incoherent light source with a wavelength of 1.3μm. The laser scanning microscope is equipped with 5×, 20×, 50× and 100× optical lenses as well as 2×, 4× and 8× digital zoom. We mainly used the 50×, objective lens since it exhibits a higher numerical aperture than the others. For our attack approach, we used three different optical probing methods: 1) EOFM in amplitude mode and phase mode, 2) LLSI, 3) EOP. A focused light beam is either raster-scanned pixel by pixel over the device's backside to obtain 2-D activity (EOFM) or logic state (LLSI) maps or parked statically at a particular position to acquire a signal in the time domain (EOP).

The experimental setup is illustrated in Figure 8. For EOFM in amplitude mode, reflected light from the DuT's backside is measured by a photo-detector for each pixel

[2]https://www.hamamatsu.com/eu/en/product/semiconductor-manufacturing-support-systems/failure-analysis-system/C11222-16.html



(a) Illustration of the experimental setup



(b) DuT under the optical microscope

Figure 8: Experimental setup

and then sent to a frequency analyzer or lock-in amplifier for characterization. To identify periodic signals on the chip, the area of interest is scanned by an optical beam while directing the output of the photo-detector into a narrow bandpass filter tuned to the target frequency. The result will be a 2D gray-coded image showing all the sites switching at the target frequency. For the phase mode, a reference signal is needed from the DuT which is in synchronization with the DuT's clock or data signal. The frequency analyzer uses two phase sensitive detectors (PSDs) and a low pass filter to generate a signal proportional to the phase difference between the reference and the photo-detector signals. As a result, performing EOFM in amplitude mode provides a map of the locations that are modulating at a specified target frequency while operating EOFM in phase mode, the phase differences between switching transistor clusters and a reference signal are recorded to create a phase map.

In the EOP setup, the output of the photo-detector is measured by an oscilloscope. A reference signal from the DuT is connected to the EOP tool as well. After the laser beam is positioned on a point of interest, the EOP tool measures the extremely weak signals over a defined time window and averages them to reduce the noise and obtain a clearer signal in the time domain.

For LLSI, the internal core voltage of the DuT has to be modulated. The sine wave signal used for this purpose is generated by a Keithley 3390 function generator, and a Toellner laboratory power supply (TOE8732) provides the DC voltage. DC voltage and the sine wave is fed to a Bias-T to modulate the core voltage. An LLSI peak-to-peak modulation amplitude up to 500mVpp at 120kHz is possible without disturbing the functionality of the device. The `clock` and the `scan in` for the DuT is supplied by an FPGA, which allows producing a certain number of clock signals and stopping the clock.

7 Verification of our Attack Approach

We verify our attack approach by using a set of experiments as demonstrated in this section. Our attack approach consists of two main parts. In the first part, the position of the target SFFs are located by analyzing the scan pattern. In the second part, we have proven our optical approach on the UlpiSPI chip. Both steps are elaborated in detail below.

7.1 Decoding the Scan Path Semantics

At first, we are going to verify the method of reverse engineering the semantics of a scan chain, as described in Section 4.2. To be able to understand the semantics of SFFs, different scan patterns are observed for different inputs. In this POC, we show that we can identify

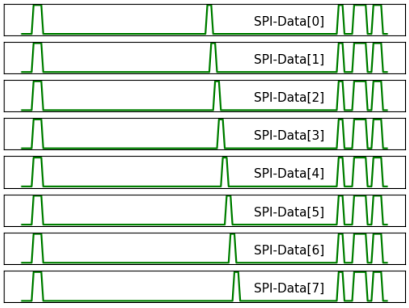


Figure 9: The shifted out data of the first 100 SFFs. These patterns have been observed after storing SPI-Data in normal mode to selected bit values

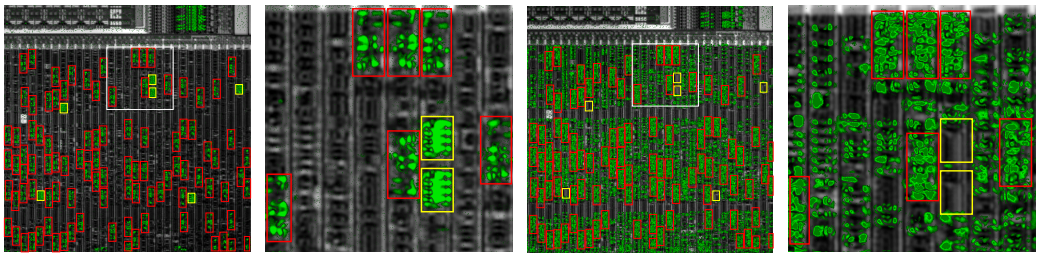


Figure 10: Experimental results for identifying the SFFs. EOFM images in amplitude mode acquired with 50× lens with and without 4× digital zoom. (a) and (b) EOFM based on f_{clk}. (c) and (d) EOFM based on f_{data}. The field of optical zoom is highlighted by a white border. SFFs are indicated by red boxes and clock buffers in yellow.

the index of the SFFs, which store the SPI-Data. This data is read by the SPI-Master whenever a transmission is initiated and is send to an SPI-Slave device respectively. In order to identify the corresponding SFFs, we decided to set SPI-Data via Universal Serial Bus (USB) in normal mode then switch back to test mode and shift out the scan pattern. By carefully selecting SPI-Data which exhibits a hamming weight of 1, the SPI-Data bits can be mapped to their corresponding scan pattern. Figure 9 depicts the first 100 shifts of several recorded scan pattern for different input data.

It can be observed that in the center of this part of the scan pattern at most a single bit is sampled high, whereas the others are set to logic low. This is due to our careful selection of input data: Each SPI-Data transferred in normal mode has exactly a single bit set. Therefore we are able to uniquely map a single input bit to a single SFF, which is identified by its index. In this example, it holds true that every additional SPI-Data bit also succeeds its predecessor in the scan pattern order. However, as in practice spatial proximity of SFFs plays a more important role than semantic relations between SFFs inside the scan chain, this is not always the case.

7.2 Optical Probing on the Scan Path

EOFM's distinctive ability to accurately trace the periodic signal within a DuT establishes it as an exceptional technique for identifying the scan chain activity. Acquisition of

frequency maps on scan data input and clock helps to distinguish sequential logic from combinational logic completely. Moreover, the utilization of EOP can provide additional validation on the spots, which have previously been detected by EOFM.

Initially, the SFFs are localized on the chip. The `scan clock` signal is represented by a square wave function with a duty cycle of 50% and a frequency defined to be f_{clk}, whereas the `scan data in` signal exhibits half its frequency ($f_{data} = \frac{f_{clk}}{2}$) and a phase shift of 90°. This results in an alternating bit sequence being sampled at the scan chain's input. EOFM in amplitude mode was performed at the frequency determined by f_{clk} and afterwards at the frequency determined by f_{data}. Figure 10 shows the frequency response maps. Locations that are modulating both at the clock and the data frequencies are candidates to be SFFs and are highlighted in red. Hence, we conclude that locations that are switching at f_{clk} but not at f_{data} are clock buffers, highlighted in yellow. In addition to SFFs, Figure 10d shows the combinational logic (spots in green) connected to the SFFs modulating at f_{data}.

In the next step, the index of the target SFFs need to be reconstructed. Specifically, our objective is to identify the Master-Out-Slave-In (MOSI) and SPI CLK registers. To accomplish this, we conduct LLSI experiments. Up to this point, we have determined the index of our target SFF in the chain in the previous step, and the indexes of the MOSI and SPI CLK registers are found to be 103rd and 104th in the chain, respectively. Additionally, we have mapped out all the SFFs on the chip. For LLSI, we modulate the core voltage and apply the input pattern similarly as depicted in Figure 7 with an exception. The `scan data input` is held at constant low, except that it is pulled up to logic high in the first and the second clock cycle. In this way, we are able to capture both registers in a single shot. The pattern is shifted in until the target SFFs are loaded with logic high. In order to achieve this, we use the FPGA tester to produce a sequence of clock cycles as many as the index of the target SFFs in the chain. After that, the clock is stopped and we perform LLSI measurements at the core voltage modulation frequency. In the second run, we fill all the SFFs with logic zero and once again perform LLSI measurements at the same frequency. After aligning these two images, subtracting them reveals the locations of the desired registers. Since the combinational logic connected to either MOSI or SPI CLK also transitions from logic low to high, it becomes visible in the subtracted image as well. Having successfully differentiated the sequential logic from the combinational logic in the previous steps, we can now correlate them to eliminate noise originating from the combinational logic.

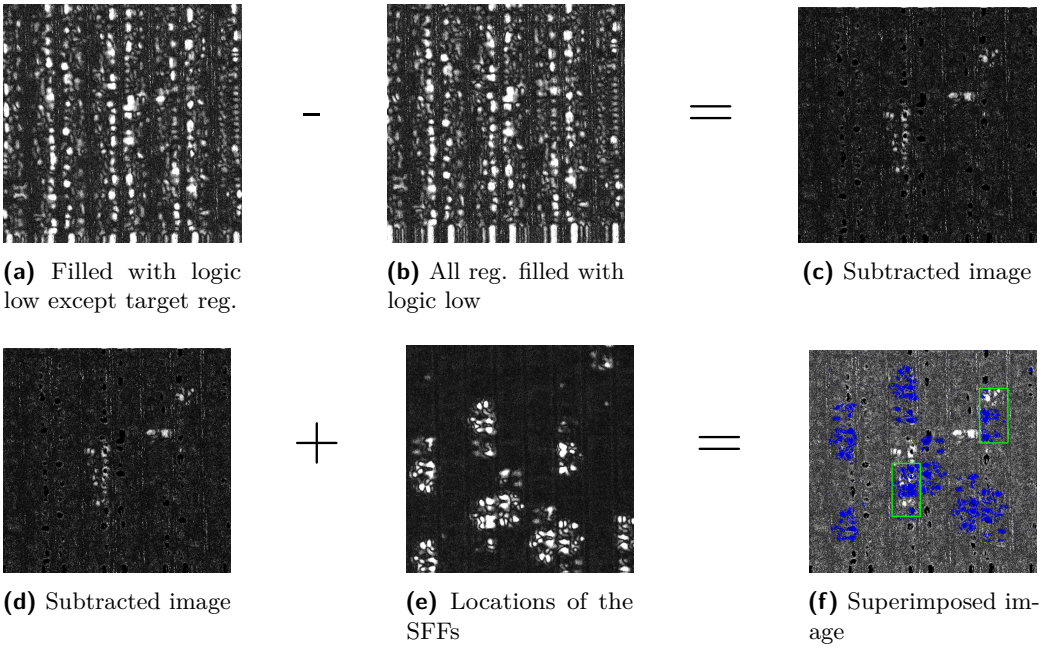
8 Results

First, we present the results of attacking the UlpiSPI DuT, a USB-to-SPI Bridge. By this attack, we aim to show that sensitive data can be disclosed on an inactive scan chain by positioning EOP on the physical location of SFFs. We show this by intercepting transmissions on an SFFs, affiliated to SPI MOSI and SPI CLK.

In the second part, we present the results of attacking an FPGA implementation of a scan chain, which additionally features scan chain-locking. By this we show, that scan chain-locking can be compromised by optical attacks, such as EOFM and EOP.

8.1 Extraction of Sensitive Data from UlpiSPI Chip

We would like to show that SPI transmissions can be intercepted without any physical contact utilizing EOP parked on a SFFs of interest. Here, we had to identify the physical location of the MOSI and SPI CLK SFFs first, before being able to intercept transmissions. This has been accomplished exactly as mentioned in Section 4: First of all the logical position of the MOSI and SPI CLK SFFs has to be identified in the scan chain, which



(a) Filled with logic low except target reg.

(b) All reg. filled with logic low

(c) Subtracted image

(d) Subtracted image

(e) Locations of the SFFs

(f) Superimposed image

Figure 11: LLSI images are used to identify the MOSI and SPI CLK registers' positions on the chip. The superimposed image displays the positions as highlighted in green. (The images are aligned before subtraction.)

consists of 2100 SFFs. Afterward, based on their identified position in the scan path, the physical location needs to be found. By implementing our Tester design introduced in Subsection 2.3 on a Xilinx `XC7A35T-1CPG236C` FPGA, we have been able to precisely control the scan chain to our demands. In addition to the scan chain signals (i.e. TDO, TDI and TCK), the FPGA controls the `scan enable` signal to switch between modes. Moreover, the output test pattern of a single scan is transferred from BRAM over USB to be stored on a computer for later evaluation. While keeping the device operating in normal mode, we store a specific byte inside the DuT's SPI-Data registers. By switching between normal and test mode, we gain knowledge on the index of the MOSI and SPI CLK registers within the scan chain, as described in Section 4. In this example, we found the index of MOSI and SPI CLK registers to be equal to 103 and 104, respectively. By exploiting the gained knowledge of index, we perform EOFM and LLSI to identify the SFF's physical location, as explained in Subsection 7.2. The physical locations of MOSI and SPI CLK are depicted in Figure 11. After being certain to have identified the right position, we moved the laser precisely to the discovered position and started EOP recordings. While operating the device exclusively in normal mode, we shifted in different MOSI data via USB and initiated an SPI transmission. In this exemplary attack, we have been storing `0xFD55`, inside the SPI-Data registers. By precisely probing the location previously identified to be the MOSI-affiliated SFF, we have been able to successfully reconstruct the data transmitted via USB, as presented in Figure 12.

Since the length of the scan chain is 2100 and the clock frequency is 1 MHz, we need 2,1 ms for shifting in one pattern and this has to be repeated one more time after modifying a single bit on the pattern for identifying the index of just one SFF in the scan path. If there are n target registers, the time needed to determine their indexes will be $2 \times n \times (1/\text{CLK freq.})$ seconds. In the localization phase, we need approximately 14 min. for a 1024x1024 pixel size EOFM image. To cover the entire chip area, we need 38 EOFM

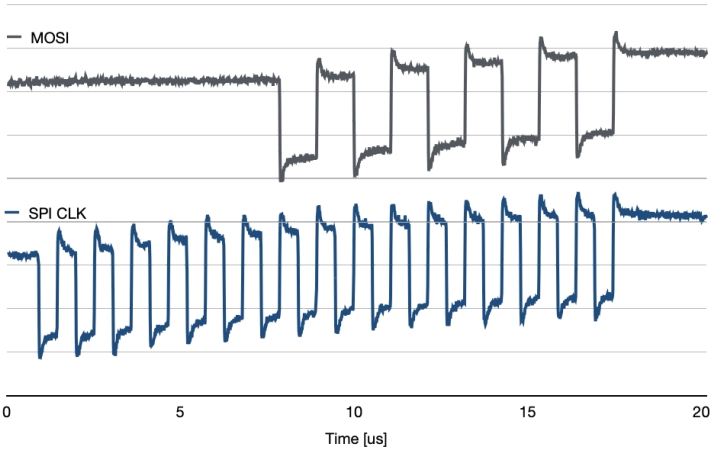


Figure 12: Extracted SPI CLK and MOSI data by EOP tool

images which results in 8,8 hours. Similarly, LLSI experiments require 8,8 hours to search the target register on the whole chip area. For the extraction of the register states, the EOP tool needs integration. It requires approximately 0.5 min. to probe one signal. In total, the total experimental time will lead to 17,6 hours.

8.2 Breaking the Locked Scan Chain Implementation on the Intel Cyclone IV

In this set of experiments, we demonstrate that we can break a locked scan chain that uses `XOR` gates for obfuscation. We assume that the number of `XOR` gates and their placement are not known to the adversary.

The Cyclone IV exhibits a more advanced technology node size of 60nm compared to the UlpiSPI chip's 250nm. Additionally, it operates at a lower core voltage of 1.2V in contrast to the UlpiSPI chip's 2.5V. To enhance the signal strength of both EOFM and EOP, the core voltage is elevated to 1.8V, remaining well within the acceptable range defined by the absolute maximum rating specification. Remarkably, despite the lower voltage levels and smaller sizes, our optical probing set-up delivers sufficient resolution and signal strength, enabling localization of the SFFs successfully.

As described in Section 5, we implemented a locked scan chain consisting of six SFFs. Except for including six registers and three `XOR` gates, the implementation does not include any additional combinational logic between them. The `scan clock` was driven with a frequency of $f_{clk} = 6$MHz and the scan data with a frequency of $f_{data} = 3$MHz with a 90° phase shift, resulting in shifting in alternating bit pattern into the scan chain. We conduct EOFM in amplitude and phase mode as presented in Figure 13. The SFFs are highlighted and numbered according to their indexes in the chain.

Figure 13c shows the SFFs cutout from the EOFM phase image. In this way, the phase differences between the flip-flops become more observable. It is clearly visible, that the 1_{st}, 4_{th}, 5_{th} and the 6_{th} flip-flops are in the same phase, whereas the 2_{nd} and 3_{rd} flip-flops exhibit a phase shift of 180°.

As a next step, EOP measurements are performed on the white dots shown in Figure 13c. The `scan clock` was kept at a frequency of $f_{clk} = 6$MHz. The scan data was kept at logic low, only shifting in a logic high every six clock cycles. Figure 14 shows EOP measurements for all six scan flip-flops sorted by the arrival time of the data pulse. With this measurement, we can easily deduce the indexes in the chain and correlate their spatial positions with their respective indexes.

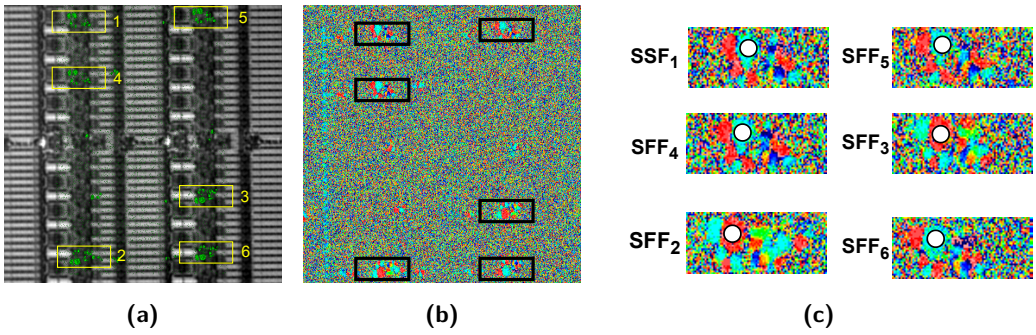


Figure 13: EOFM images reveal the location of the SFFs. (a) EOFM in amplitude mode overlayed on the reflected light micrograph of the device.(b) EOFM in phase mode (c) Zoomed in EOFM phase mode images of each SFF

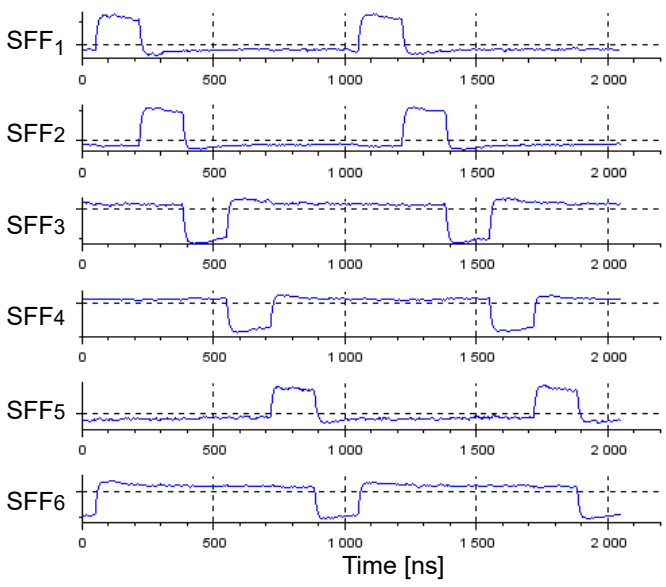


Figure 14: EOP on SFFs enables sorting out their indexes in the chain and detecting the conversions between them.

The EOP measurements conducted on the individual SFFs not only provide the attacker with information regarding the position of a specific SFF within the scan chain but also reveal inversions between these flip-flops. As depicted in Figure 14, it becomes evident that the scan data is inverted between SFF_1 and SFF_2, SFF_3 and SFF_4 and between SFF_4 and SFF_5. Armed with this knowledge about the architecture of the locked scan chain, an attacker can readily deduce the secret key $k = 111$, thereby enabling the computation of operations on the scan-in and scan-out patterns. Furthermore, even an attacker lacking prior knowledge about the placement of obfuscation gates can perform the computation on the scan-in and scan-out pattern by probing each SFF.

9 Discussion

9.1 Countermeasures

The primary objective of a countermeasure against our attack is to prevent the extraction of sensitive data. In our attack scenario, the scan chain serves as a tool to locate the target registers containing sensitive data, complemented by optical probing to complete the data extraction process. If the register locations are readily known, there is no need for scan-chain side channel. At that stage, optical probing alone would be sufficient to execute a successful attack. Similarly, if obfuscation techniques are not in use and the scan chain is accessible, the scan chain side-channel can be successfully employed to attack the chips without using optical probing. First, we begin by examining potential countermeasures outlined against scan chain side-channel in the literature, before delving into countermeasures specifically tailored to combat optical attacks.

Various countermeasures have been proposed in recent years that either improve obfuscation design techniques against new emerging attacks or integrate a test authentication to thwart scan chain side-channel analysis. Karmakar et. al. proposed [KCK20, KKC21] an obfuscation technique based on Dynamically Obfuscated Scan (DOS) [WZH+18]. This time, the obfuscation key is not static but updated periodically. DOS consists of a LFSR to produce the keys, a control unit to define the update frequency of the keys, and a shadow chain to counteract resetting attacks. Key gates in their model are mux-based and very similar to the obfuscation technique that we have used as a target device in Subsection 8.2. As we mentioned in Subsection 2.4, optical side-channel attacks are very successful in tracking the signals on the chip and extracting data from the flip-flops. LFSR consists of flip-flops and their content can be directly read out by optical probing which even eases launching the attack. Additionally, they propose restricting the scan access via scan-enable input encryption. Only trusted test engineers who hold the test key can unlock the scan chain. As opposed to their threat model, we assume in our approach that the outsourced foundry and the test company are fully untrusted environments where the test engineers have full access to the scan chain interface. In [LKK+21], authors present DisORC which aims to defend devices against oracle-based attacks. Upon detecting any attempt to access the chip's scan interface, the defense system promptly erases all traces of the encryption key and disables its connection to the circuit, effectively preventing the use of scan chains as long as the correct key is in the system. We should emphasize that our attack approach does not require any scan access on the target device as discussed in Section 3.

Partial Scan has been presented in [CA90] which includes only a specific subset of registers in the scan chain, effectively addressing concerns related to area and power overhead. However, such an approach decreases the test coverage, since it can not isolate the defects within the excluded flip-flops [WZH+18]. While the main objective is to optimize testability with minimal area and power impact, excluding security-sensitive registers from the scan chain also helps mitigate the risk of scan chain leakage. For instance, in the Caliptra framework, it is strongly recommended that debofuscation key flip-flops are

not included in the scan chain as a measure to enhance multi-layered security[3]. However, in [DRDNFR12], the authors introduce an attack capable of extracting the secret key even when partial scan design is utilized. In their approach, the authors first utilize a procedure to determine if any flip-flops from the round register appear in the scan-out response during an attack on an AES core. If present, they can recover the secret key from this partial information. However, if the initial procedure fails, indicating that none of the round-register flip-flops are included in the scan path, it suggests that a scan-based attack will be unsuccessful.

On-chip compression [LH07, DEG+13] which is widely adopted by industry is thought to naturally counteract scan chain side-channel attacks. On the other hand, it was shown that test-mode-only attacks are able to squeeze out AES keys in the presence of on-chip compression [SASK14]. If integrated into our attack approach, test-mode-only attacks can be employed to decode the semantics of the scan chain, the first step of our attack. To perform the second and third step of the proposed attack, the decompressor architecture needs to be known, to ensure the attacker can shift in data with a strictly periodic behavior (second step) and is able to scan in logic `HIGH`s only to the registers of interest (third step). Knowledge about the decompressor structure is also a requirement for the attack proposed in [SASK14], where it is assumed that the attacker can obtain through the EDA vendor flow or reverse engineering.

The only way to counteract optical side-channel attacks is to protect the backside of the ICs. Optical probing techniques require the light beam to enter and/or exit the silicon from the back surface of the device. Consequently, an effective protection structure for the IC back surface must be opaque to IR light. In [ABH+18a, ABH+18b], it has been shown that an optically active layer deposited on the IC backside can be a comprehensive countermeasure against optical contactless techniques. The integrity of the protection layer is constantly verified using light-emitting diodes and light detectors on the front side. The light emitted by diodes interacts with photodetectors that absorb the light reflected from the IC backside, thereby generating a photocurrent. The opaque protection layer changes the intensity of the reflected light depending on the angle of incidence of the light. The photocurrent of the detectors is a signature of the layer. If the protection layer is damaged or removed, the signal of the detectors will change. Confidential data stored on the device is programmed to be erased in the case of such an attack. This protection structure is quite cost-effective and applicable to ICs of various thicknesses and applications. It does not require an additional step for manufacturing. Moreover, preparing this type of optical film is not expensive.

9.2 Applicability on Smaller Technology Devices

The continuous miniaturization of IC technology and new complex emerging technologies such as System-on-Modules (SoMs) introduce some challenges for optical side-channel attacks. The spatial resolution (R) of the optical setup depends on the wavelength of the light (λ) and the numerical aperture (NA) of the lens and it can be defined as $R = 1,22\lambda/NA$ [Ray79].

Our optical probing setup utilizes a 1300 nm wavelength light source with a spot diameter of 1 µm, which is larger than the gate of a minimum-size transistor. The comparison between technology size and optical resolution can sometimes lead to the misconception that optical probing is not viable for smaller technology sizes. This misconception can be attributed to the formal definition of 'pitch', which encompasses the combined sizes of the gate, source, drain, and isolation oxide regions, resulting in a dimension that is up to four times the minimum technology node size. Furthermore, considering the attacker's point of view, it is required to distinguish between opposing logic states within clusters of

[3] https://github.com/chipsalliance/caliptra-rtl/blob/main/docs/CaliptraIntegrationSpecification.md

transistors, rather than at the individual transistor level. Additionally, the intensity profile of a light beam versus its radius follows the Gaussian distribution, hence the intensity is the strongest in the center of the beam and fades out through the periphery. Interestingly, this misconception has already been debunked in a study [TLSB17], where the authors successfully extracted the bitstream from a 28nm FPGA. In case it is required, we can improve the resolution to 200 nm by increasing the NA with a solid immersion lens (SIL). The usage of a SIL has been shown to enable optical probing for a 10 nm technology device [VHRG+15].

When the technologies scale down, the supply voltage decreases, as well. Optical probing signal strength is only linearly correlated to voltage when compared to photon emission microscopy which is strongly dependent on supply voltage [ABB+21]. Hence, optical probing is the preferred technique for FA engineers in the new millennium, as well.

Regarding sample preparation, the most recent flip-chip packaging technology eliminates the need for de-packaging process. The die inside a flip-chip package is readily placed upside-down, thereby exposing the silicon backside. The only requirement is to remove the attached heat-spreader, a task that can be efficiently accomplished using a knife under high or sub-zero temperatures. After removing the heat sink, the backside of the chip is exposed and the silicon substrate thickness is thin enough for conducting near-infrared (NIR) analysis without any further alterations.

9.3 Localization Complexity in Large Devices with and without Scan Chain Side-Channel

Since modern ICs consist of billions of transistors and have large silicon dimensions, locating the targeted registers on the chip without the GDSII file requires more time and resources. In each optical technique, the attacker has to locate the registers before probing them, which can be cumbersome depending on the application and the DUT. Memory blocks occupy a relatively large area and they consist of repetitive features that can be identified easily from reflected light images. Similarly, locating registers in an FPGA is trivial since FPGAs are made out of logic elements (LEs) that are laid out as regular structures that repeat themselves at each LE. On the other hand, registers in an ASIC are situated within the logic area that consists of different blocks with individual functions. They have irregular structures and they take up a very small area. Therefore, localization of the target registers can be difficult in an ASIC depending on the application if the chip area is very large. In such a case, scan chains are a remarkably beneficial side-channel for overcoming the localization challenge. Our DuT, the Ulpi-SPI bridge, has dimensions of 20 x 14 mm and contains 2100 flip-flops. With a scan clock operating at 1 MHz, the time required to shift out the entire pattern is 2.1 ms. In contrast, modern ICs typically include millions of flip-flops and have slightly larger silicon sizes. As a comparison, the Zynq UltraScale+ MPSoC features a chip size of 35 x 35 mm. Having millions of SFFs instead of thousands will increase the time required for shifting the pattern from milliseconds to seconds which affects the time needed for decoding the semantics in the first step. However, this increase does not significantly impact the overall time required for the attack, when compared with the second and the third steps where scanning the entire chip optically requires hours as discussed in Subsection 8.1. For example, when comparing our DuT to the Zynq UltraScale+ MPSoC, this would result in a 4.4-fold increase in scanning time. With all the steps combined in our attack approach, the time spent to localize a register is a matter of device dimension rather than the number of registers. Additionally, optical techniques such as lock-in thermography, PE, or TLS can be employed to locate specific structures in SoMs, such as cryptographic cores within a chip by tracking their activity, resulting in a reduced search space [Loc23, LTK+18b]. After that, our attack approach can be utilized to detect single registers within the identified building block.

Moreover, it is crucial to emphasize that for EOFM to operate at its best, the target signal must be periodic, and with a high enough frequency for the detection and the duty cycle should be optimally set at 50%. Any deviation from these optimal conditions will result in a reduction in the EOFM signal strength [SG19]. In such a case, scan chains as a side-channel are convenient. Because the attacker is able to control the scan clock and data shift frequency which is a perfect scenario for conducting EOFM measurements.

10 Conclusion

In this work, our primary focus lies in the comprehensive assessment of the potential risks entailed by including scan chain structures in the ICs. We demonstrate for the first time the power of employing a non-invasive optical probing technique in conjunction with scan chain exploitation. To achieve this, we develop a Tester circuitry capable of analyzing the intricate semantics of a scan chain. Leveraging this acquired knowledge, we successfully launch an optical side-channel attack for reverse engineering the scan path. Moreover, we showcase the efficacy of our approach by launching an attack on a secure scan chain implemented on an Intel Cyclone IV FPGA platform. Furthermore, we present how, with prior knowledge gained by reverse engineering the scan path, sensitive data can be extracted from SFFs of an ASIC USB-to-SPI Converter by optical probing in normal mode. This research unveils valuable insights into the potential vulnerabilities associated with scan chain structures, thereby contributing to the advancement of secure DfT structures.

References

[ABB+21] Elham Amini, Kai Bartels, Christian Boit, Marius Eggert, Norbert Herfurth, Tuba Kiyan, Thilo Krachenfels, Jean-Pierre Seifert, and Shahin Tajik. Special session: Physical attacks through the chip backside: Threats, challenges, and opportunities. In *2021 IEEE 39th VLSI Test Symposium (VTS)*, pages 1–12, 2021.

[ABH+18a] E. Amini, A. Beyreuther, N. Herfurth, A. Steigert, R. Muydinov, B. Szyszka, and C. Boit. Ic security and quality improvement by protection of chip backside against hardware attacks. *Microelectronics Reliability*, 88:22–25, 2018.

[ABH+18b] Elham Amini, Anne Beyreuther, Norbert Herfurth, Alexander Steigert, Bernd Szyszka, and Christian Boit. Assessment of a Chip Backside Protection. *Journal of Hardware and Systems Security*, 2(4):345–352, 2018.

[AGM16] Leonid Azriel, Ran Ginosar, and Avi Mendelson. Exploiting the scan side channel for reverse engineering of a vlsi device. *Technion, Israel Institute of Technology, Tech. Rep. CCIT Report*, 897, 2016.

[AGM17] Leonid Azriel, Ran Ginosar, and Avi Mendelson. Revealing on-chip proprietary security functions with scan side channel based reverse engineering. In *Proceedings of the on Great Lakes Symposium on VLSI 2017*, GLSVLSI '17, page 233–238, New York, NY, USA, 2017. Association for Computing Machinery.

[ASYT12] Yuta Atobe, Youhua Shi, Masao Yanagisawa, and Nozomu Togawa. Dynamically changeable secure scan architecture against scan-based side channel attack. In *2012 International SoC Design Conference (ISOCC)*, pages 155–158, 2012.

[AYS+19] Lilas Alrahis, Muhammad Yasin, Hani Saleh, Baker Mohammad, Mahmoud Al-Qutayri, and Ozgur Sinanoglu. Scansat: Unlocking obfuscated scan chains. In *Proceedings of the 24th Asia and South Pacific Design Automation Conference*, ASPDAC '19, page 352–357, New York, NY, USA, 2019. Association for Computing Machinery.

[BT18] Swarup Bhunia and Mark Tehranipoor. *Hardware Security: A Hands-on Learning Approach*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 1st edition, 2018.

[BTS+16] Christian Boit, Shahin Tajik, Philipp Scholz, Elham Amini, Anne Beyreuther, Heiko Lohrke, and Jean-Pierre 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)*, pages 365–369. IEEE, 2016.

[CA90] K.-T. Cheng and V.D. Agrawal. A partial scan method for sequential circuits with feedback. *IEEE Transactions on Computers*, 39(4):544–548, 1990.

[DEG+13] Amitabh Das, Barış Ege, Santosh Ghosh, Lejla Batina, and Ingrid Verbauwhede. Security analysis of industrial test compression schemes. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 32(12):1966–1977, 2013.

[DRDNFR12] Jean Da Rolt, Giorgio Di Natale, Marie-Lise Flottes, and Bruno Rouzeyre. Are advanced dft structures sufficient for preventing scan-attacks? In *2012 IEEE 30th VLSI Test Symposium (VTS)*, pages 246–251, 2012.

[GPY+12] S. H. Goh, Yan Pan, G. F. You, Y. H. Chan, He ran, Thomas Herrman, Thomas Heller, Victor S. K. Lim, Z. H. Mai, Jeffrey Lam, C. M. Chua, W. P. Chua, and S. H. Tan. Effectiveness of frequency mapping on 28 nm device broken scan chain failures. *Review of Scientific Instruments*, 83(2):023702, 02 2012.

[Jin14] Yier Jin. Design-for-security vs. design-for-testability: A case study on dft chain in cryptographic circuits. In *Proceedings of the 2014 IEEE Computer Society Annual Symposium on VLSI*, ISVLSI '14, page 19–24, USA, 2014. IEEE Computer Society.

[KAFT22] Hadi Mardani Kamali, Kimia Zamiri Azar, Farimah Farahmandi, and Mark M. Tehranipoor. Advances in logic locking: Past, present, and prospects. *IACR Cryptol. ePrint Arch.*, page 260, 2022.

[KB20] Jan-Peter Kleinhans and Nurzat Baisakova. The global semiconductor value chain, 2020.

[KBB08] Tuba Kiyan, Christian Boit, and C. Brillert. Timing sensitivity analysis of logical nodes in scan design integrated circuits by pulsed diode laser stimulation. pages 180–187, 01 2008.

[KCK18] Rajit Karmakar, Santanu Chatopadhyay, and Rohit Kapur. Encrypt flip-flop: A novel logic encryption technique for sequential circuits, 2018.

[KCK20] Rajit Karmakar, Santanu Chattopadhyay, and Rohit Kapur. A scan obfuscation guided design-for-security approach for sequential circuits. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 67(3):546–550, 2020.

[KGM+21] Thilo Krachenfels, Fatemeh Ganji, Amir Moradi, Shahin Tajik, and Jean-Pierre Seifert. Real-world snapshots vs. theory: Questioning the t-probing security model. In *2021 IEEE Symposium on Security and Privacy (SP)*, pages 1955–1971, 2021.

[KKC21] Rajit Karmakar, Harshit Kumar, and Santanu Chattopadhyay. Efficient key-gate placement and dynamic scan obfuscation towards robust logic encryption. *IEEE Transactions on Emerging Topics in Computing*, 9(4):2109–2124, 2021.

[KLB18] Tuba Kiyan, Heiko Lohrke, and Christian Boit. Comparative Assessment of Optical Techniques for Semi-Invasive SRAM Data Read-out on an MSP430 Microcontroller. volume ISTFA 2018: Conference Proceedings from the 44th International Symposium for Testing and Failure Analysis of *International Symposium for Testing and Failure Analysis*, pages 266–271, 10 2018.

[KWT+07] Ulrike Kindereit, Gary Woods, Jing Tian, Uwe Kerst, Rainer Leihkauf, and Christian Boit. Quantitative investigation of laser beam modulation in electrically active devices as used in laser voltage probing. *IEEE Transactions on Device and Materials Reliability*, 7(1):19–30, 2007.

[KY12] Abdel Alim Kamal and Amr M. Youssef. A scan-based side channel attack on the ntruencrypt cryptosystem. In *2012 Seventh International Conference on Availability, Reliability and Security*, pages 402–409, 2012.

[LCP+17] Shih Yuan Liu, Hsin Hung Chou, Man Ting Pang, Kuang Yuan Chao, James C. C. Chang, Jian Chang Lin, and Chun Ming Chen. Laser voltage imaging and probing, efficient techniques for scan chain verification in advanced node. In *2017 IEEE 24th International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA)*, pages 1–4, 2017.

[Lee17] Serge Leef. In pursuit of secure silicon. Technical report, https://rb.gy/ngjzfd, 2017.

[LH07] Chunsheng Liu and Yu Huang. Effects of embedded decompression and compaction architectures on side-channel attack resistance. In *25th IEEE VLSI Test Symposium (VTS'07)*, pages 461–468, 2007.

[LKK+21] Nimisha Limaye, Emmanouil Kalligeros, Nikolaos Karousos, Irene G. Karybali, and Ozgur Sinanoglu. Thwarting all logic locking attacks: Dishonest oracle with truly random logic locking. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 40(9):1740–1753, 2021.

[Loc23] *Lock-in Thermography for the Localization of Security Hard Blocks on SoC Devices*, volume ISTFA 2023: Conference Proceedings from the 49th International Symposium for Testing and Failure Analysis of *International Symposium for Testing and Failure Analysis*, 11 2023.

[LTK+18a] Heiko Lohrke, Shahin Tajik, Thilo Krachenfels, Christian Boit, and Jean-Pierre Seifert. Key Extraction Using Thermal Laser Stimulation A Case Study on Xilinx Ultrascale FPGAs. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2018(3):573–595, 2018.

[LTK+18b] Heiko Lohrke, Shahin Tajik, Thilo Krachenfels, Christian Boit, and Jean-Pierre Seifert. Key extraction using thermal laser stimulation: A case study on xilinx ultrascale fpgas. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2018(3):573–595, Aug. 2018.

[LTP06] J. Lee, M. Tehranipoor, and J. Plusquellic. A low-cost solution for protecting ips against scan-based side-channel attacks. In *24th IEEE VLSI Test Symposium*, pages 6 pp.–99, 2006.

[LWK11] Yu Liu, Kaijie Wu, and Ramesh Karri. Scan-based attacks on linear feedback shift register based stream ciphers. *ACM Trans. Des. Autom. Electron. Syst.*, 16(2), apr 2011.

[LWN+22] Nimisha Limaye, Christian Wachsmann, Mohammed Nabeel, Mohammed Ashraf, Arun Kanuparthi, and Ozgur Sinanoglu. Antidote: Protecting debug against outsourced test entities. *IEEE Transactions on Emerging Topics in Computing*, 10(3):1507–1518, 2022.

[NKC+14] Baohua Niu, Grace Mei Ee Khoo, Yuan-Chuan Steven Chen, Fernando Chapman, Dan Bockelman, and Tom Tong. Laser logic state imaging (llsi). volume ISTFA 2014: Conference Proceedings from the 40th International Symposium for Testing and Failure Analysis of *International Symposium for Testing and Failure Analysis*, pages 65–72, 11 2014.

[NSSO12] D. Nedospasov, J. Seifert, A. Schlösser, and S. Orlic. Functional integrated circuit analysis. In *2012 IEEE International Symposium on Hardware-Oriented Security and Trust*, pages 102–107, June 2012.

[NSY+10] Ryuta NARA, Kei SATOH, Masao YANAGISAWA, Tatsuo OHTSUKI, and Nozomu TOGAWA. Scan-based side-channel attack against rsa cryptosystems using scan signatures. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E93.A(12):2481–2489, 2010.

[Pan21] Vineet Pancholi. Taking advantage of outsourced test services. https://amkor.com/blog/taking-advantage-of-outsourced-test-services/, 2021.

[RAWT96] Haverkos KWJ Richard A. Wheelus TD. Integrated circuit memory using fusible links in a scan chain, 1996. US Patent U567 7917.

[Ray79] Rayleigh. Xxxi. investigations in optics, with special reference to the spectroscope. *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, 8(49):261–274, 1879.

[RKK14] Masoud Rostami, Farinaz Koushanfar, and Ramesh Karri. A primer on hardware security: Models, methods, and metrics. *Proceedings of the IEEE*, 102(8):1283–1295, 2014.

[RKM08] Jarrod A. Roy, Farinaz Koushanfar, and Igor L. Markov. Epic: Ending piracy of integrated circuits. In *Proceedings of the Conference on Design, Automation and Test in Europe*, DATE '08, page 1069–1074, New York, NY, USA, 2008. Association for Computing Machinery.

[RNFR13] Jean Da Rolt, Giorgio Di Natale, Marie-Lise Flottes, and Bruno Rouzeyre. A novel differential scan attack on advanced dft structures. *ACM Trans. Des. Autom. Electron. Syst.*, 18(4), oct 2013.

[RPSK12] Jeyavijayan Rajendran, Youngok Pino, Ozgur Sinanoglu, and Ramesh Karri. Security analysis of logic obfuscation. In *DAC Design Automation Conference 2012*, pages 83–89, 2012.

[Ruh22] Tim Ruhlig. China's digital power - assessing the implications for the eu, 2022.

[SASK14] Samah Mohamed Saeed, Sk Subidh Ali, Ozgur Sinanoglu, and Ramesh Karri. Test-mode-only scan attack and countermeasure for contemporary scan architectures. In *2014 International Test Conference*, pages 1–8, 2014.

[SB87] Richard A Soref and Brian R Bennett. Electrooptical effects in silicon. *IEEE journal of quantum electronics*, 23(1):123–129, 1987.

[SDB+18] Keith A. Serrels, Kris Dickson, Dan Bodoh, Kent Erington, Anusha Weerakoon, and Eric Foot. Scan chain fault isolation using single event upsets induced by a picosecond 1064nm laser. volume ISTFA 2018: Conference Proceedings from the 44th International Symposium for Testing and Failure Analysis of *International Symposium for Testing and Failure Analysis*, pages 93–103, 10 2018.

[SG19] Keith A. Serrels and Ulrike Ganesh. Laser Voltage Probing of Integrated Circuits: Implementation and Impact. In *Microelectronics Failure Analysis: Desk Reference*. ASM International, 11 2019.

[SMC07] Gaurav Sengar, Debdeep Mukhopadhyay, and Dipanwita Roy Chowdhury. Secured flipped scan-chain model for crypto-architecture. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 26(11):2080–2084, 2007.

[SRM15] P. Subramanyan, S. Ray, and S. Malik. Evaluating the security of logic encryption algorithms. In *2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pages 137–143, Los Alamitos, CA, USA, may 2015. IEEE Computer Society.

[TLSB17] Shahin Tajik, Heiko Lohrke, Jean-Pierre Seifert, and Christian Boit. On the Power of Optical Contactless Probing: Attacking Bitstream Encryption of FPGAs. In *CCS 2017*, pages 1661–1674. ACM, 2017.

[VHRG+15] M Von Haartman, S Rahman, S Ganguly, J Verma, A Umair, and T Deborde. Optical Fault Isolation and Nanoprobing Techniques for the 10 nm Technology Node and Beyond. In *Proceedings of the 41st International Symposium for Testing and Failure Analysis*, pages 47–51, 2015.

[WA73] M.J.Y. Williams and J.B. Angell. Enhancing testability of large-scale integrated circuits via test points and additional logic. *IEEE Transactions on Computers*, C-22(1):46–60, 1973.

[WZH+18] Xiaoxiao Wang, Dongrong Zhang, Miao He, Donglin Su, and Mark Tehranipoor. Secure scan and test using obfuscation throughout supply chain. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 37(9):1867–1880, 2018.

[YSN+17] Muhammad Yasin, Abhrajit Sengupta, Mohammed Thari Nabeel, Mohammed Ashraf, Jeyavijayan (JV) Rajendran, and Ozgur Sinanoglu. Provably-secure logic locking: From theory to practice. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, CCS '17, page 1601–1618, New York, NY, USA, 2017. Association for Computing Machinery.

[YWK04] Bo Yang, Kaijie Wu, and Ramesh Karri. Scan based side channel attack on data encryption standard. Cryptology ePrint Archive, Paper 2004/083, 2004. https://eprint.iacr.org/2004/083.

[YWK06] B. Yang, K. Wu, and R. Karri. Secure scan: A design-for-test architecture for crypto chips. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 25(10):2287–2293, 2006.