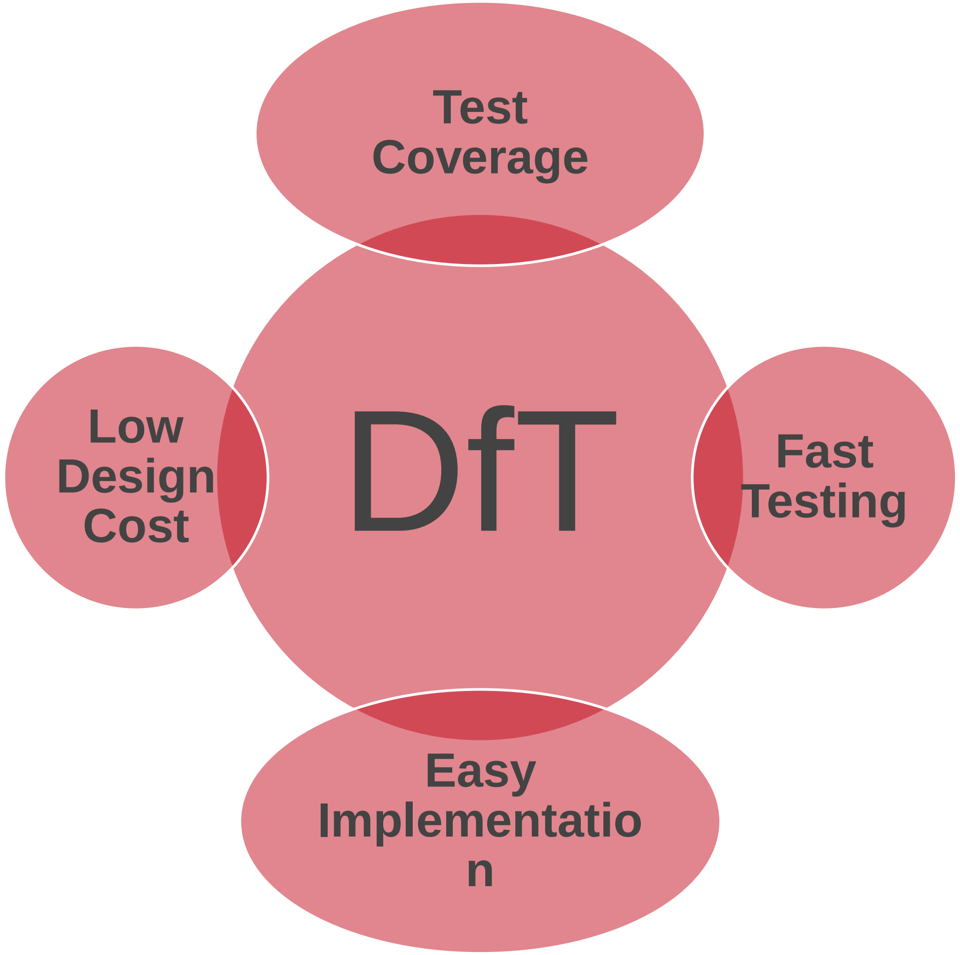
Security Analysis of locked Scan Chains with Failure Analysis Tools

Lars Renkes | SecT | Tage der vertrauenswürdigen Elektronik 2024
lars.renkes@gmx.de

Outline

- Background
- Threat Model
- Attacker’s Approach
- Verification of our attack approach
- Breaking the scan chain obfuscation
- Countermeasures

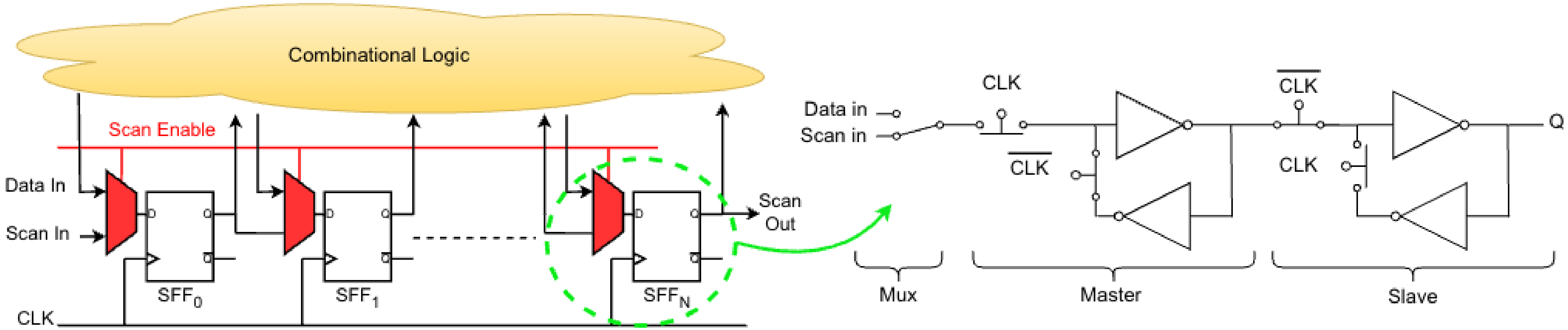
Design for Testing (DfT)



- DFT is used for post-manufactured devices.
- It is generally implemented in an ASIC design and is inserted prior to place and route.
- It can be used to detect manufacturing defects and can be used to perform functional testing.
- It increases the controllability and observability of a given device.
- It is hidden logic and is disabled/restricted after testing.

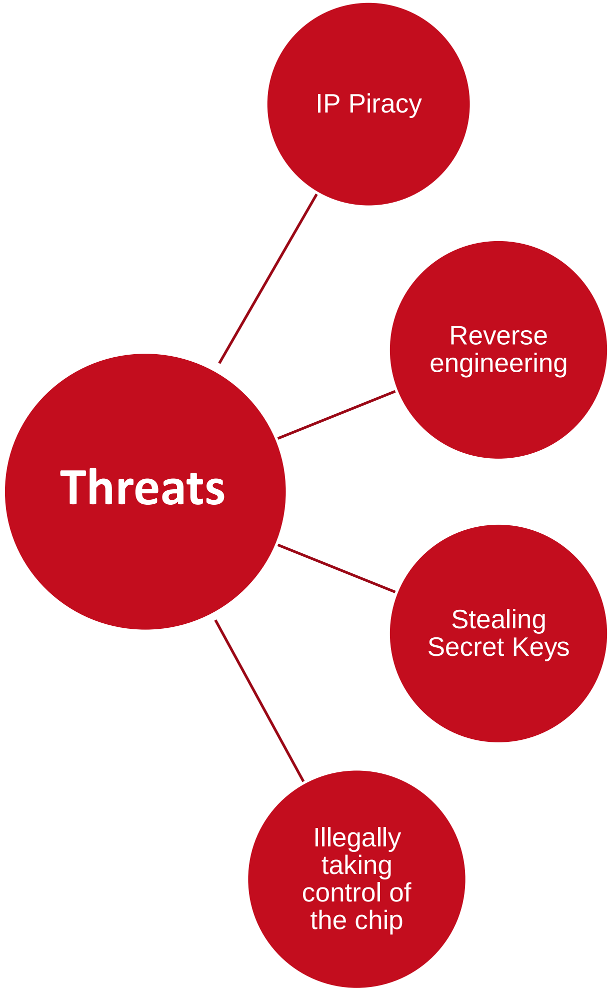
Background

What is a Scan Chain?



- A scan chain consists of a configurable shift register, used in testing to control and observe the internal nodes of a chip.
- During the functional testing, the SFF registers are loaded with a desired state by shifting the input vector through the scan path.
- It drastically decreases the testing time at a post-silicon testing stage.

Security vs. Design for Test



Scan Chain Side - Channel Attacks

An adversary can gain access to the system and do the following:

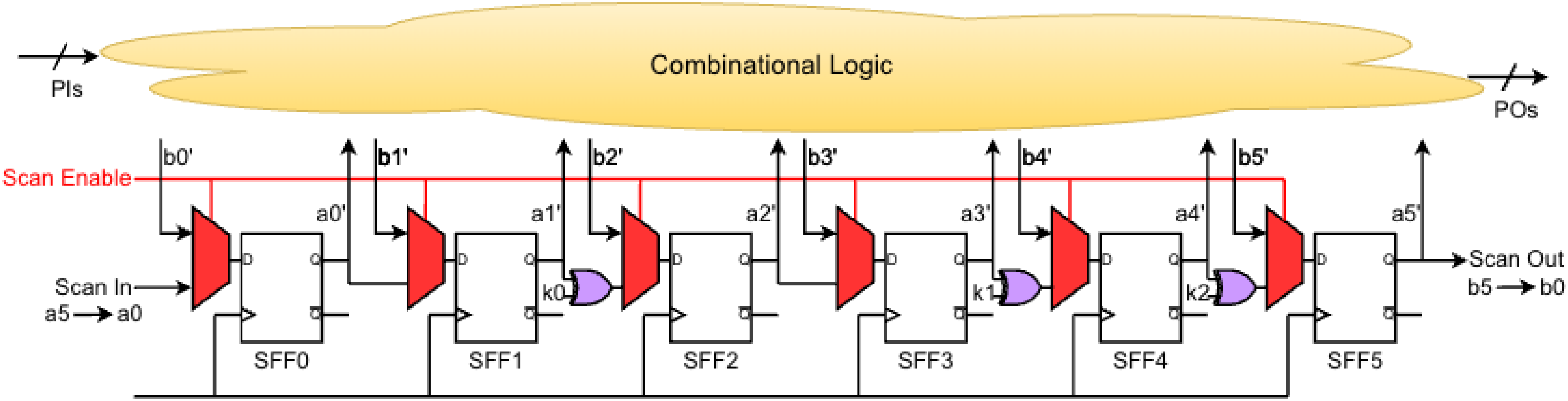
- Change or disrupt the operational state.
- Run test vectors to gain knowledge of the device.

Countermeasures

- Disabling or restricting the scan access
- Resetting the SFFs' content while switching between normal and test mode
- Advanced industrial application techniques → scan compression, masking, or dynamic scrambling of SFFs
- Obfuscation → Scan - Locking

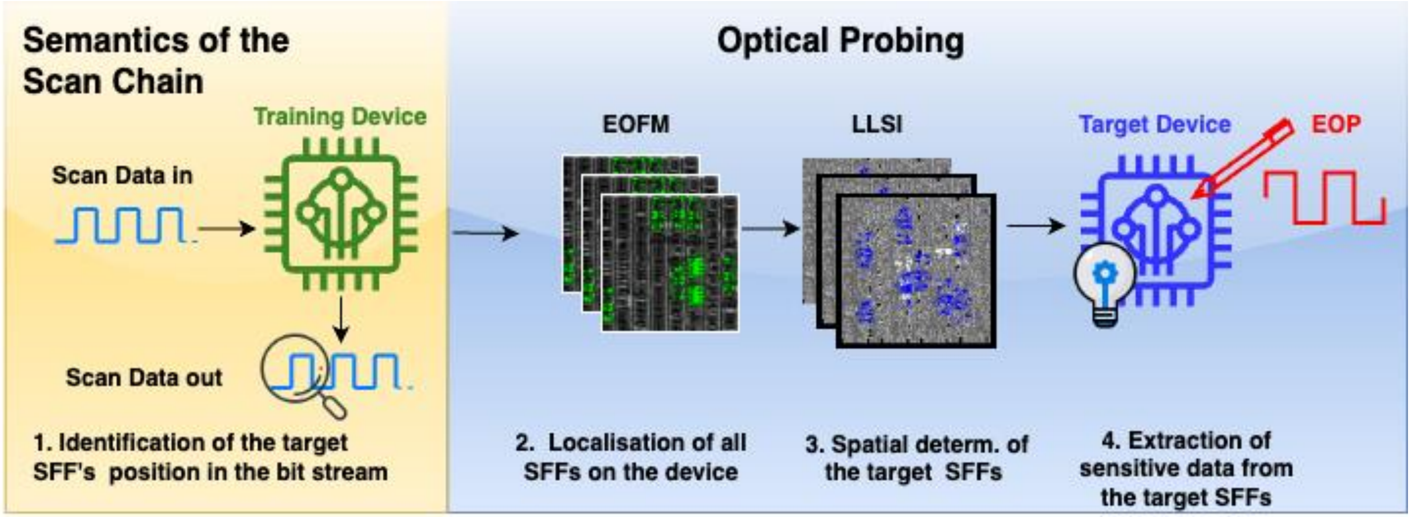
Background

Scan Chain Obfuscation



- Obfuscates the scan chain’s data in order to hide the chip’s functionality during the testing
- Insertion of specific amount of key gates in between the SFFs
- The key gates transform the `Scan In` and `Scan Out` data.

Attacker’s Approach


Semantics of the Scan Chain
Training Device
Scan Data in
Scan Data out
1. Identification of the target SFF's position in the bit stream
Optical Probing
EOFM
LLSI
Target Device
EOP
2. Localisation of all SFFs on the device
3. Spatial determ. of the target SFFs
4. Extraction of sensitive data from the target SFFs

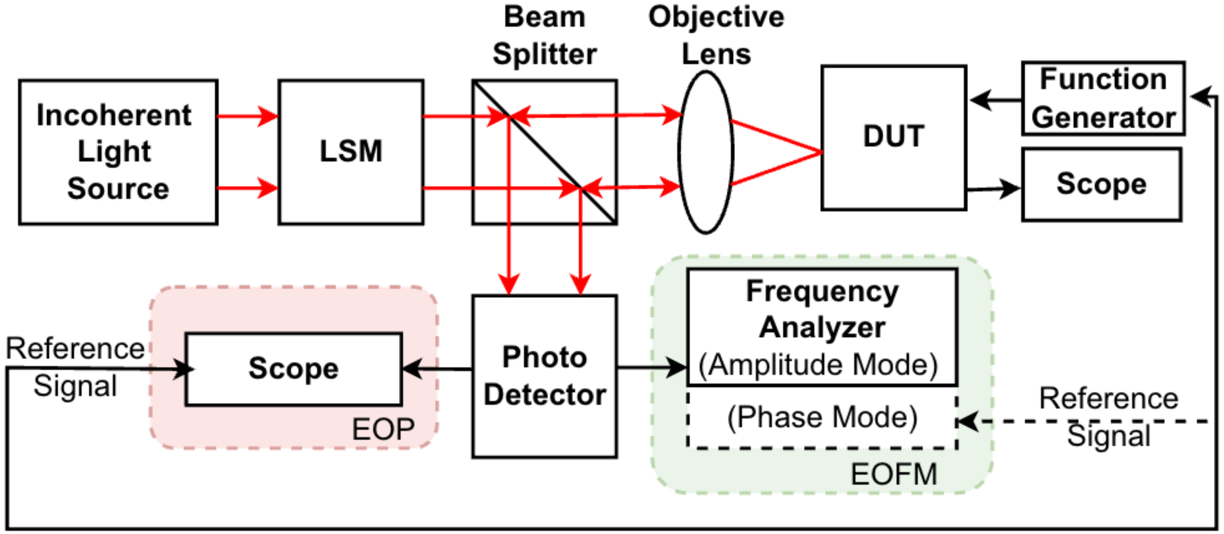
1. Decoding the Scan Path Semantics
2. The spatial localization of all SFFs
3. Localisation of the target SFFs on the chip
4. Extraction of sensitive data

Devices under Test (DuTs)

1. **UlpiSPI Chip :**
   - USB-to-SPI bridge
   - ASIC produced by IHP
   - Produced in 0.25 µm CMOS technology
   - Core voltage : 2.5 V
   - 2100 SFFs
   - No scan access restriction or obfuscation

2. **Intel Cyclone IV :**
   - FPGA
   - Produced in 60 nm technology
   - Core voltage : 1.2 V
   - Each LE includes a 4-input Lookup -Table and a single register cell.
   - We have implemented a locked scan chain, with a length of 6 and 3 XOR gates as key gates

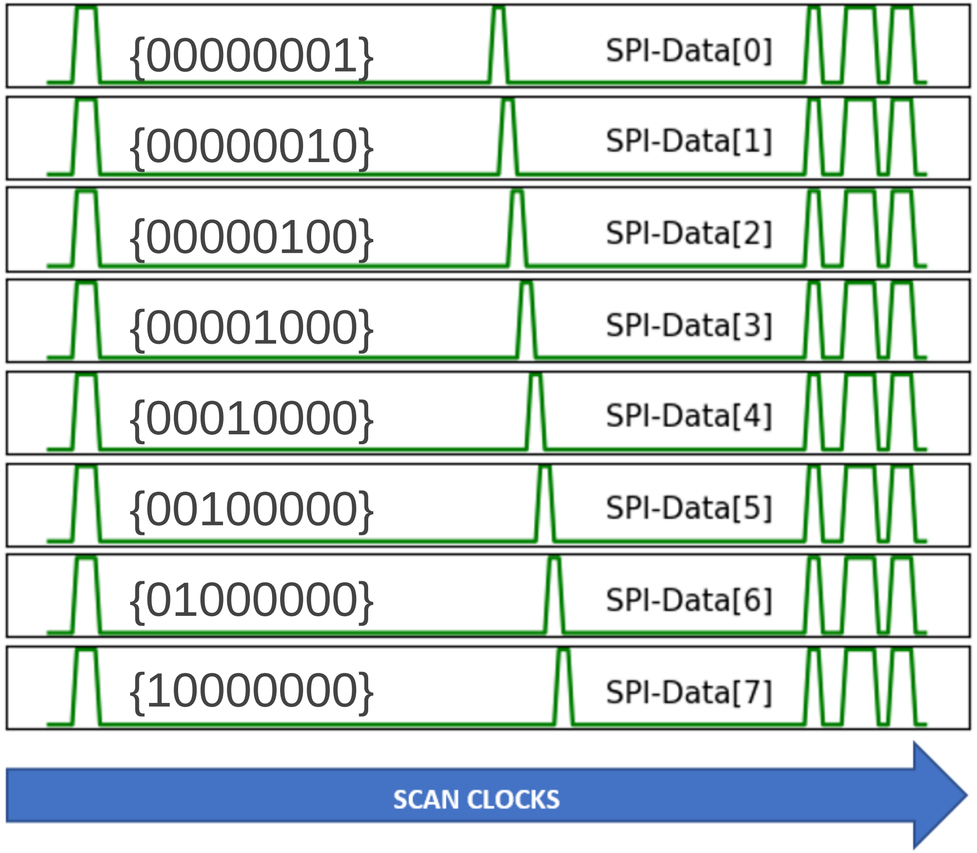
Optical Probing



- The infrared light beam passes through the backside Si → interacts with the active devices on the front side → reflects back through the backside.
- The reflected light beam is modulated depending on the exposed transistor’s operation.
- The weak modulation in the returned light is detected and converted into an electrical signal by a sensitive light detector.
- EOFM → 2-D Frequency Mapping of a selected area
- EOP → scopes the signal at a particular point on a transistor
- LLSI → the core voltage is modulated with a certain frequency and EOFM is performed

Verification of our Attack Approach on SPI Chip

1. Decoding the Scan Path Semantics



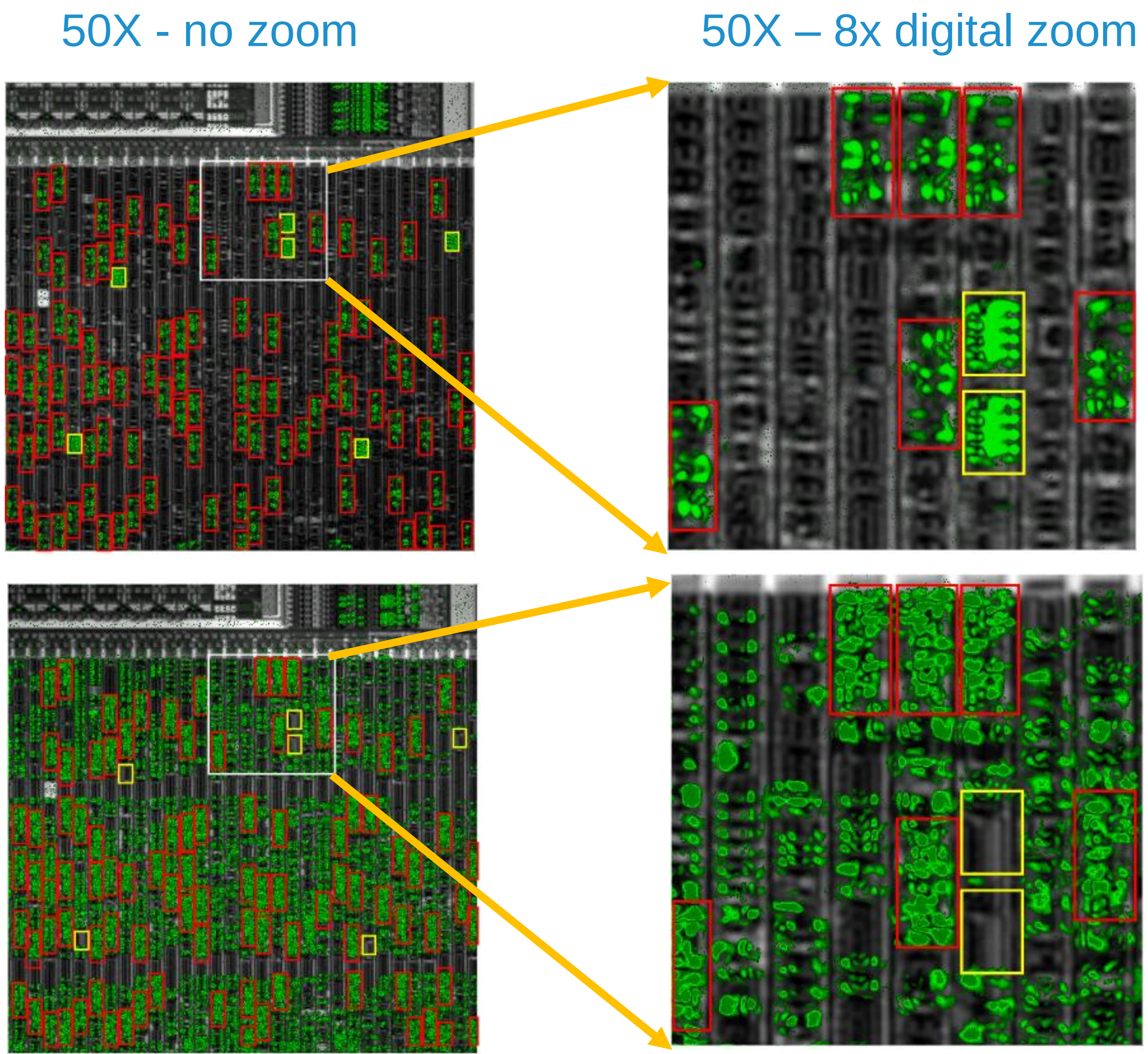
Identification of the order of the SFFs, storing the SPI-Data.

Target SFF's order in the scan chain can be identified, by switching between modes and analyzing the scan out pattern.

1. Reset the DuT into its initial state and set SPI-Data via USB in normal mode in order to store a known byte into an unknown set of SFFs.
2. Switch to test mode and shift out all the scan pattern.
3. Change the SPI data and repeat the same procedure.

Verification of our Attack Approach on SPI Chip

2. Identification of SFFs by EOFM



→ EOFM at clock freq.

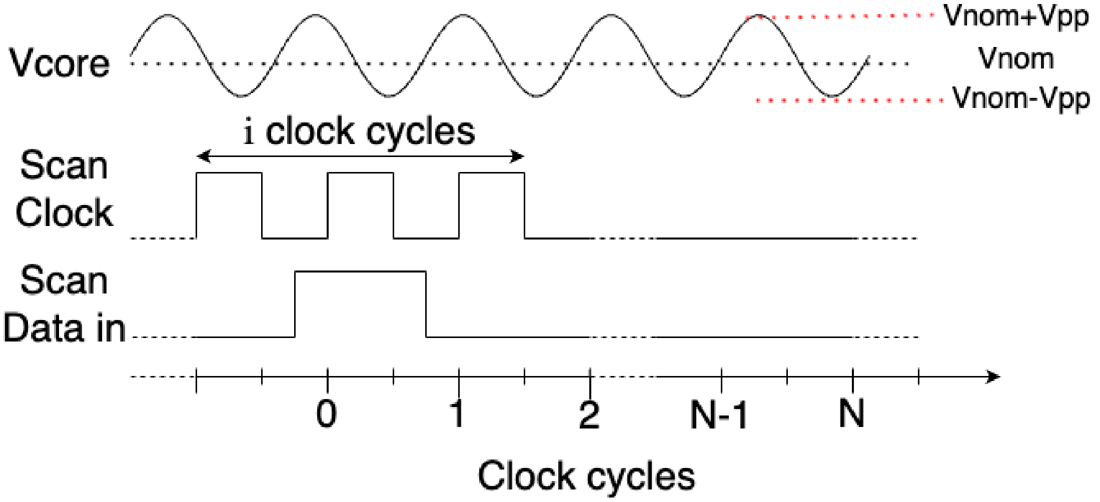
- Locations → modulating at the clock + the data frequencies candidates to be SFFs
- Highlighted in red

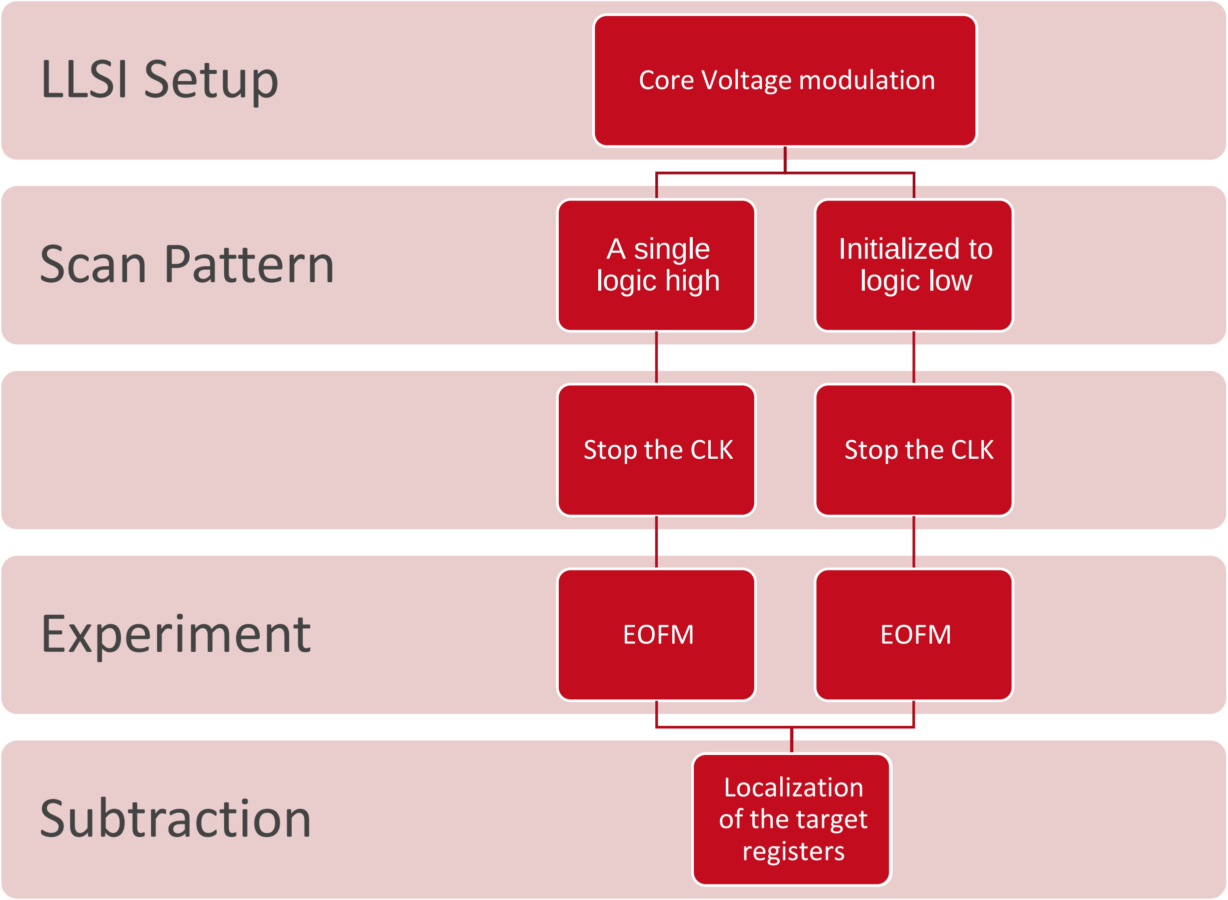
→ EOFM at scan data freq.

Verification of our Attack Approach on SPI Chip

3. Localization of the target SFFs by LLSI

# of CLK cycles = the order of the target SFF





LLSI Setup
- Core Voltage modulation

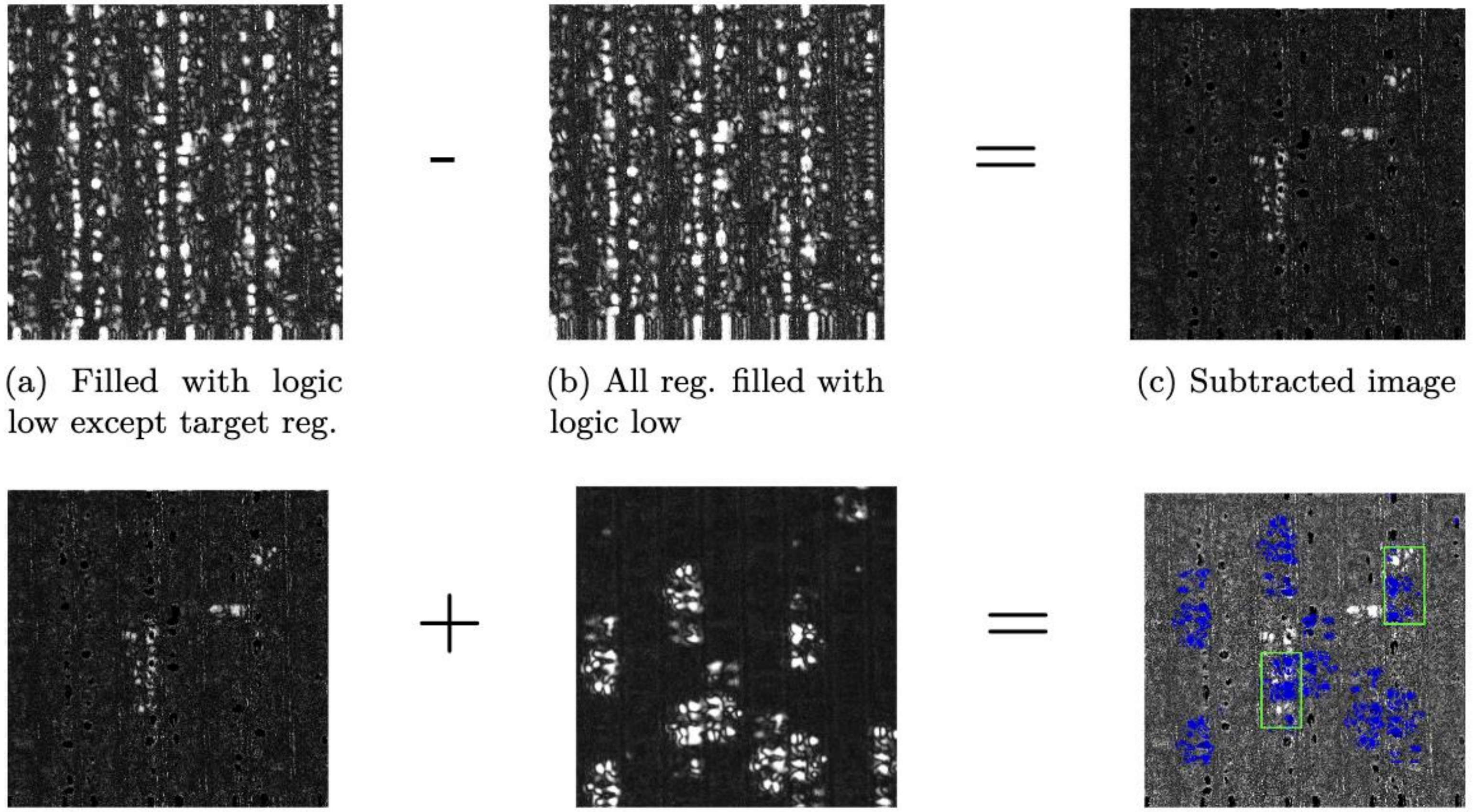
Scan Pattern
- A single logic high
- Initialized to logic low

- Stop the CLK
- Stop the CLK

Experiment
- EOFM
- EOFM

Subtraction
- Localization of the target registers

Identified positions of MOSI and SPI CLK registers



(a) Filled with logic low except target reg.

(b) All reg. filled with logic low

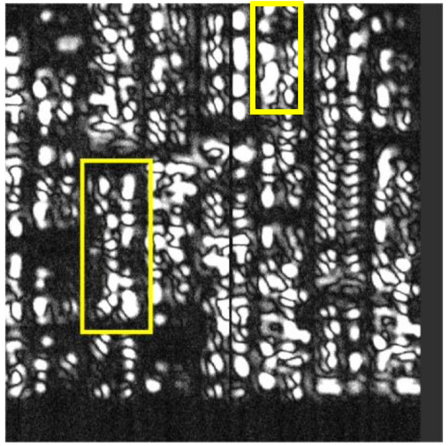
(c) Subtracted image

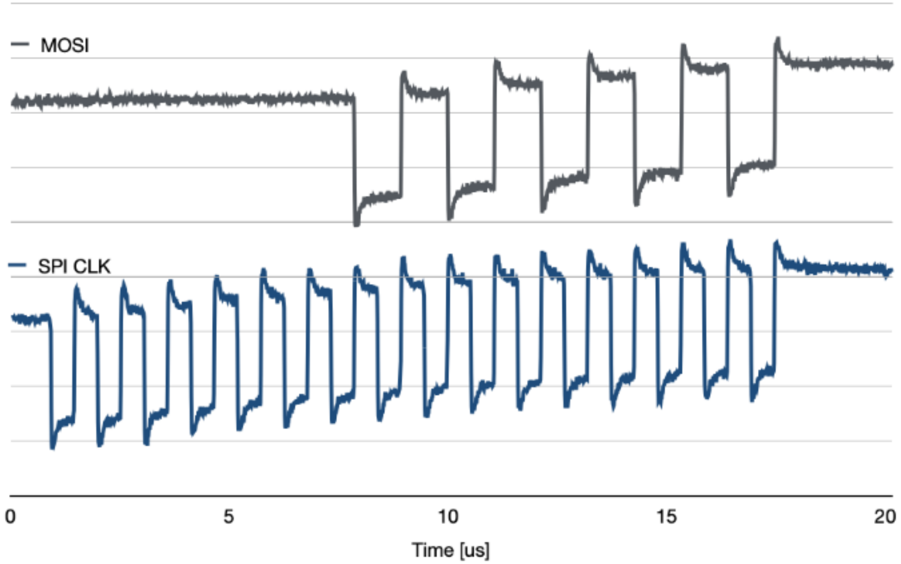
(d) Subtracted image

(e) Locations of the SFFs

(f) Superimposed image

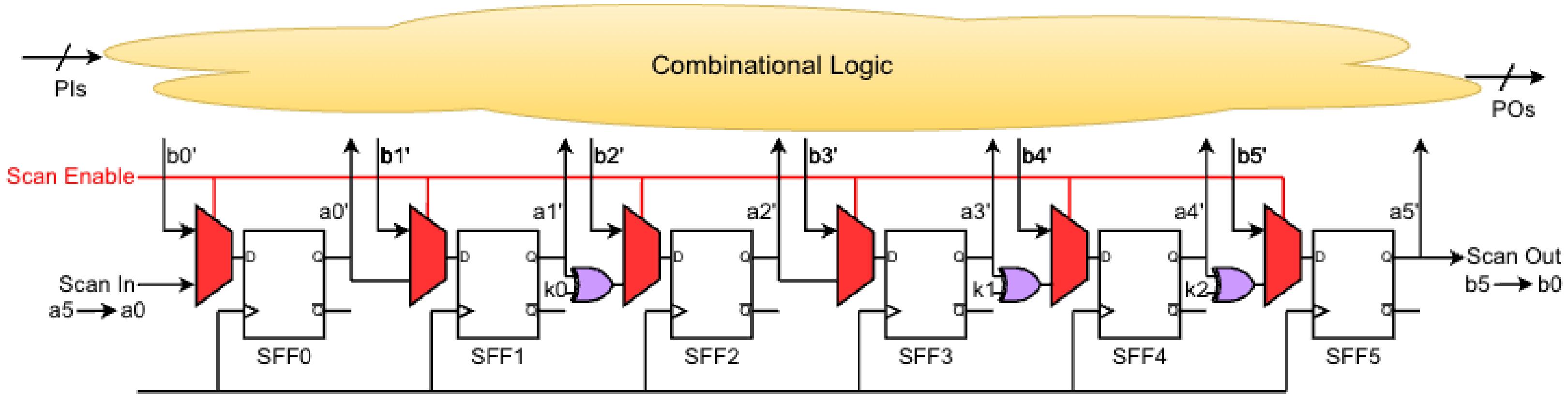
MOSI and SPI Clock Data Extraction in Normal Mode





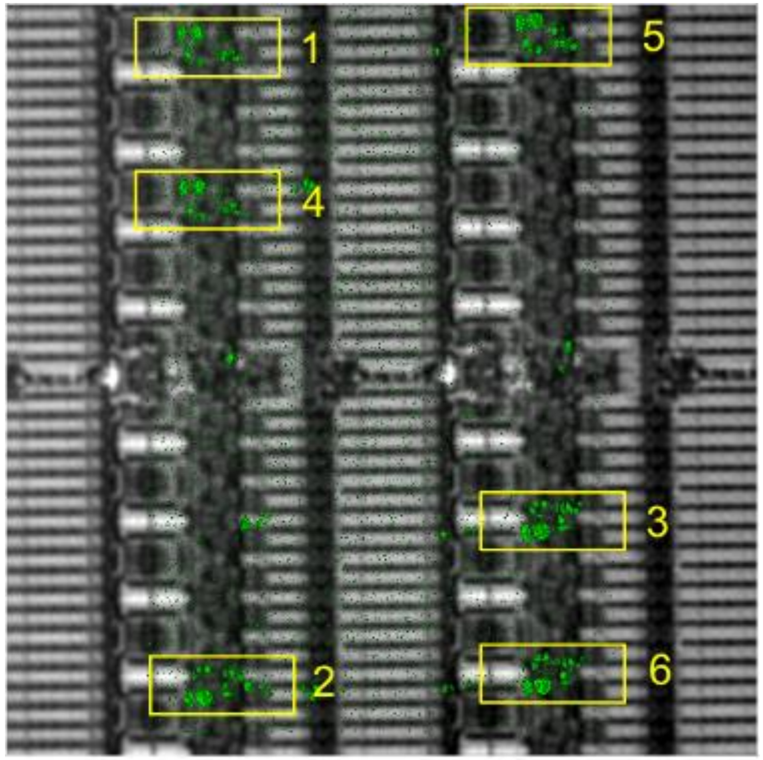
By using the EOP tool, we probe the location previously identified to be the MOSI and SPI CLK, we successfully reconstruct the data transmitted via USB which is found to be `0xFD55`.

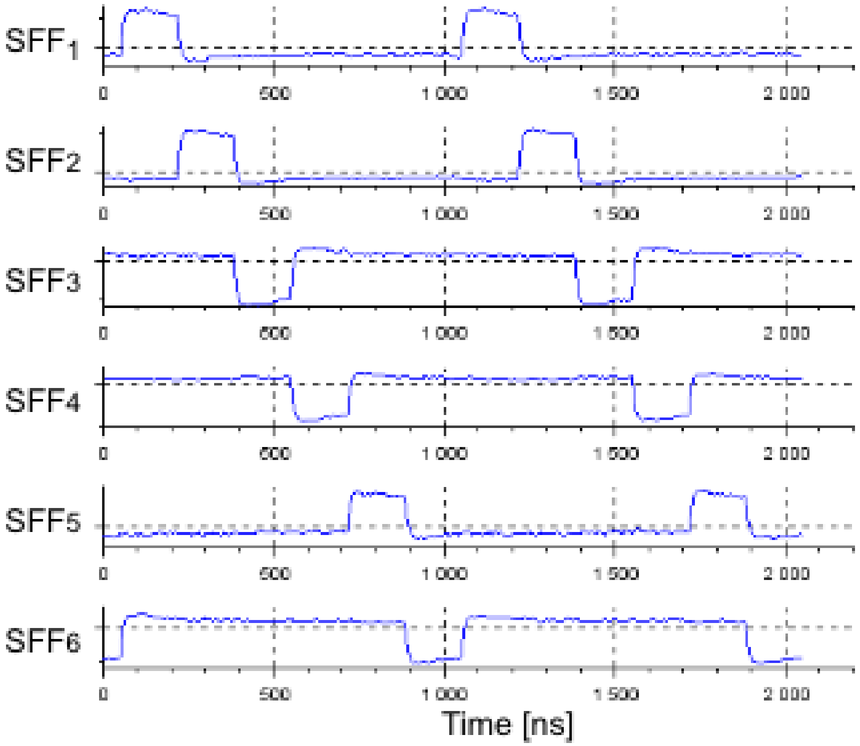
Breaking the Locked Scan Chain Implementation on FPGA



- A locked scan chain that uses `XOR` gates for obfuscation is implemented on Cyclone IV FPGA.
- We assume that the number of `XOR` gates and their placement are not known to the adversary.
- The core voltage is elevated to 1.8V.

Breaking the Locked Scan Chain





- EOFM → f_{clk} = 6 MHz and f_{data} = 3 MHz with a 90^{0}phase shift, resulting in shifting in alternating bit pattern into the scan chain. → input pattern = {101010}

- EOP → input pattern = {100000} → The SFFs are highlighted and numbered according to their order in the chain.

Conclusion

- Our primary focus lies in the comprehensive assessment of the potential risks entailed by including scan chain structures in the ICs.
- We demonstrate the power of employing a non-invasive optical probing technique in conjunction with scan chain exploitation.
- Scan chains are a remarkably beneficial side-channel for overcoming the localization challenge.
- We present how, with prior knowledge gained by reverse engineering the scan path, sensitive data can be extracted from SFFs even if the scan test mode is disabled.
- This research unveils valuable insights into the potential vulnerabilities associated with scan chain structures, thereby contributing to the advancement of secure DfT structures.

Thank you!

Question?