TECHNISCHE UNIVERSITÄT BERLIN

Unveiling Sensitive Data through Optical Scan Chain Probing

Tuba KIYAN | HARRIS Workshop
tuba.kiyan@tu-berlin.de

18. March 2025

SECT

Outline

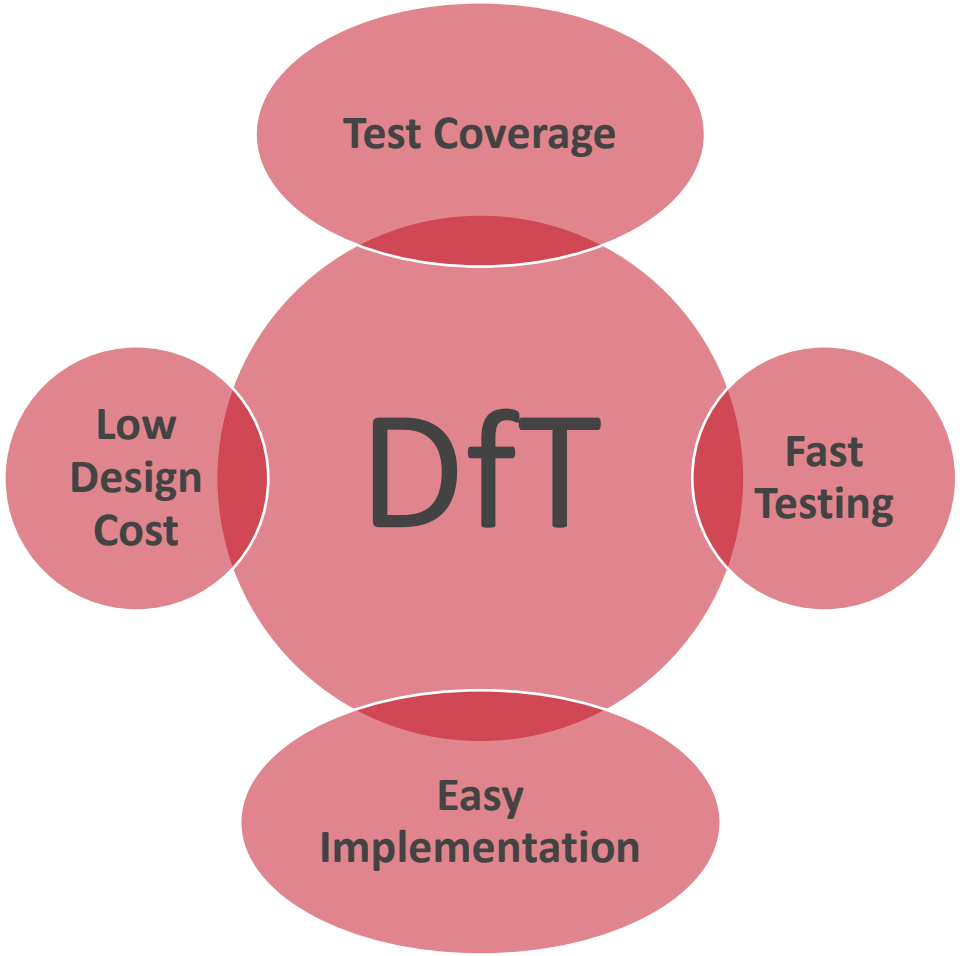
- Background
- Attacker’s Approach
- Results
  - Data Extraction from an SPI-to-USB Bridge
  - Breaking the Scan-chain Locking on an FPGA

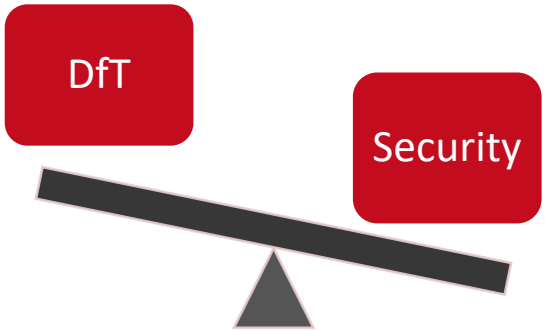
Motivation

Evaluation of threats that combine scan chain and optical probing attacks

- Leverage scan chain operation to reverse engineer the physical position of a register to overcome the localization complexity.
- Optical probing attacks to break scan chain obfuscation.
- Extraction of data from SFFs in normal mode even if the access to the scan chain is restricted or disabled.
- Neither the netlist nor the GDS file are required.

Design for Testing (DfT)

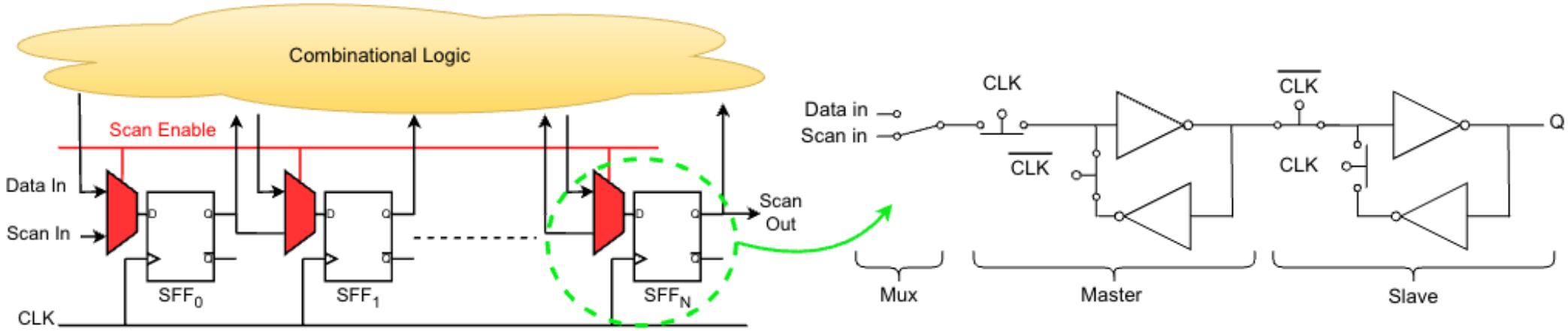




.

- It is generally implemented in an ASIC design and is inserted prior to place and route.
- It can be used to perform functional testing and to detect manufacturing defects.
- 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 is 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. After that, the device is put into normal mode for one or two clk cycles and finally the scan pattern is shifted out in test mode.
- 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.
- This makes it a portal for hackers.

Security vs. Design for Test

Scan Chain Side - Channel Attacks

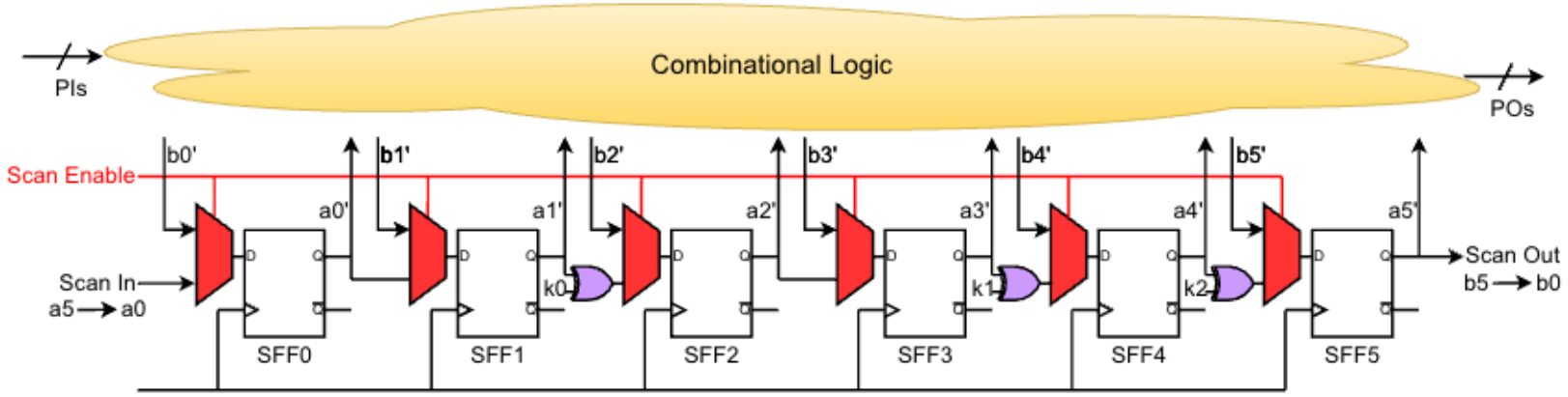
An adversary can gain access to the system and do the following:

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

Countermeasures

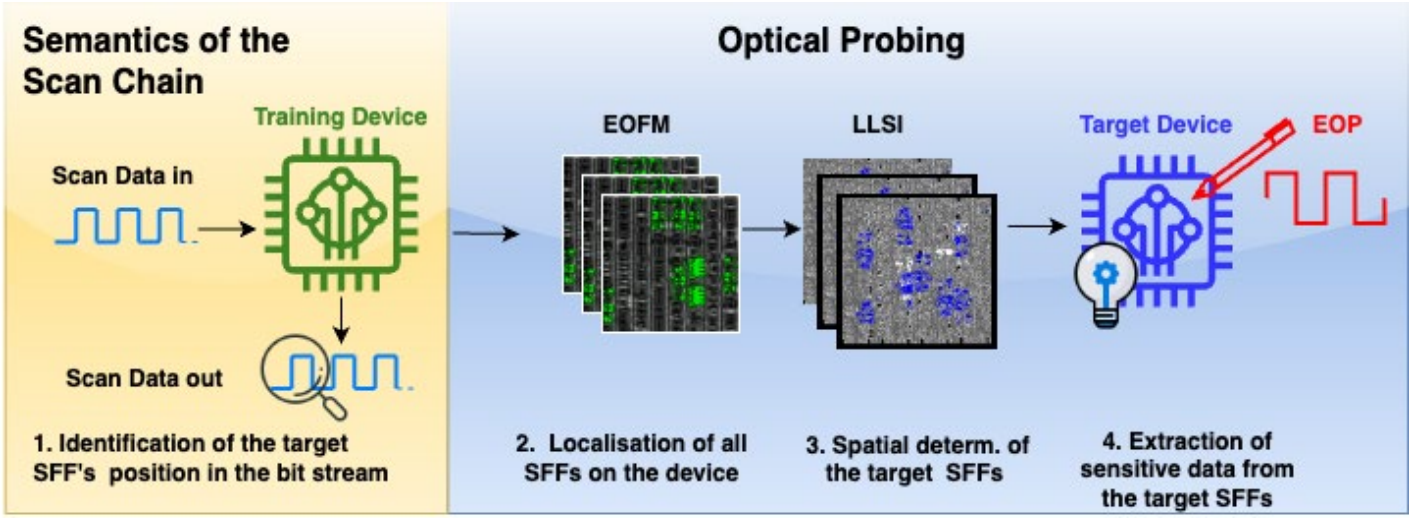
- Disabling or restricting the scan access
- Resetting the SFFs' content while switching between normal and test mode
- Advanced industrial application techniques → scan compression
- Obfuscation → Scan - Locking

Background
Scan Chain Locking



- 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



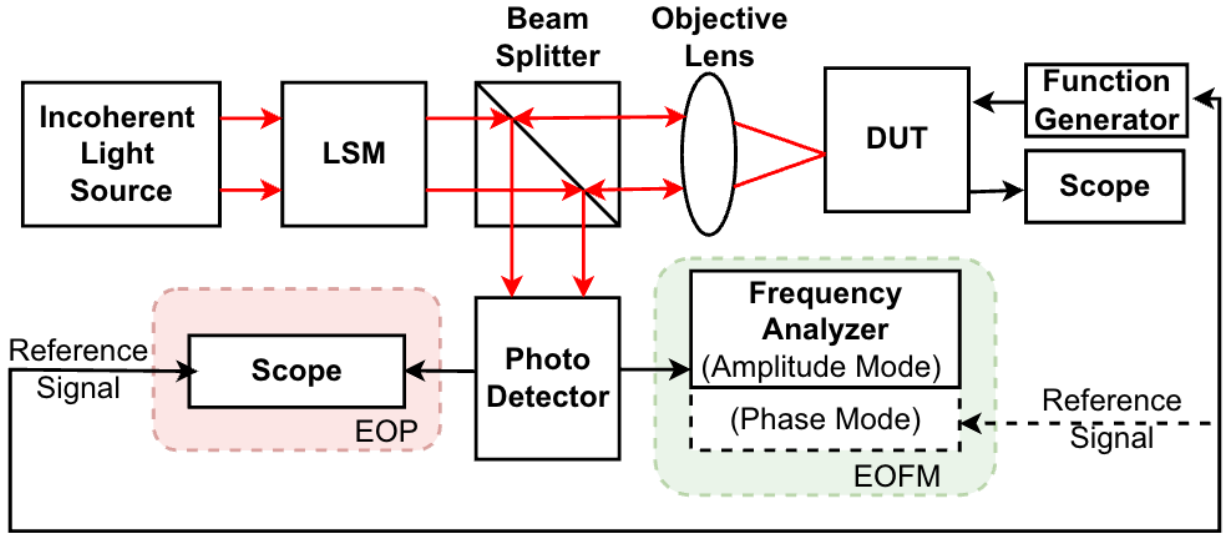
1. Decoding the Scan Path Semantics
2. The spatial localization of all SFFs
3. Localisation of the target SFFs on the chip
4. Extraction of sensitive data

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

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

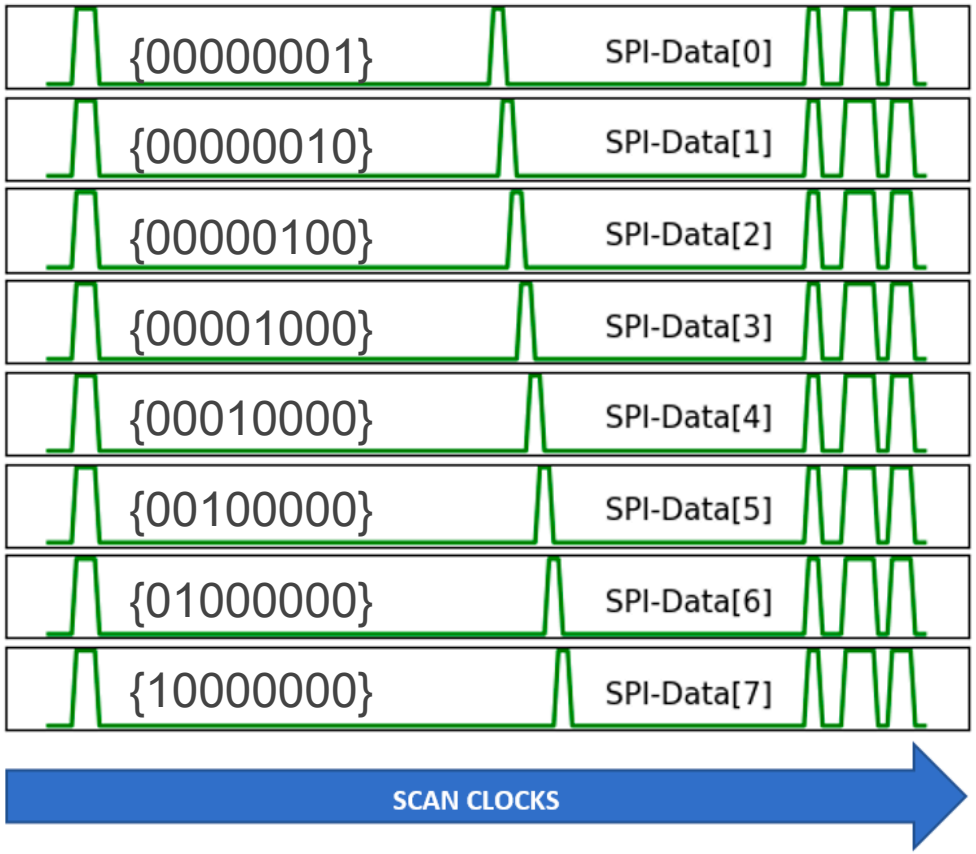
Optical Probing



- 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 the device
- LLSI → 2-D Logic State Mapping of a selected area

Verification of our Attack Approach on SPI Chip

1. Decoding the Scan Path Semantics



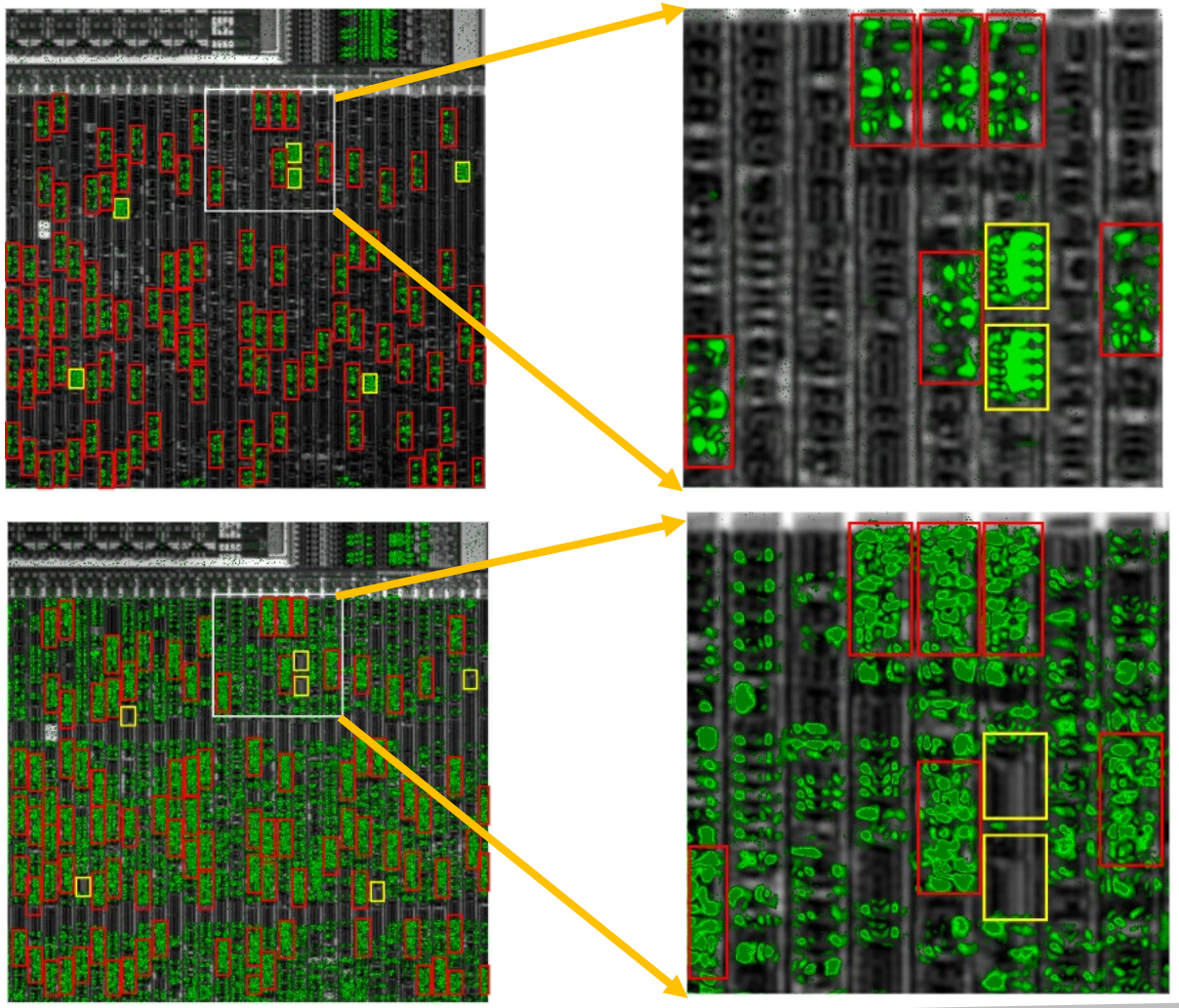
Identification of the order of the SFFs, storing the SPI-Data.

- 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.

2. Identification of physical locations of SFFs by EOFM

50X - no zoom

50X – 8x digital zoom



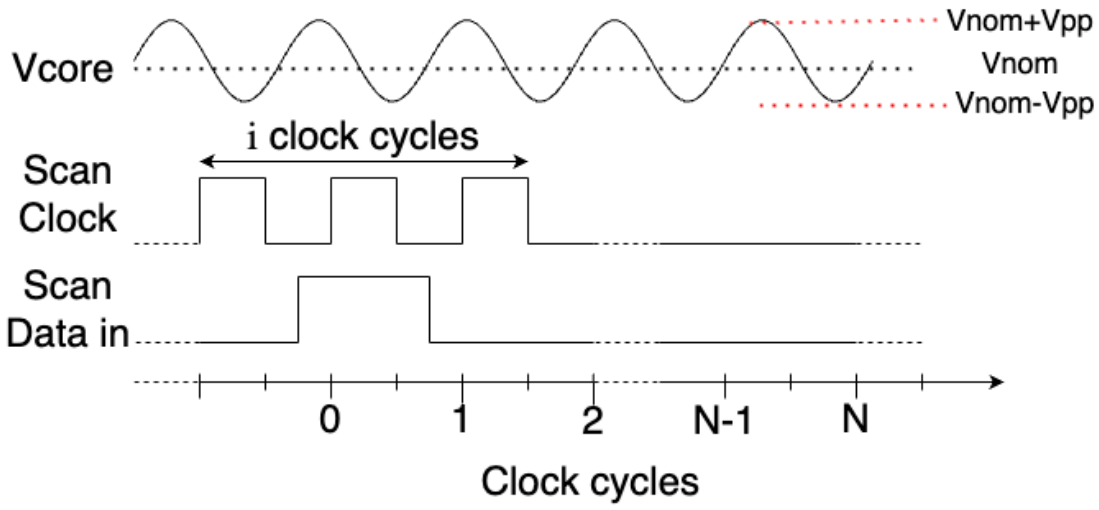
→ EOFM at clock freq.

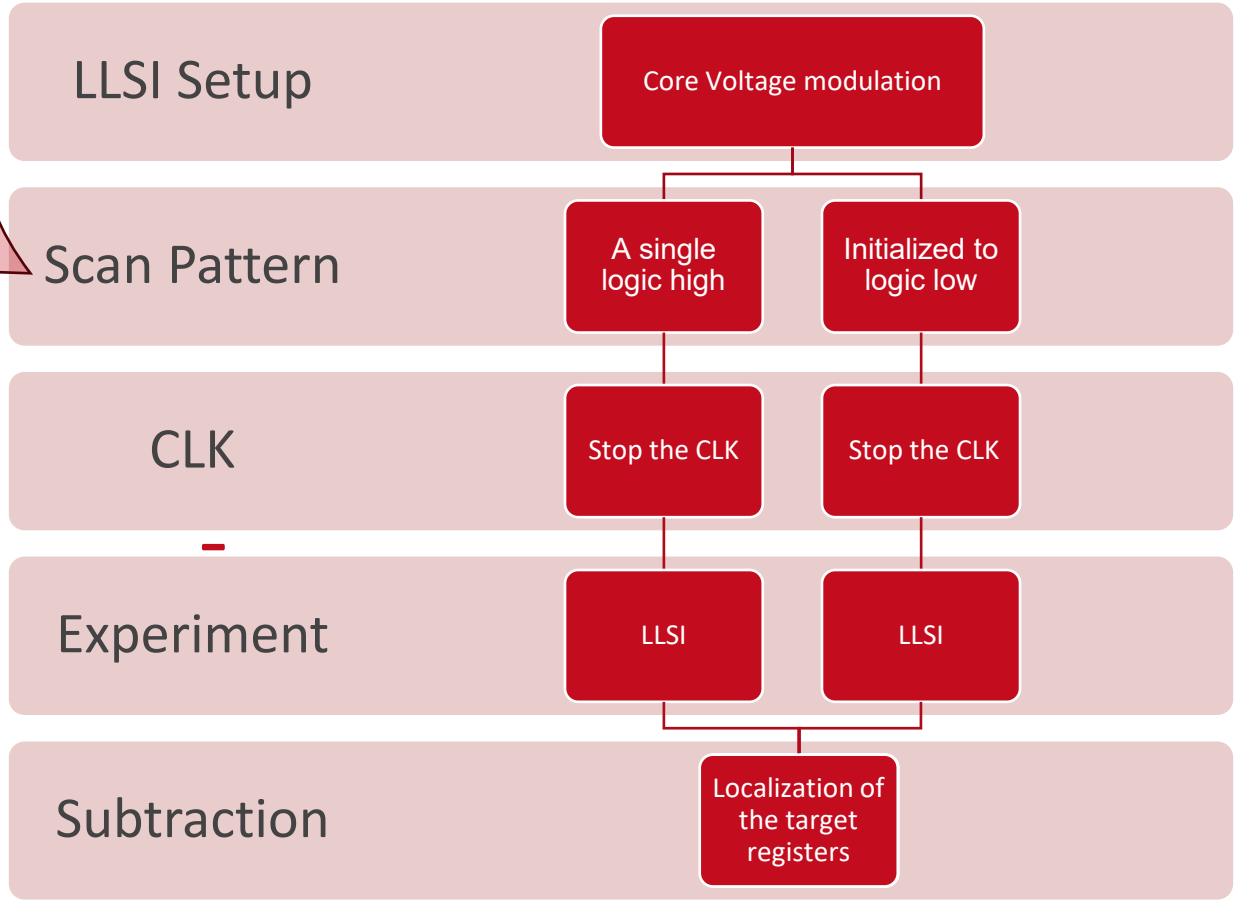
- Locations → modulating at the clock + the data frequencies candidates to be SFFs
- Highlighted in red

→ EOFM at scan data freq.

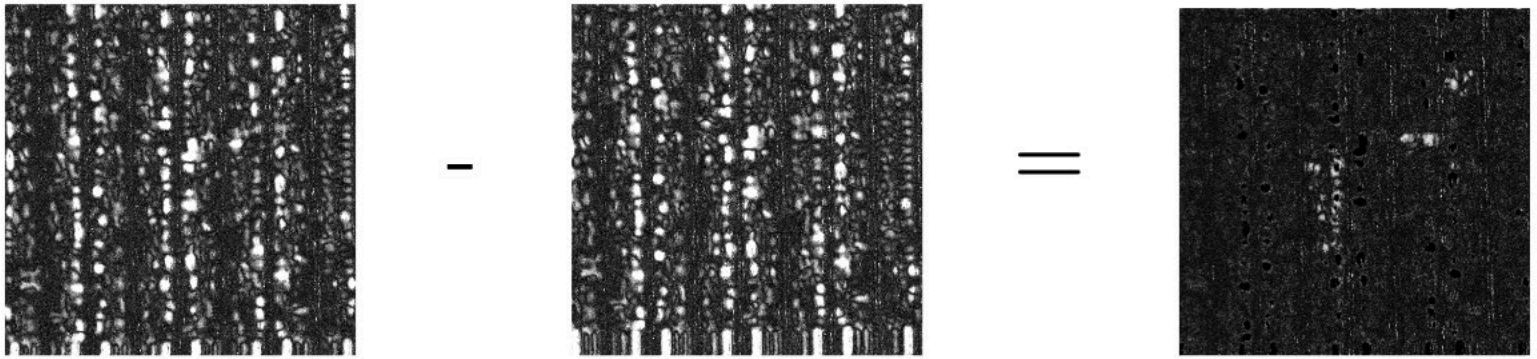
3. Localization of the target SFFs by LLSI

# of CLK cycles = the order of the target SFF





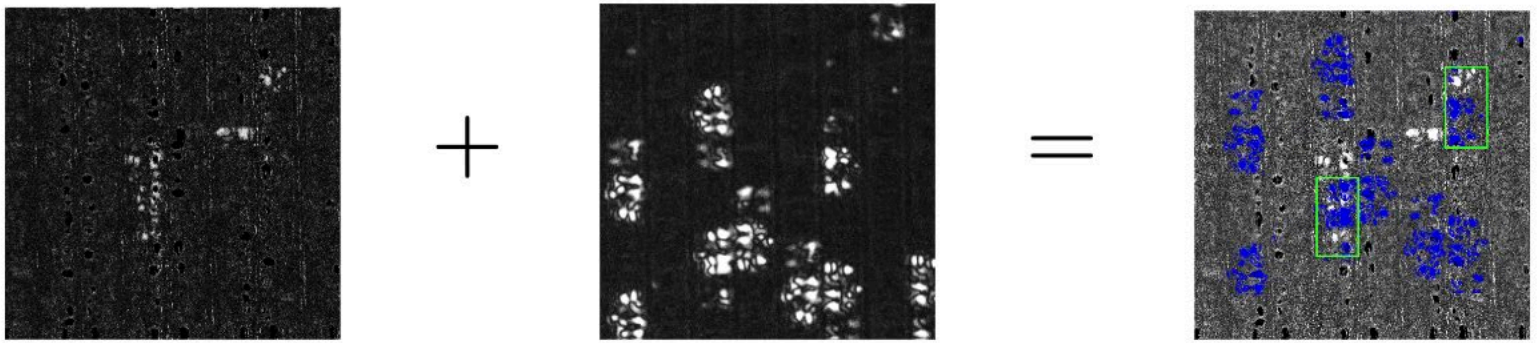
3. Identified positions of MOSI and SPI CLK registers



(a) Filled with logic low except target reg.

(b) All reg. filled with logic low

(c) Subtracted image

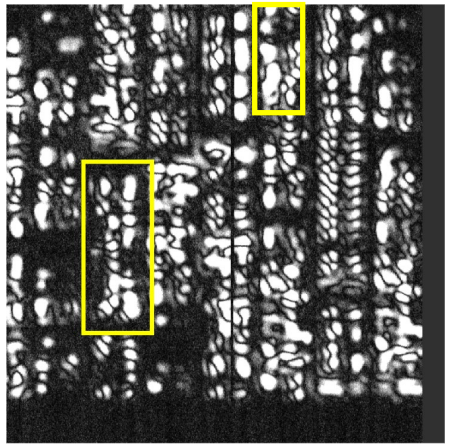


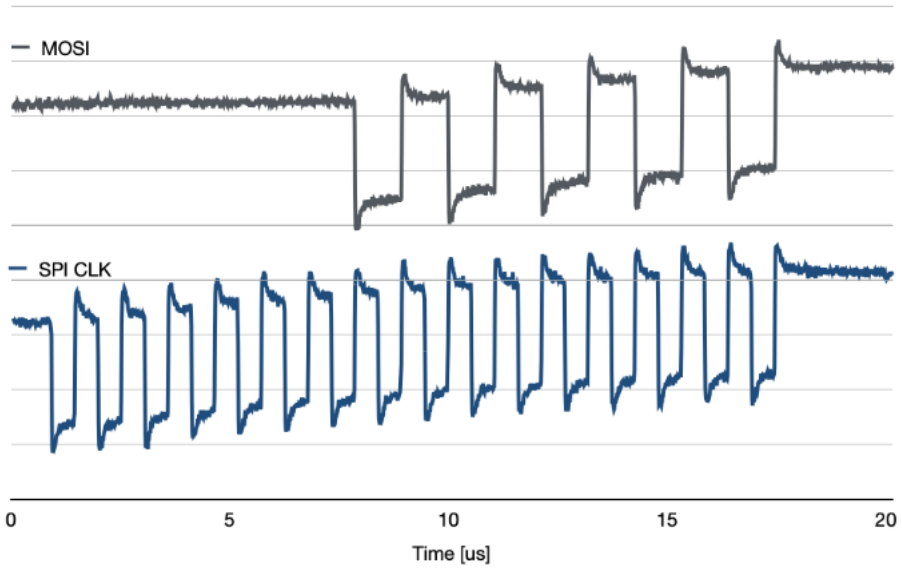
(d) Subtracted image

(e) Locations of the SFFs

(f) Superimposed image

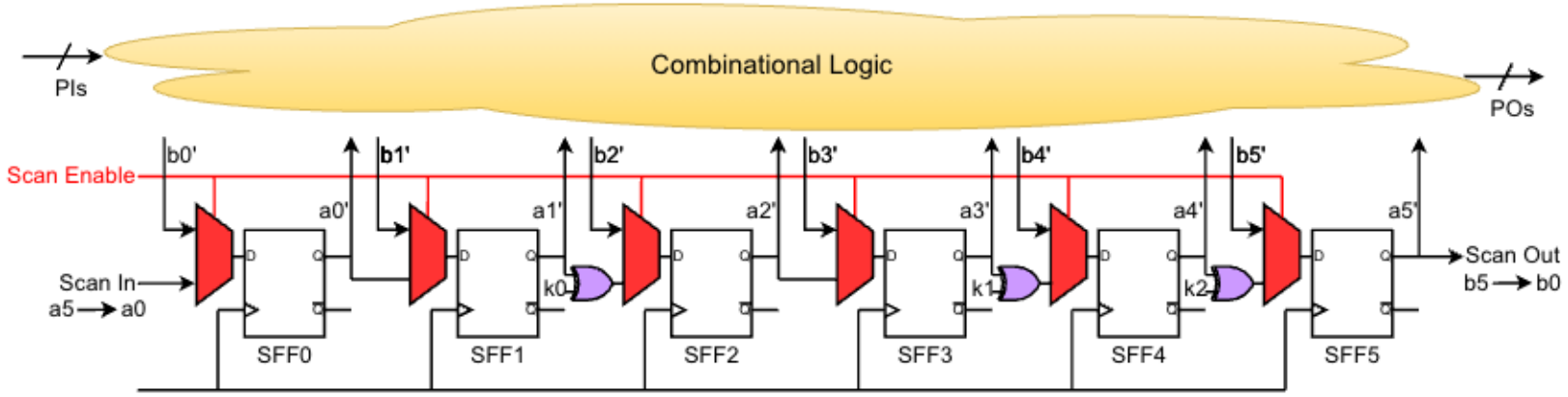
4. MOSI and SPI Clock Data Extraction in Normal Mode





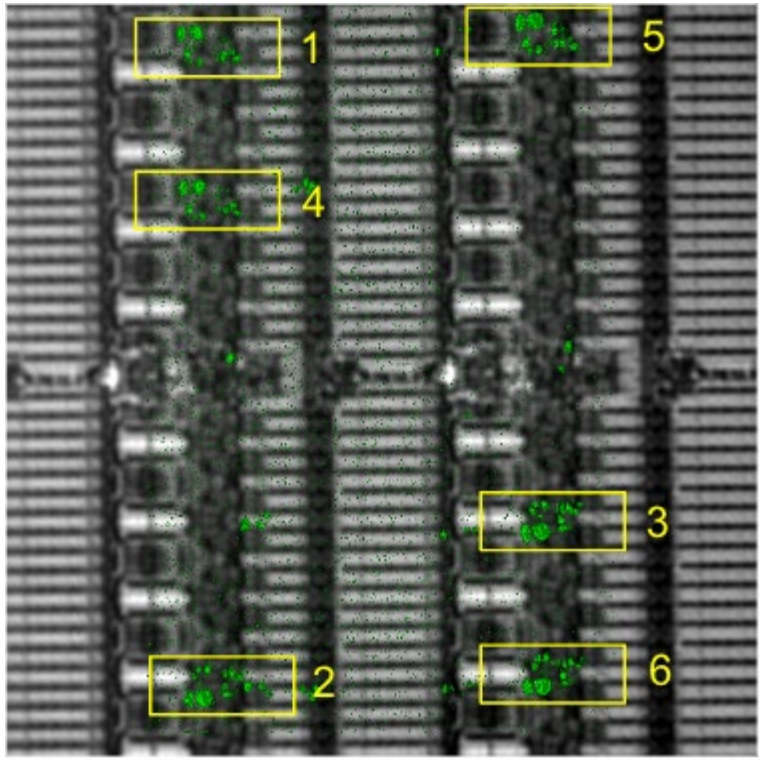
By using the EOP tool, we probe the location previously identified to be the MOSI and SPI CLK, we successfully reconstruct the data transmitted via USB which is found to be `0xFD55`.

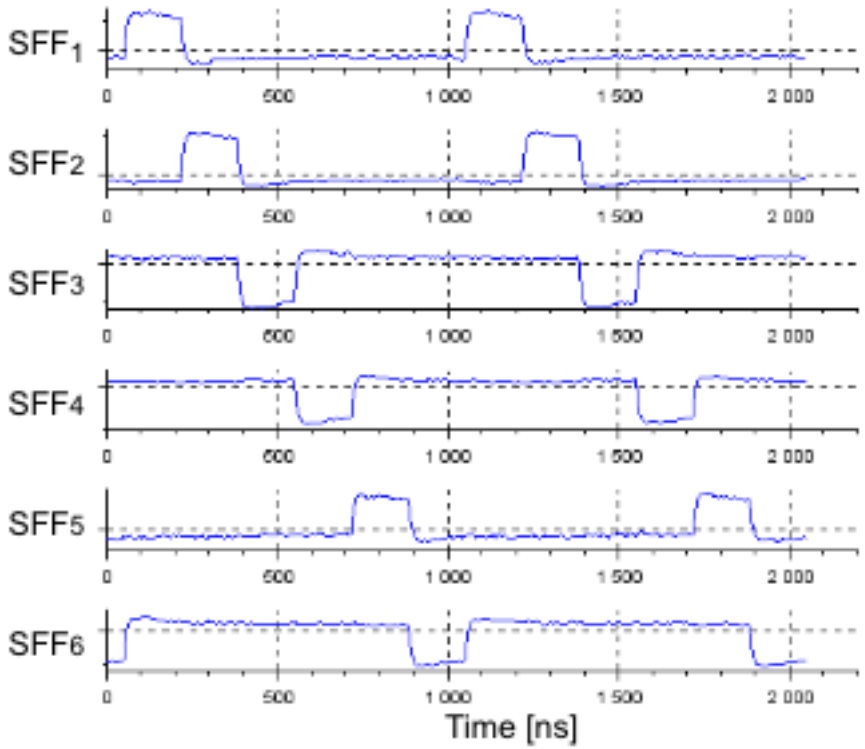
Breaking the Locked Scan Chain Implementation on FPGA



- 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 90^0phase 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

- Scan chains can be exploited to overcome the localization challenge.
- 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!