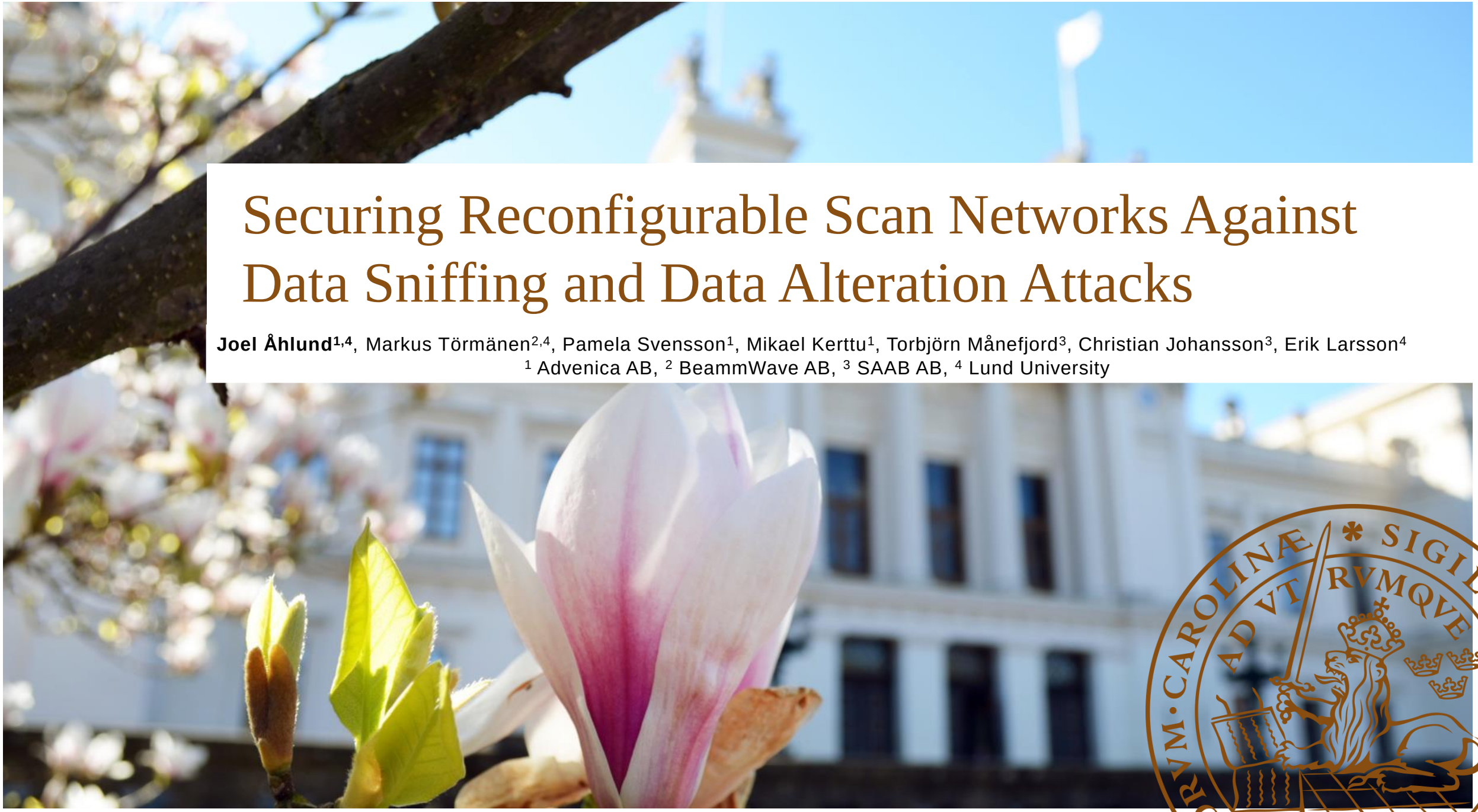


Securing Reconfigurable Scan Networks Against Data Sniffing and Data Alteration Attacks

Joel Åhlund[1,4], Markus Törmänen[2,4], Pamela Svensson[1], Mikael Kerttu[1], Torbjörn Månefjord[3], Christian Johansson[3], Erik Larsson[4]

[1] Advenica AB, [2] BeammWave AB, [3] SAAB AB, [4] Lund University

Motivation

- Modern circuits require a lot of on-chip test features, referred to as instruments, which could be imported from third parties.
- Instruments may be integrated into a reconfigurable scan network, for easy and efficient access.
- There is a risk that instruments in the network are malicious and may perform data sniffing and data alteration attacks.
- We propose a security measure, realized in the microarchitecture of Segment Insertion Bit (SIB) components in the reconfigurable scan network, to protect against data sniffing and data alteration attacks from malicious instruments.

LUND UNIVERSITY

Outline

- **Introduction**
- Related work
- Our solution

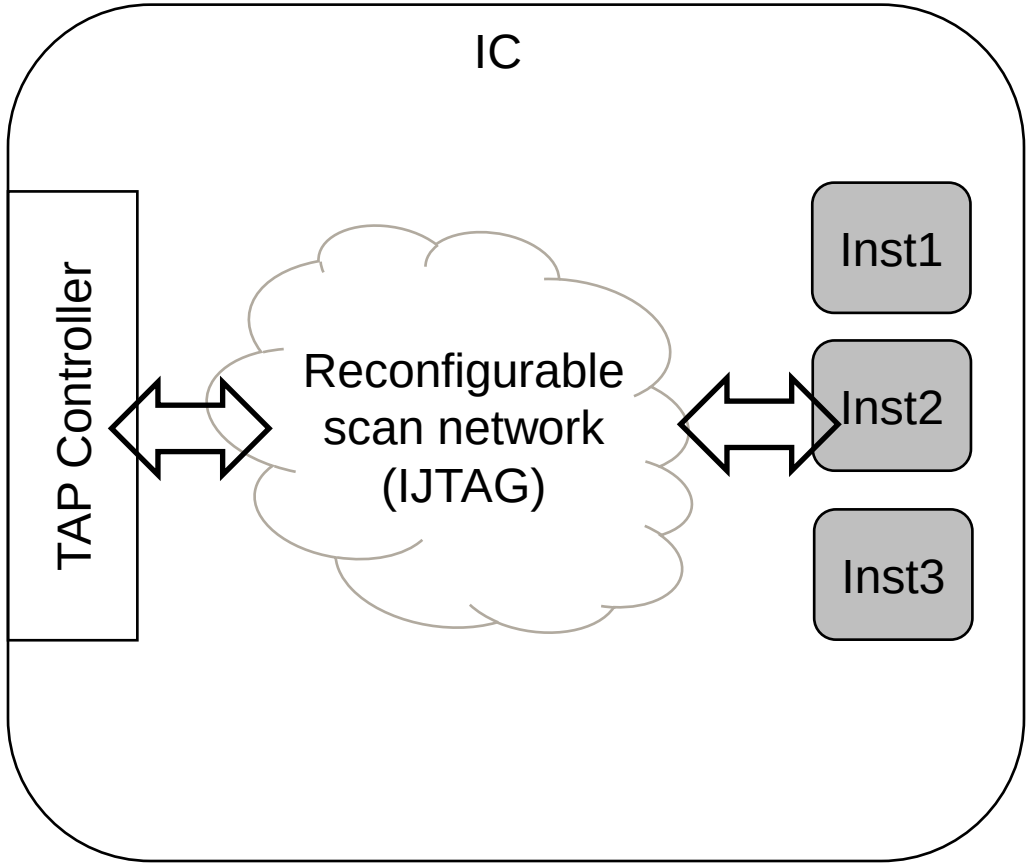
On-Chip Instruments

- On-chip test features (instruments) are used for post-production test, configuration, monitoring, …
  - Example: Built-In Self Test (BIST) instruments, sensors
- Many instruments may be needed
  - Example: If one on-chip instrument can ensure correct function of 10K transistors, a chip with 1 billion transistors needs 100K instruments
- Reconfigurable scan network, IEEE Std. 1687 (IJTAG), allows for efficient and flexible access to many on-chip instruments

LUND UNIVERSITY

IEEE Std. 1687 (IJTAG)

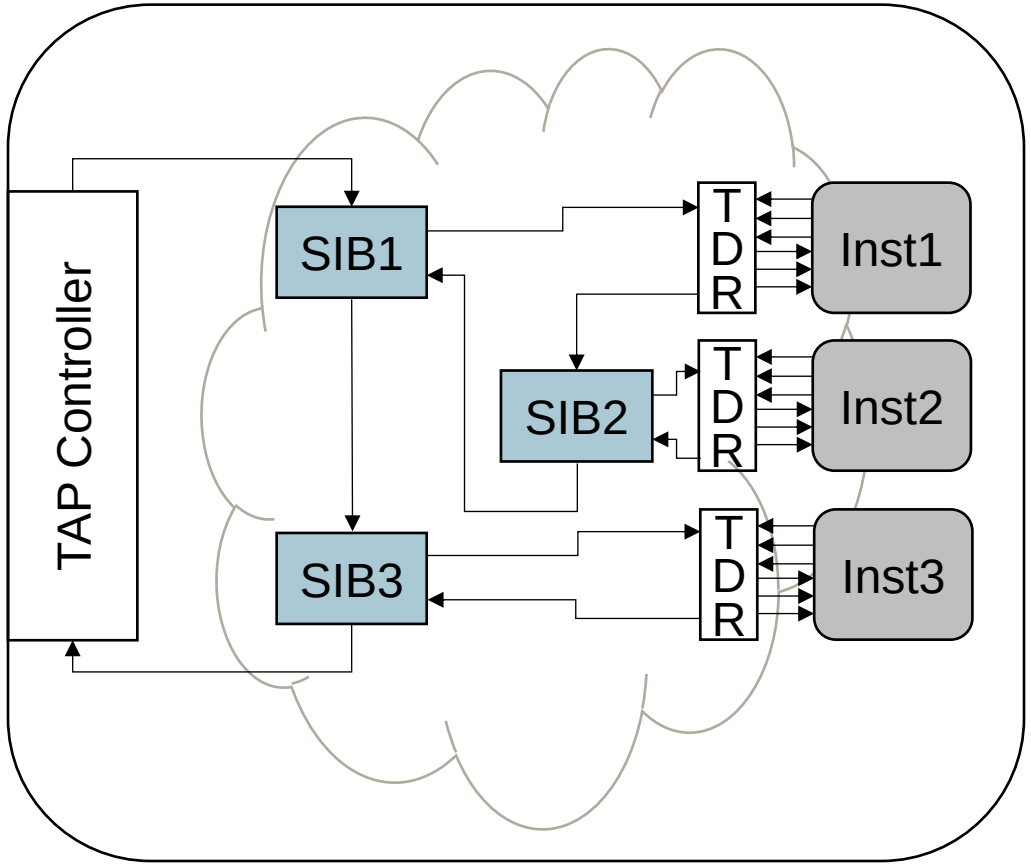
- Test Access Port (TAP) controller
- Reconfigurable Scan Network



LUND UNIVERSITY

IEEE Std. 1687 (IJTAG)

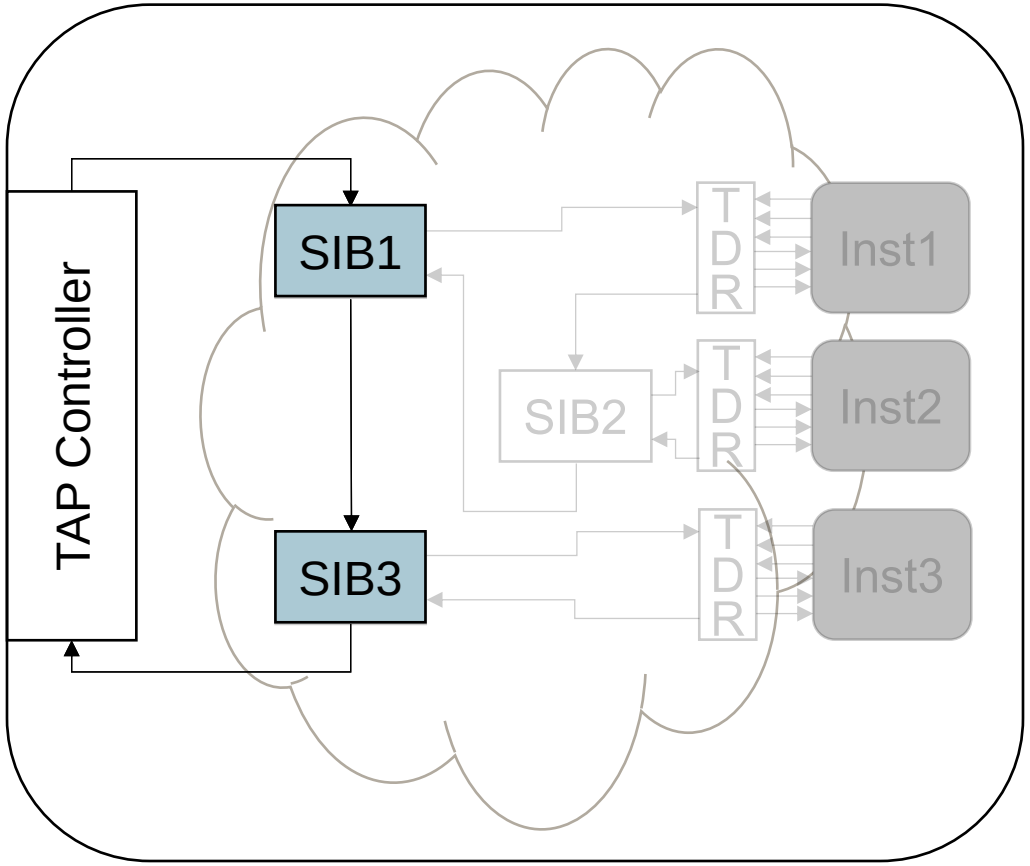
- Test Access Port (TAP) controller
- Reconfigurable Scan Network
- Test Data Register (TDR)
- Segment Insertion Bit (SIB)



LUND UNIVERSITY

IEEE Std. 1687 (IJTAG)

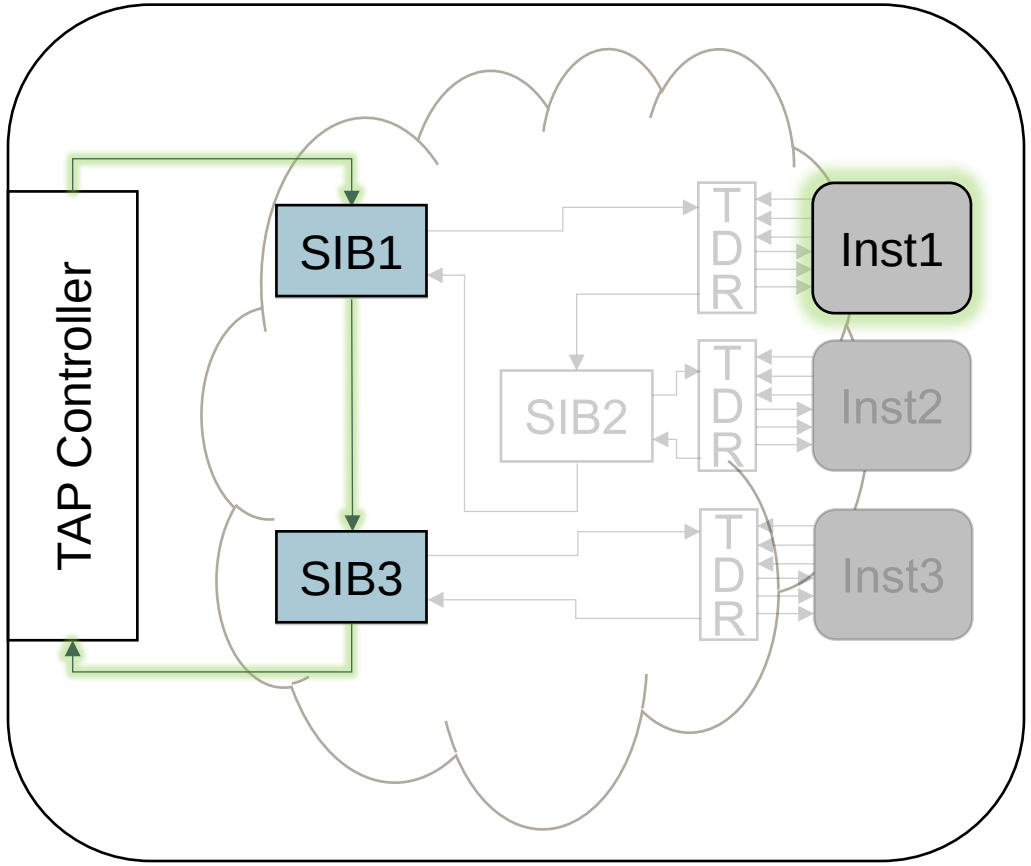
- Capture, Shift and Update (CSU) cycle



LUND UNIVERSITY

IEEE Std. 1687 (IJTAG)

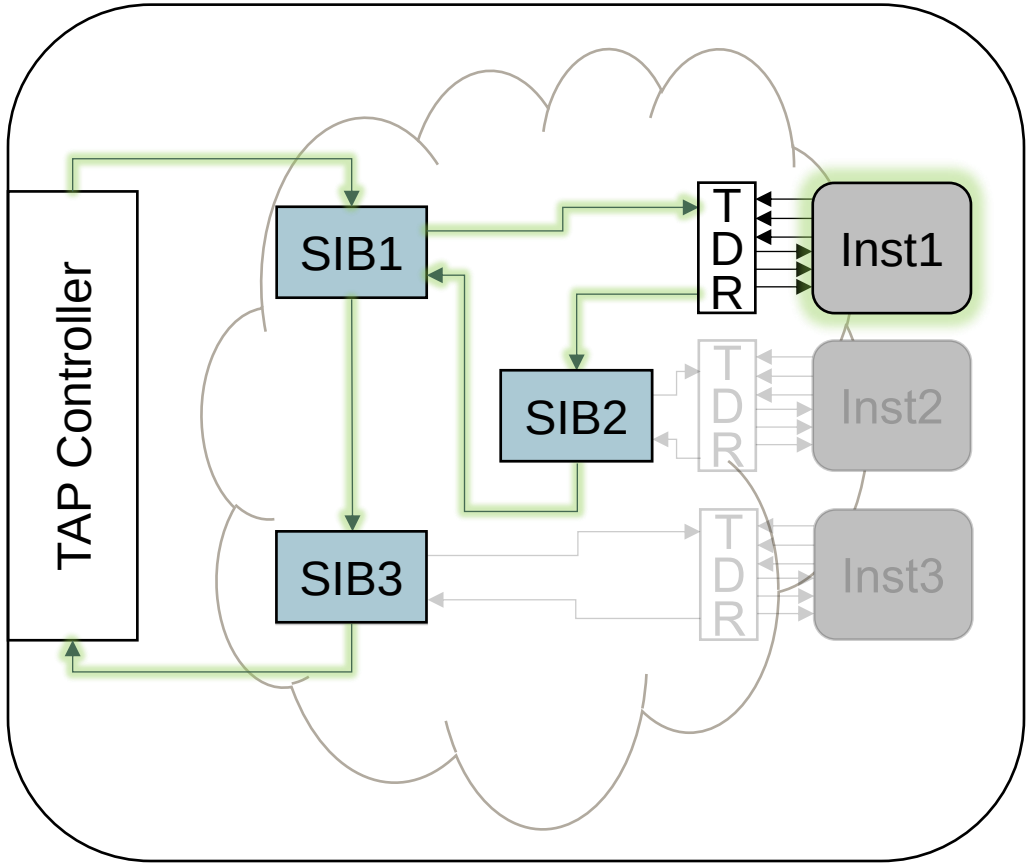
- Capture, Shift and Update (CSU) cycle
- Active scan path



LUND UNIVERSITY

IEEE Std. 1687 (IJTAG)

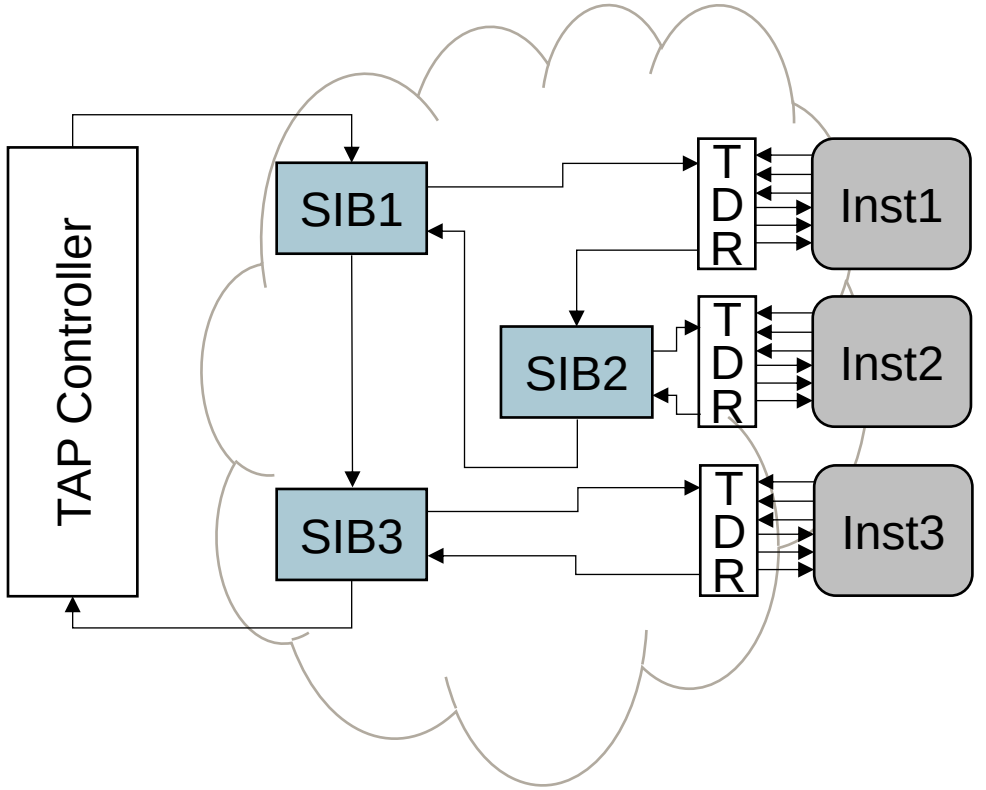
- Capture, Shift and Update (CSU) cycle
- Active scan path



LUND UNIVERSITY

Security Risks in IJTAG

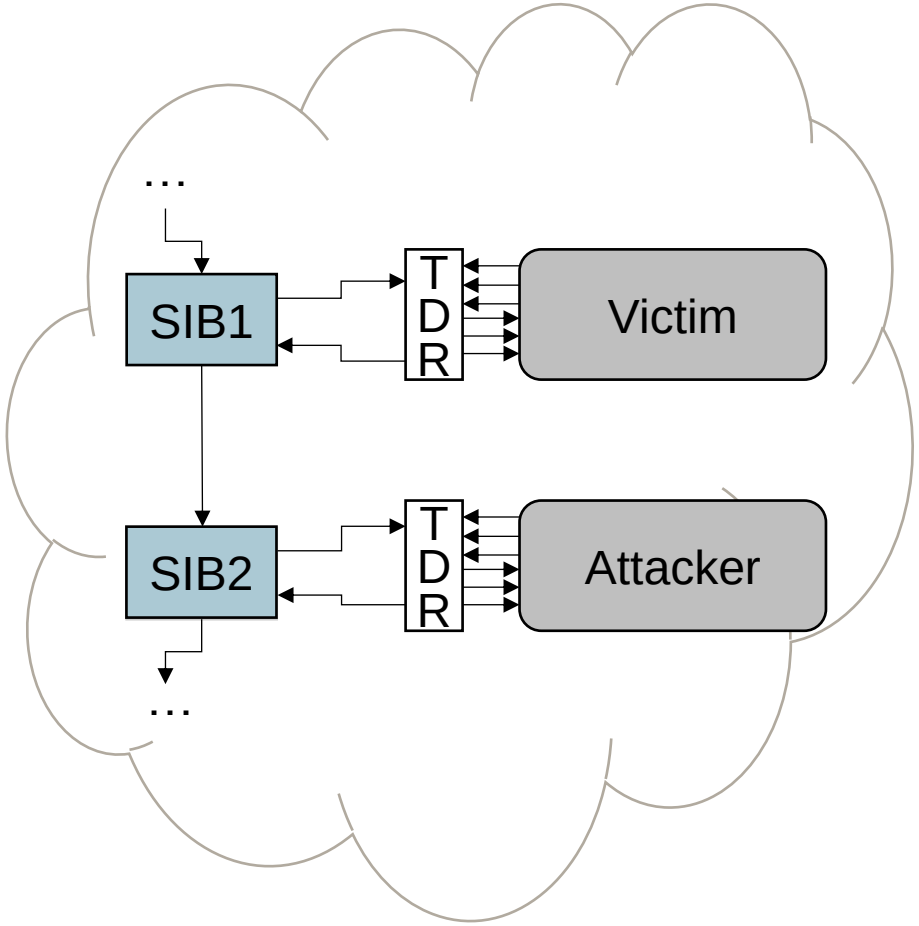
- Powerful instruments in the IJTAG network
- Instruments may be imported from untrusted third parties
- Risk of hardware trojans in third party instruments
- Data sniffing and data alteration attacks



LUND UNIVERSITY

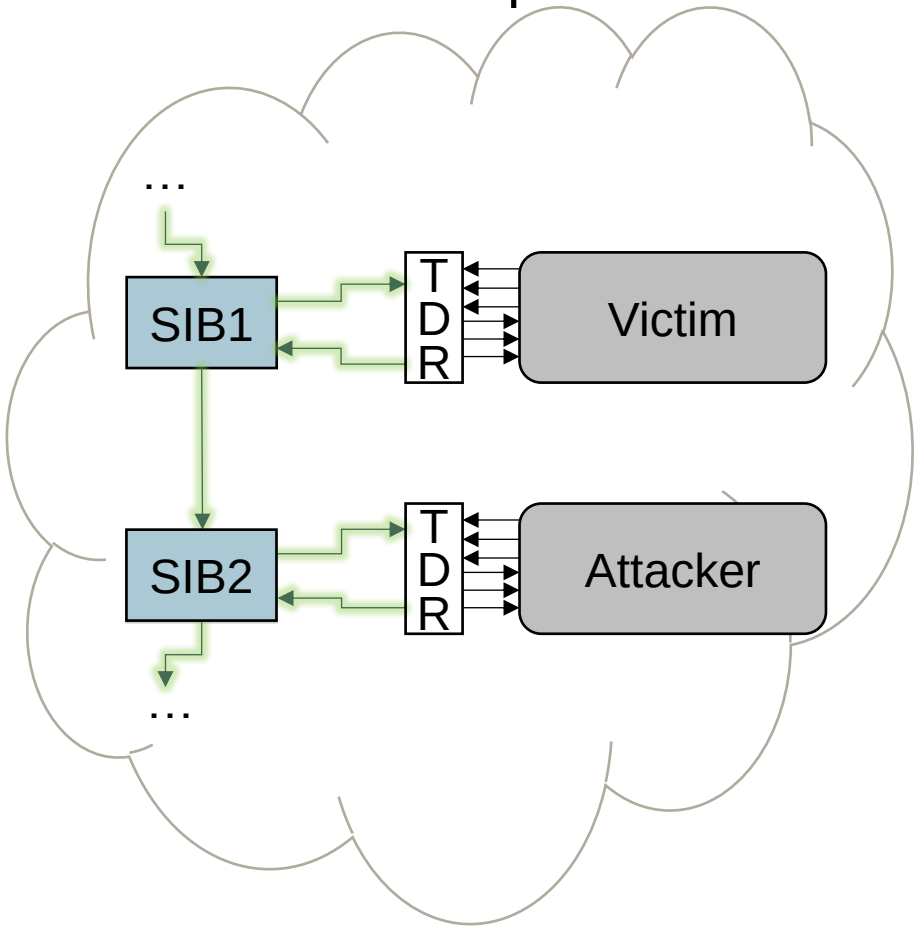
Data Sniffing and Alteration Attacks

- Example: One victim and one attacker



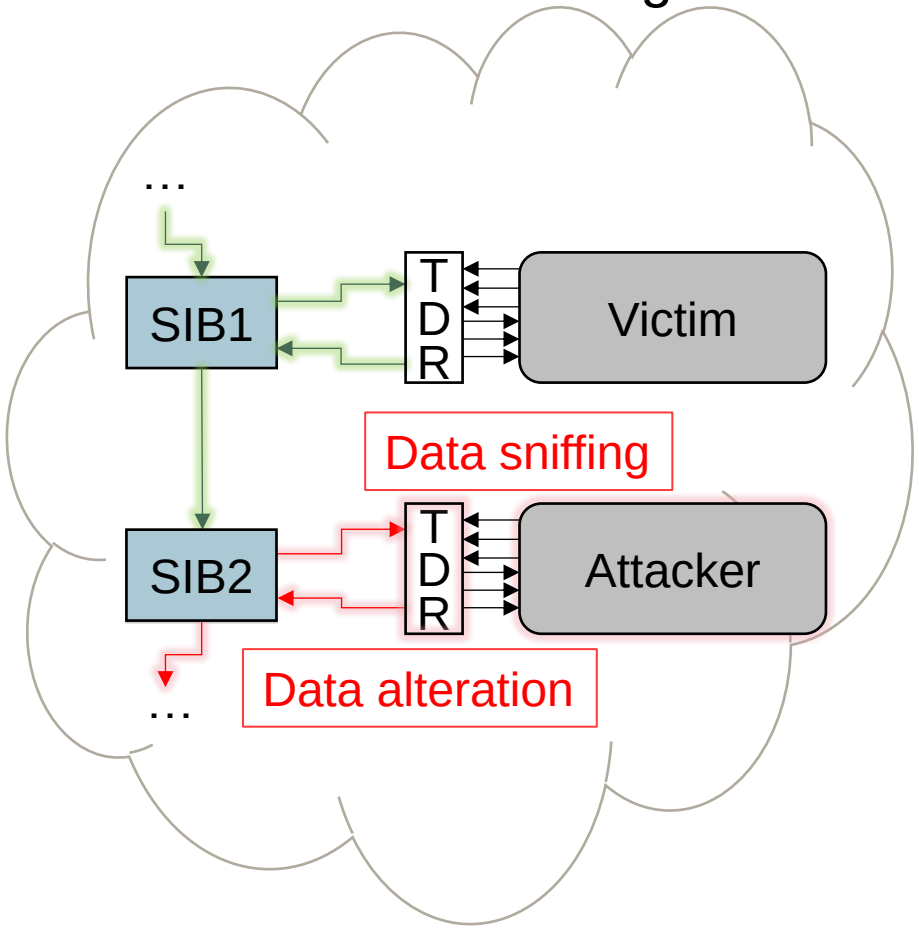
Data Sniffing and Alteration Attacks

- Both SIB1 and SIB2 in the active scan path



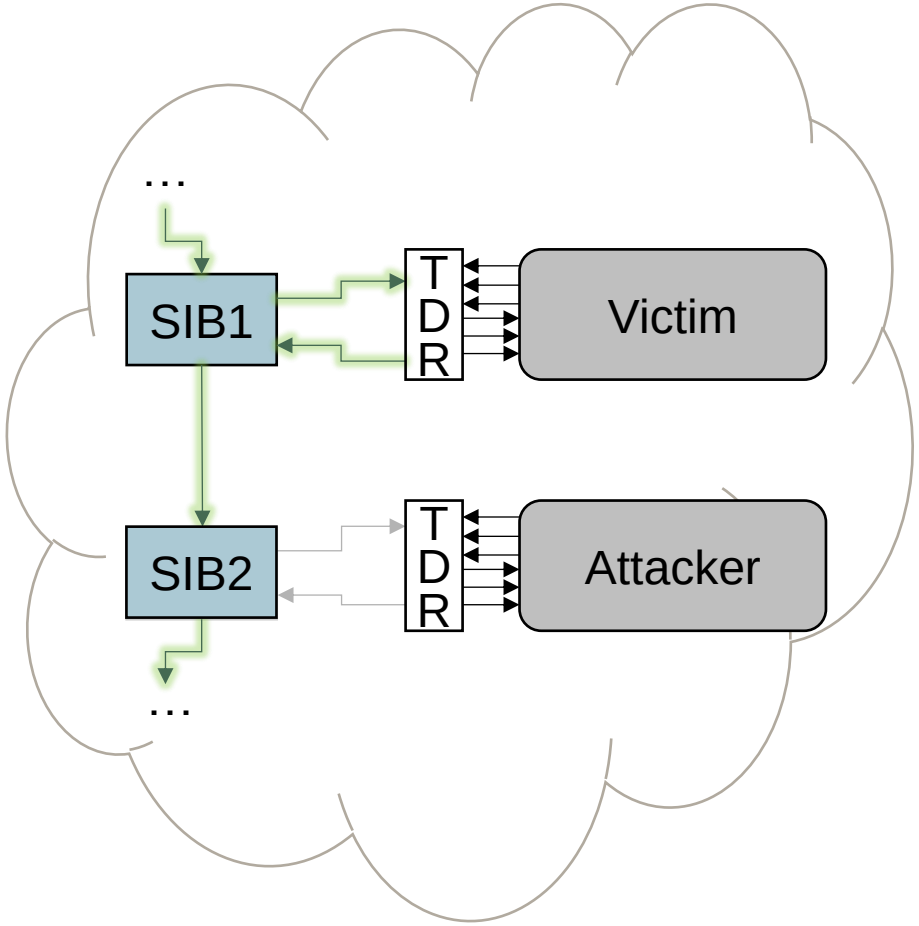
Data Sniffing and Alteration Attacks

- Data shifted through Attacker → Data sniffing and data alteration attacks



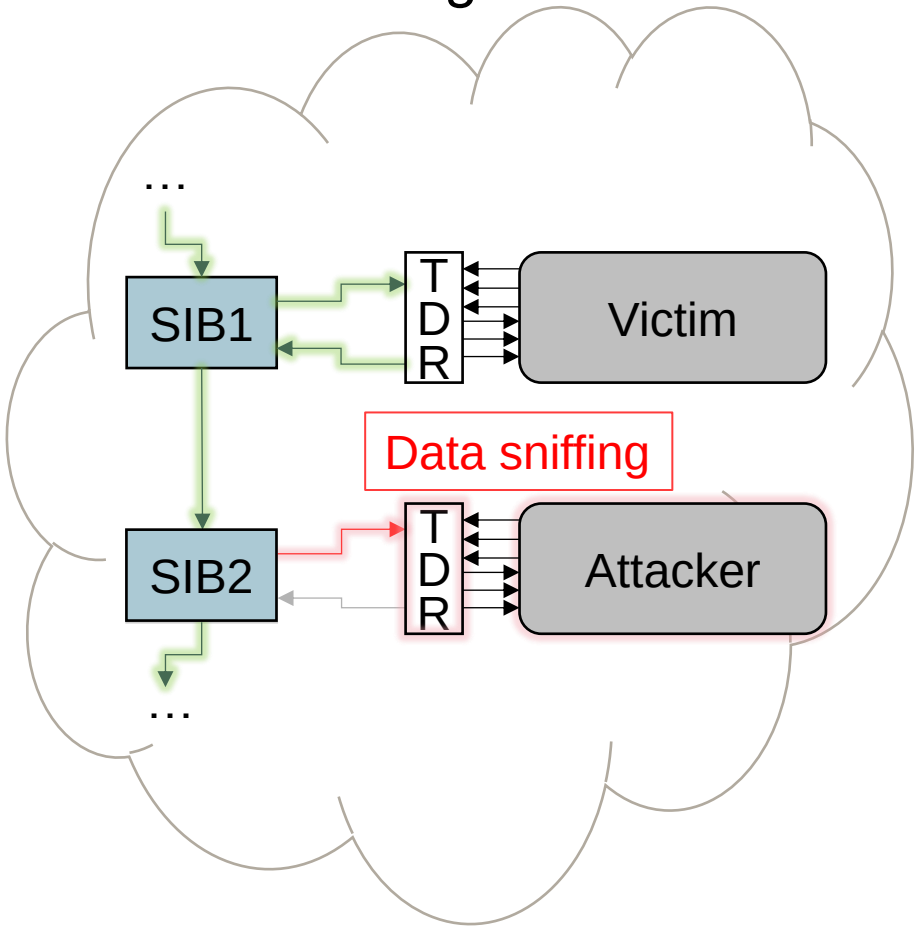
Data Sniffing and Alteration Attacks

- **Reconfigurable** Scan Network→ Close SIB2 → Avoid attacker?



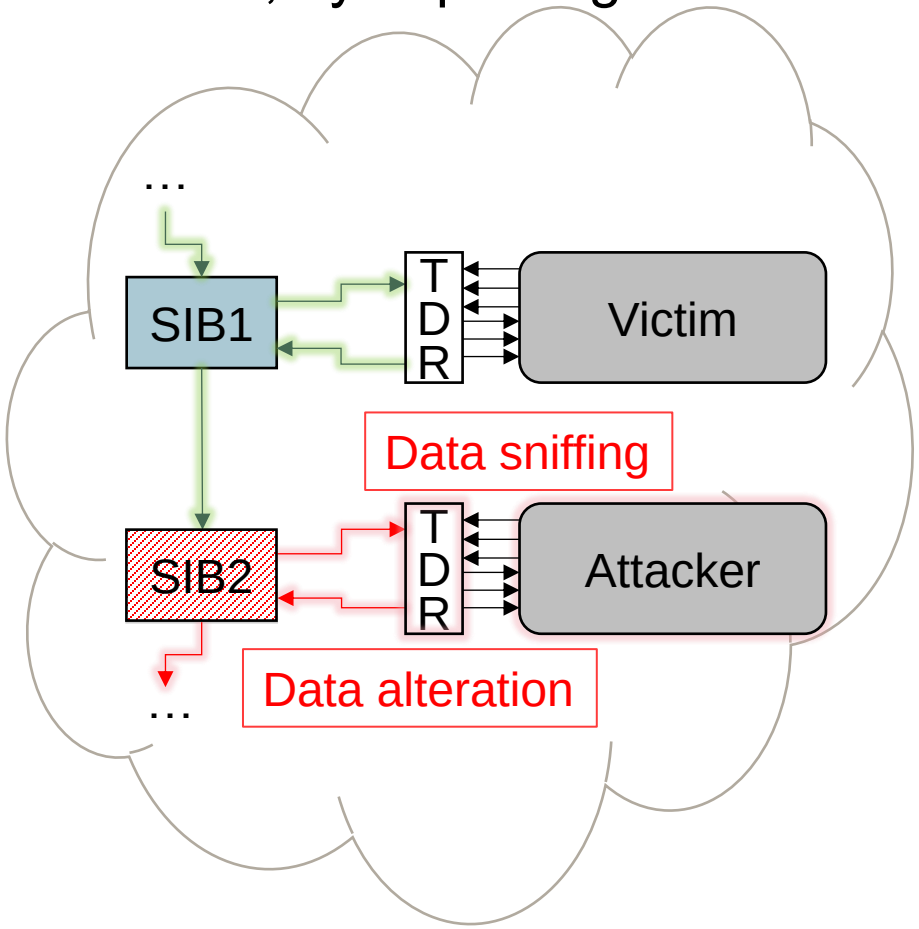
Data Sniffing and Alteration Attacks

- Attacker can still perform data sniffing attacks …



Data Sniffing and Alteration Attacks

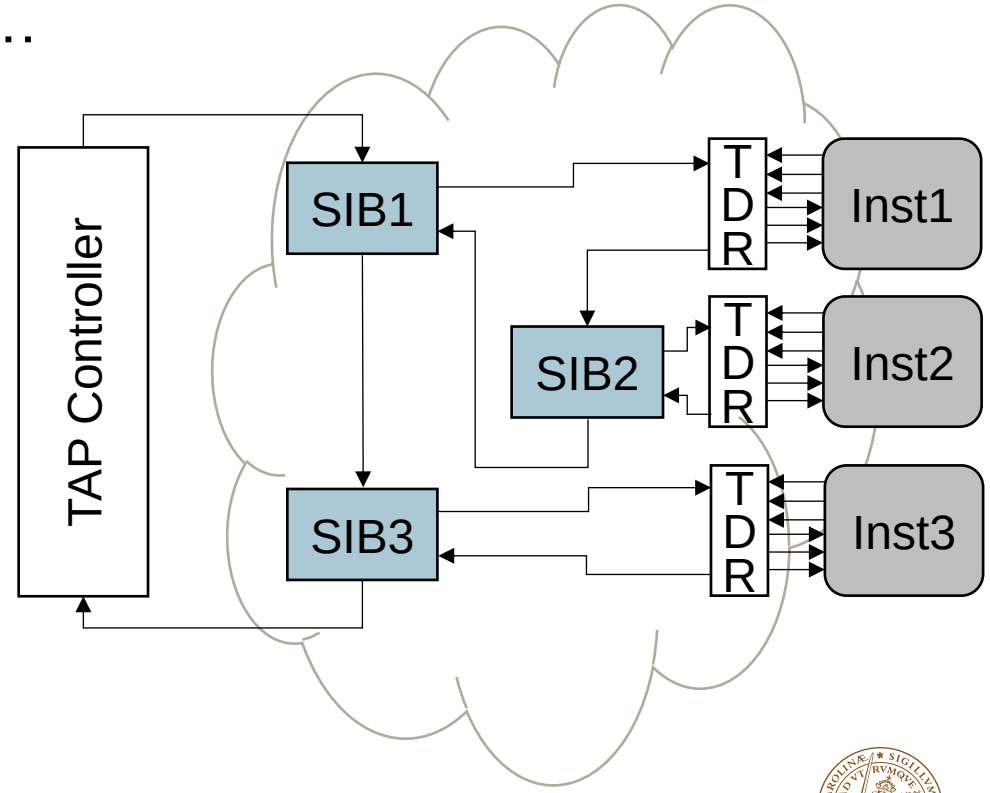
- … and data alteration attacks, by exploiting SIB2



LUND UNIVERSITY

Attacks in IJTAG

- Read sensitive information
  - Device configuration, keys, test results, …
- Falsify test responses
- Change the IJTAG network configuration
  - Access other instruments
- Issue commands to other instruments
  - MBIST, debug, …



LUND UNIVERSITY

Requirements

- Security against data sniffing and data alteration attacks
- Compliance with IEEE Std. 1687 (IJTAG)
- Scalability (many instruments)
- Easily integrated into an EDA tool
- Low test time overhead
- Low area overhead

IJTAG Benchmark[1]	Nr. of SIBs	Nr. of TDRs	Area (post-synthesis)
TreeFlat	12	11	13 734 μm^2
Mingle	10	8	35 854 μm^2
TrapOrFlap	11	8	149 089 μm^2
TreeBalanced	43	44	453 789 μm^2

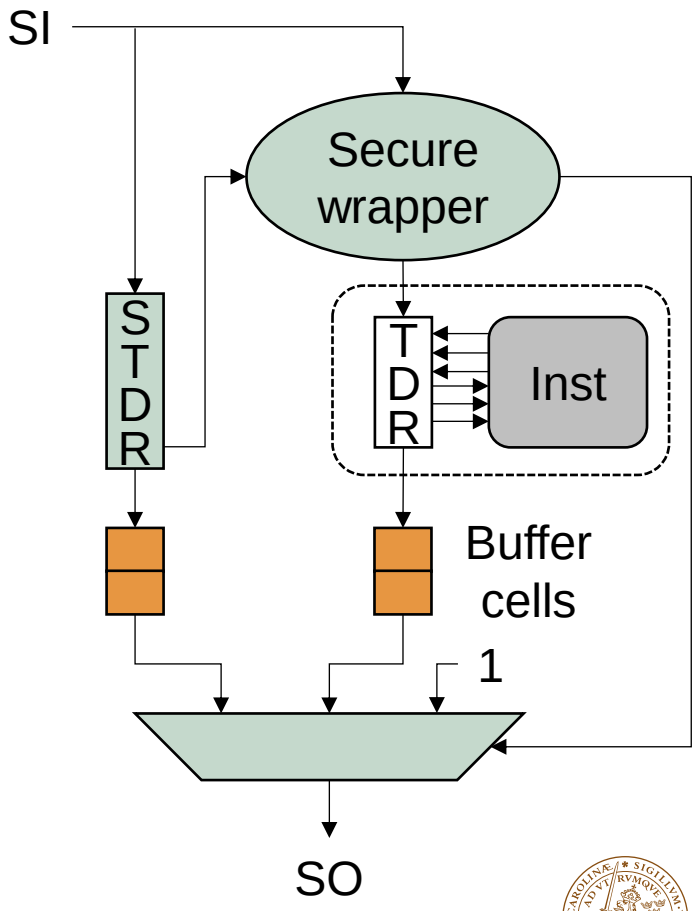
1. A. Tšertov, *et al.*, "*A suite of IEEE 1687 benchmark networks*"

Outline

- Introduction
- **Related work**
- Our solution

Related Work – IJTAG Security

- Shadow TDR (STDR) with secure wrapper[2]

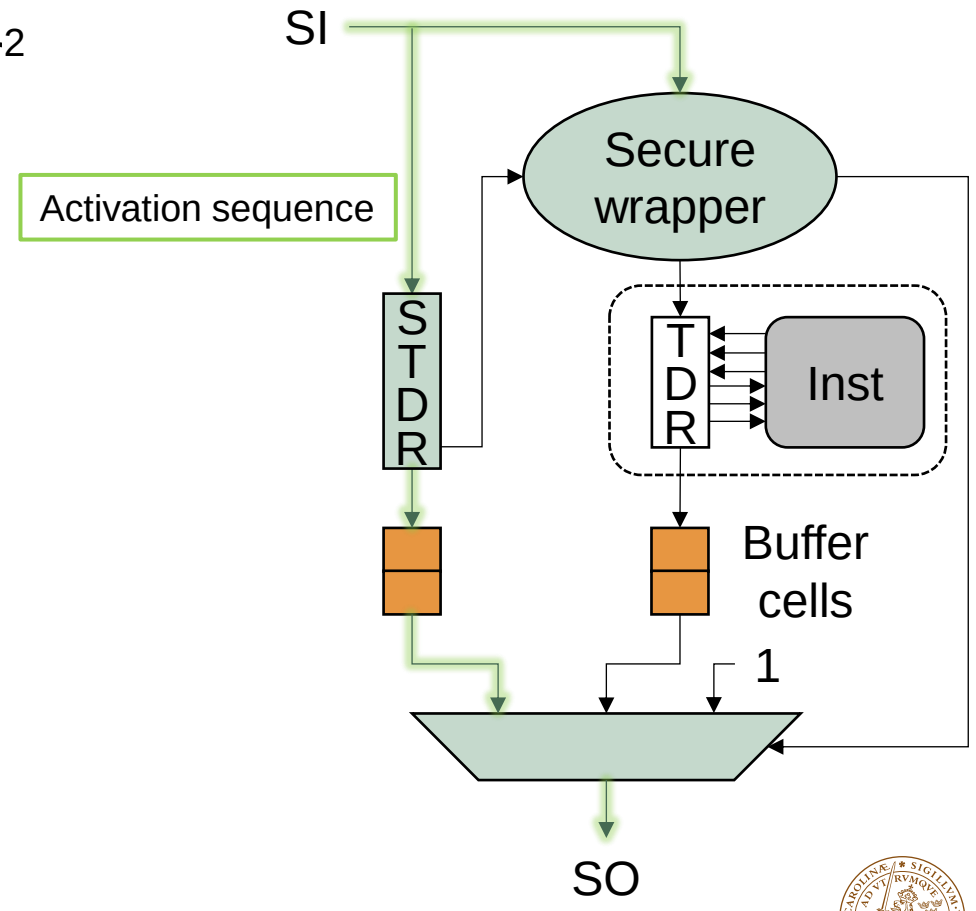


2. R. Elnaggar, *et al.*, "*Security against data sniffing and alteration attacks in IJTAG*"

LUND UNIVERSITY

Related Work – IJTAG Security

- Shadow TDR (STDR) with secure wrapper[2]

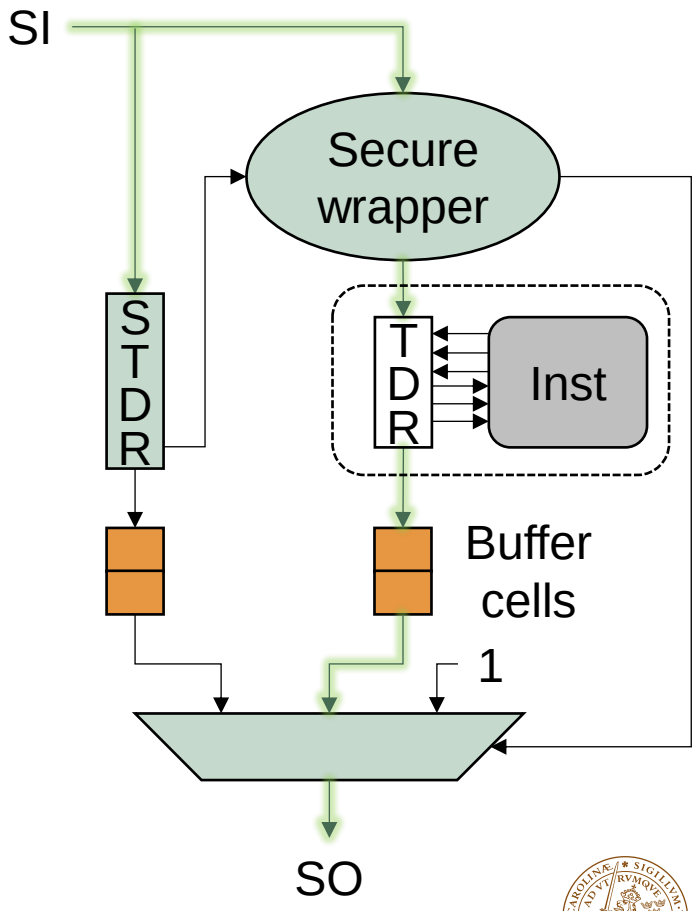


2. R. Elnaggar, *et al.*, "*Security against data sniffing and alteration attacks in IJTAG*"

LUND UNIVERSITY

Related Work – IJTAG Security

- Shadow TDR (STDR) with secure wrapper[2]



2. R. Elnaggar, *et al.*, "*Security against data sniffing and alteration attacks in IJTAG*"

LUND UNIVERSITY

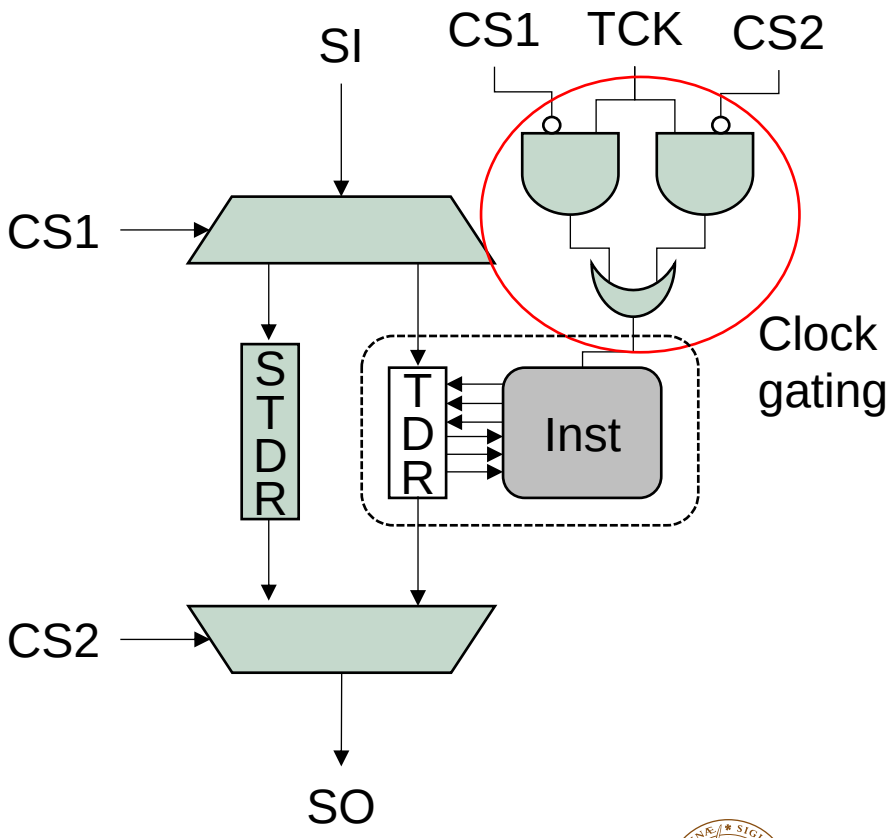
Requirements	STDR with secure wrapper[2]
IJTAG compliance?	Yes
Scalability issues?	None
IJTAG EDA tool?	No
Test time overhead?	Activation sequence
Area overhead?	Large

IJTAG Benchmark[1]	STDR with secure wrapper[2]
TreeFlat	92.46 %
Mingle	96.79 %
TrapOrFlap	-
TreeBalanced	73.91 %

1. A. Tšertov, *et al.*, "*A suite of IEEE 1687 benchmark networks*"
2. R. Elnaggar, R. Karri, K. Chakrabarty, "*Security against data sniffing and alteration attacks in IJTAG*"
3. S.-J. Wang, *et al.*, "*Improving IJTAG test efficiency and security*"

Related Work – IJTAG Security

- STDR with control signals[3]



3. S.-J. Wang, *et al.*, "*Improving IJTAG test efficiency and security*"

LUND UNIVERSITY

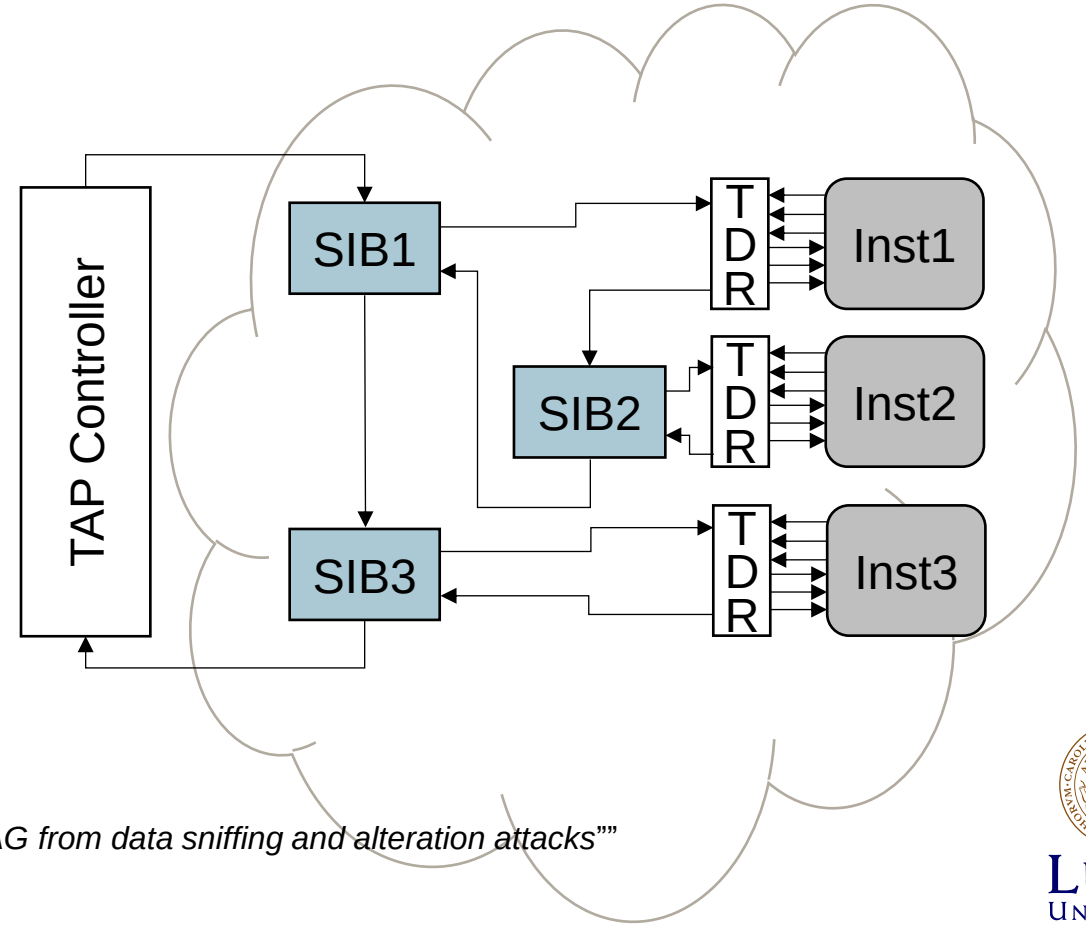
Requirements	STDR with secure wrapper[2]	STDR with control signals[3]
IJTAG compliance?	Yes	Yes
Scalability issues?	None	Many control signals
IJTAG EDA tool?	No	No
Test time overhead?	Activation sequence	No
Area overhead?	Large	Large

IJTAG Benchmark[1]	STDR with secure wrapper[2]
TreeFlat	92.46 %
Mingle	96.79 %
TrapOrFlap	-
TreeBalanced	73.91 %

1. A. Tšertov, *et al.*, "*A suite of IEEE 1687 benchmark networks*"
2. R. Elnaggar, R. Karri, K. Chakrabarty, "*Security against data sniffing and alteration attacks in IJTAG*"
3. S.-J. Wang, *et al.*, "*Improving IJTAG test efficiency and security*"

Related Work – IJTAG Security

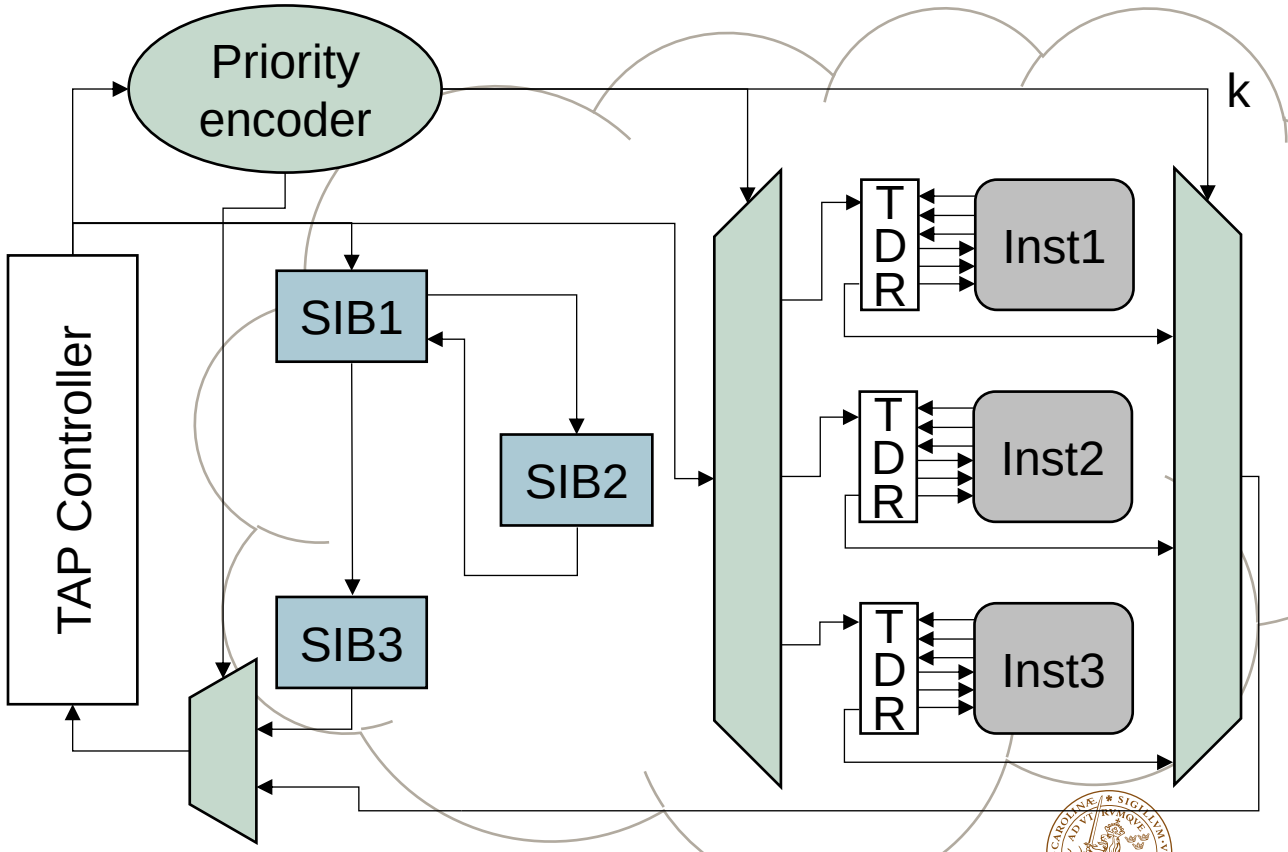
- Priority encoder[4]



4. A. Riaz, *et al.*, "*On protecting IJTAG from data sniffing and alteration attacks*""

Related Work – IJTAG Security

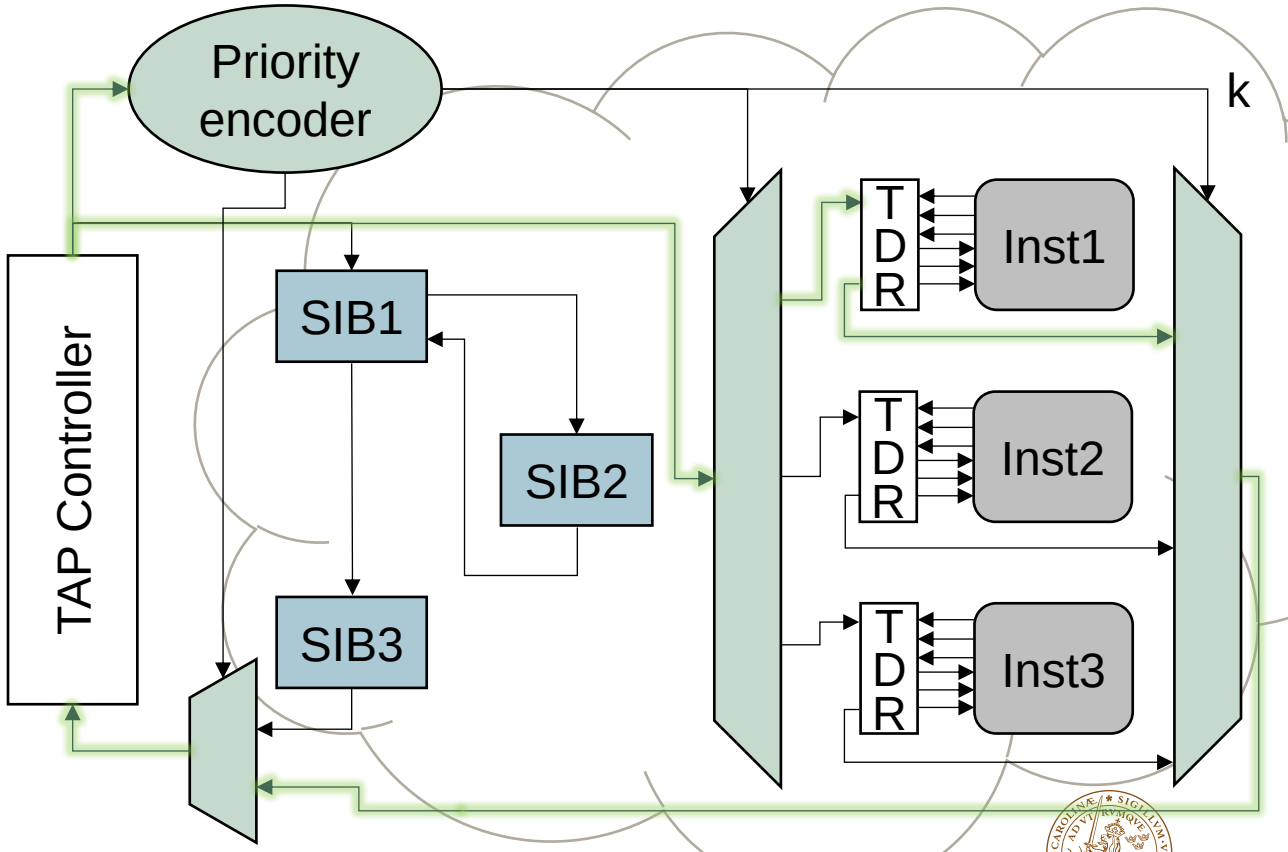
- Priority encoder[4]



4. A. Riaz, *et al.*, "*On protecting IJTAG from data sniffing and alteration attacks*"

Related Work – IJTAG Security

- Priority encoder[4]



4. A. Riaz, *et al.*, "*On protecting IJTAG from data sniffing and alteration attacks*"

LUND UNIVERSITY

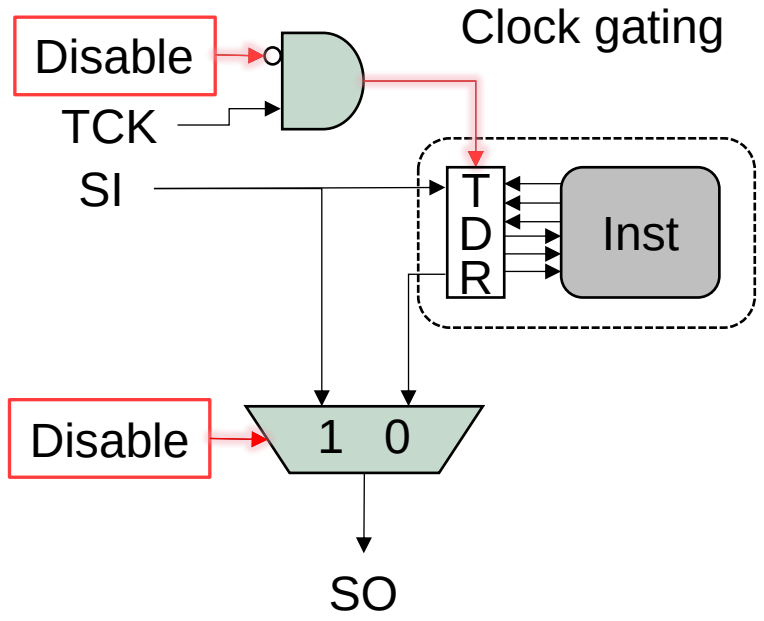
Requirements	STDR with secure wrapper[2]	STDR with control signals[3]	Priority encoder[4]
IJTAG compliance?	Yes	Yes	Yes, re-arrange test data
Scalability issues?	None	Many control signals	None
IJTAG EDA tool?	No	No	No
Test time overhead?	Activation sequence	No	No parallel access
Area overhead?	Large	Large	Medium

IJTAG Benchmark[1]	STDR with secure wrapper[2]	Priority encoder[4]
TreeFlat	92.46 %	12.40 %
Mingle	96.79 %	15.08 %
TrapOrFlap	-	-
TreeBalanced	73.91 %	1.55 %

1. A. Tšertov, *et al.*, "*A suite of IEEE 1687 benchmark networks*"
2. R. Elnaggar, R. Karri, K. Chakrabarty, "*Security against data sniffing and alteration attacks in IJTAG*"
3. S.-J. Wang, *et al.*, "*Improving IJTAG test efficiency and security*"
4. A. Riaz, G. Kumar, J. Tudu, S. Ahlawat, "*On protecting IJTAG from data sniffing and alteration attacks*"

Related Work – IJTAG Security

- Isolation scheme[5]



5. A. Das, N. A. Touba, "*A graph theory approach towards IJTAG security via controlled scan chain isolation*"

Requirements	STDR with secure wrapper[2]	STDR with control signals[3]	Priority encoder[4]	Isolation scheme[5]
IJTAG compliance?	Yes	Yes	Yes, re-arrange test data	Yes, manage control signals
Scalability issues?	None	Many control signals	None	Many control signals
IJTAG EDA tool?	No	No	No	No
Test time overhead?	Activation sequence	No	No parallel access	No
Area overhead?	Large	Large	Medium	Small

IJTAG Benchmark[1]	STDR with secure wrapper[2]	Priority encoder[4]	Isolation scheme[5]
TreeFlat	92.46 %	12.40 %	1.50 %
Mingle	96.79 %	15.08 %	0.42 %
TrapOrFlap	-	-	0.10 %
TreeBalanced	73.91 %	1.55 %	0.18 %

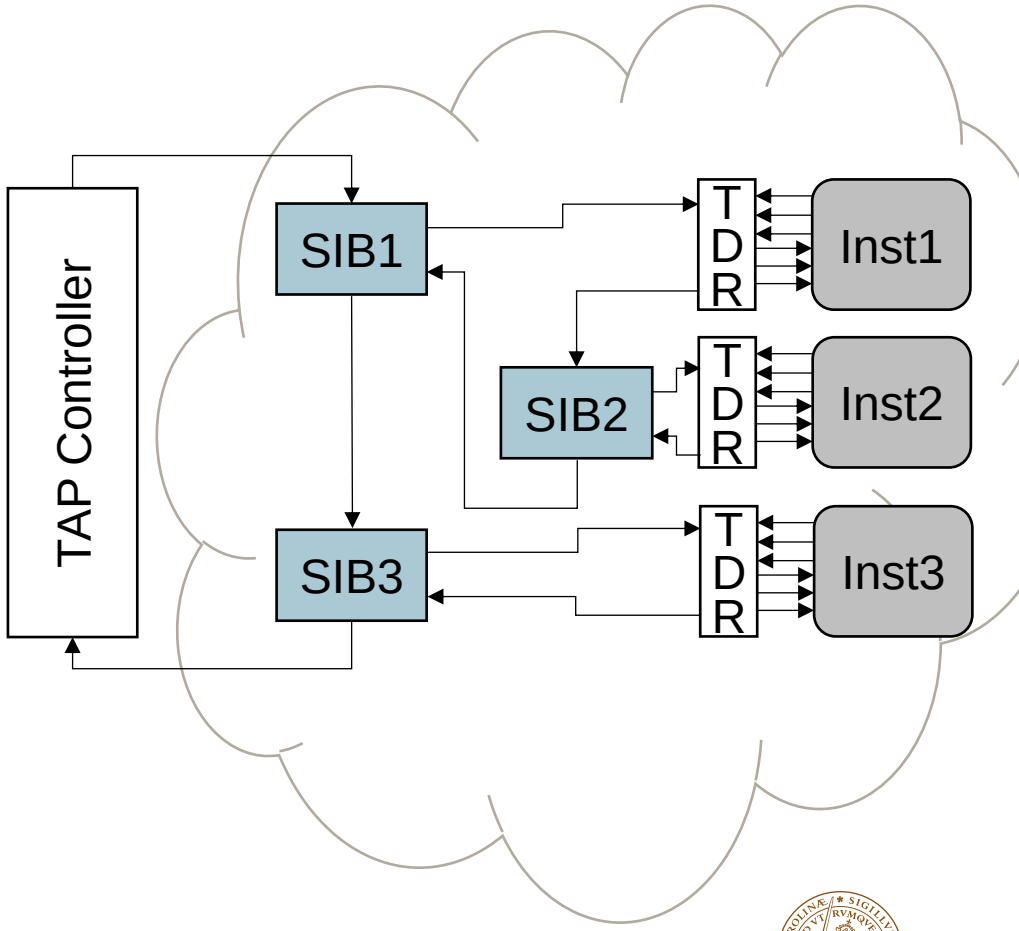
1. A. Tšertov, *et al.*, "*A suite of IEEE 1687 benchmark networks*"
2. R. Elnaggar, R. Karri, K. Chakrabarty, "*Security against data sniffing and alteration attacks in IJTAG*"
3. S.-J. Wang, *et al.*, "*Improving IJTAG test efficiency and security*"
4. A. Riaz, G. Kumar, J. Tudu, S. Ahlawat, "*On protecting IJTAG from data sniffing and alteration attacks*"
5. A. Das, N. A. Touba, "*A graph theory approach towards IJTAG security via controlled scan chain isolation*"

Outline

- Introduction
- Related work
- **Our solution**

Our Idea

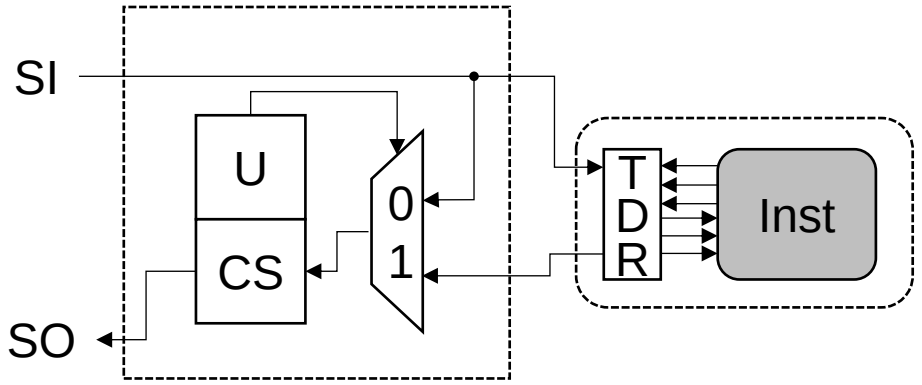
- Much related work first require the instrument to be in the active scan path, then a separate method (control signals, activation sequence, ...) for access
- We want to secure the IJTAG network, to protect against attacks from malicious instruments outside of the active scan path



LUND UNIVERSITY

Weakness in the SIB Components

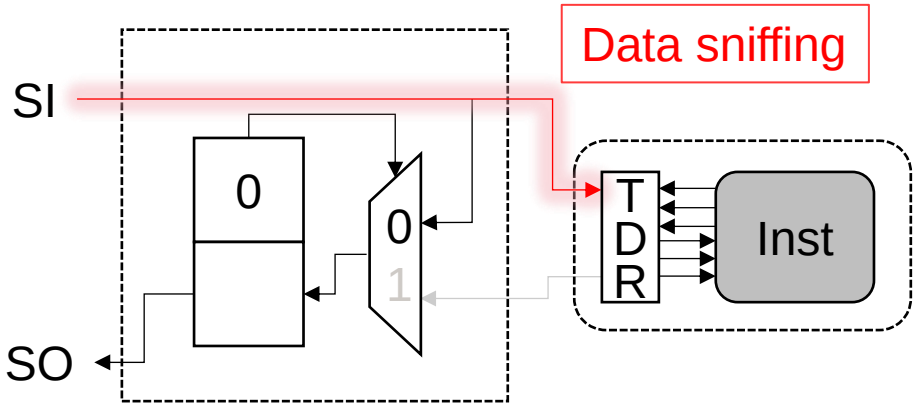
- Two SIB architectures proposed in IEEE Std. 1687 (IJTAG)



Pre MUX SIB

Weakness in the SIB Components

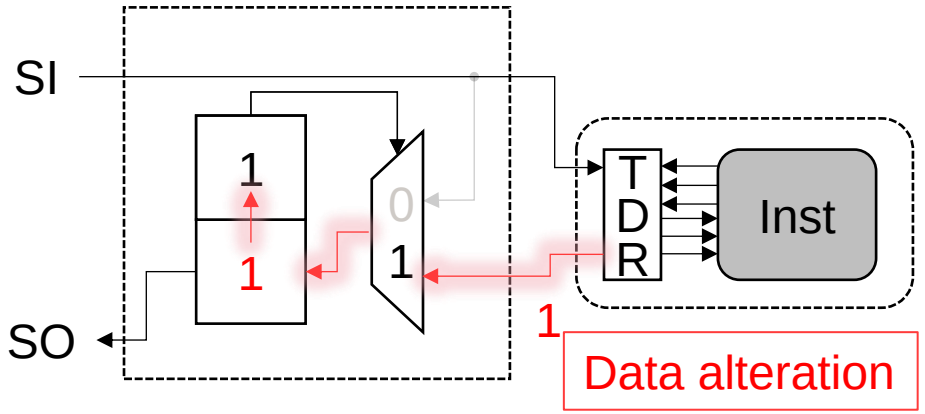
- Two SIB architectures proposed in IEEE Std. 1687 (IJTAG)



Pre MUX SIB

Weakness in the SIB Components

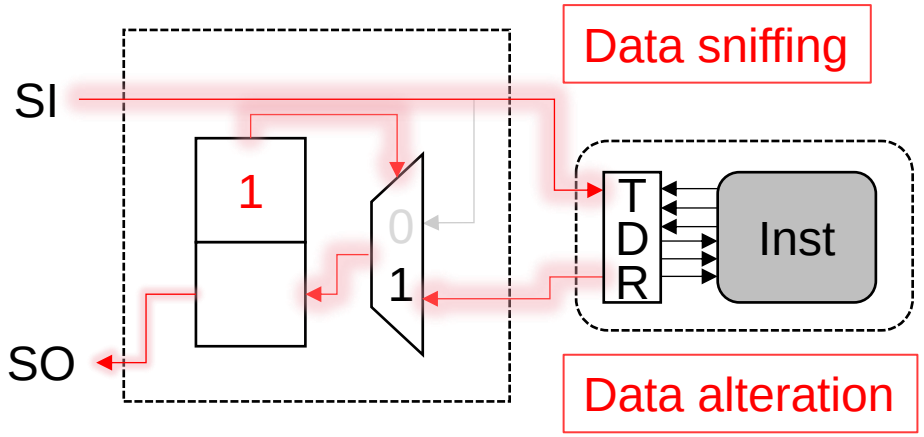
- Two SIB architectures proposed in IEEE Std. 1687 (IJTAG)



Pre MUX SIB

Weakness in the SIB Components

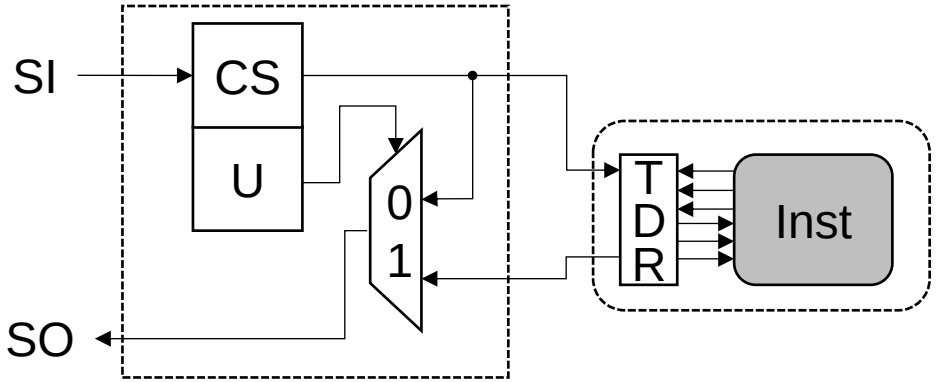
- Two SIB architectures proposed in IEEE Std. 1687 (IJTAG)



Pre MUX SIB

Weakness in the SIB Components

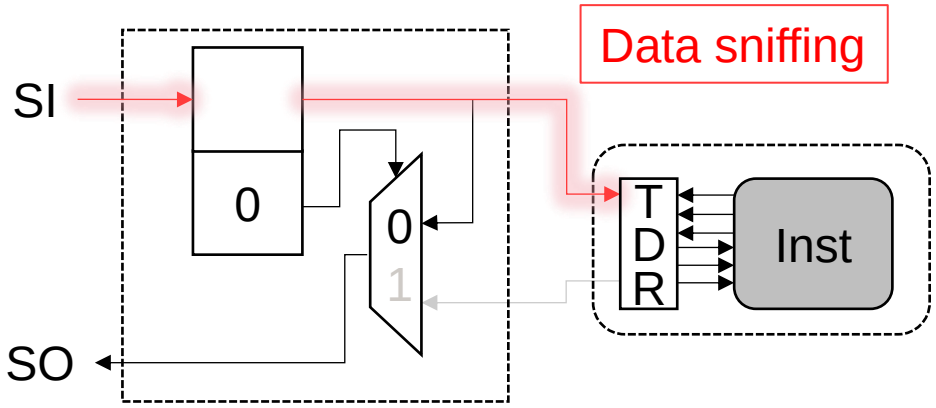
- Two SIB architectures proposed in IEEE Std. 1687 (IJTAG)



Post MUX SIB

Weakness in the SIB Components

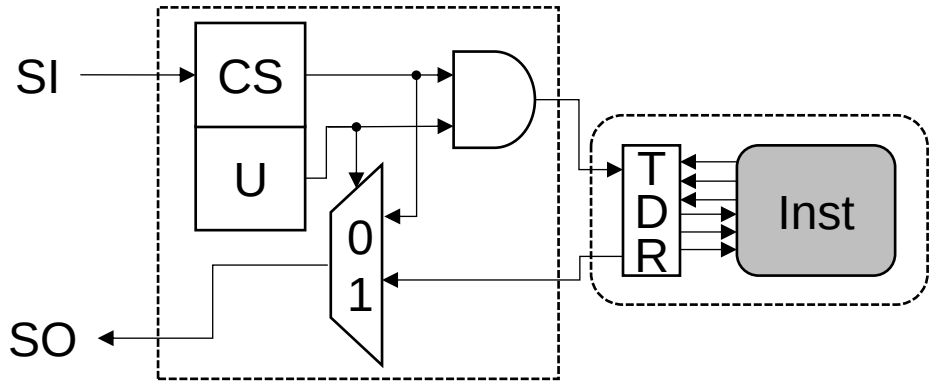
- Two SIB architectures proposed in IEEE Std. 1687 (IJTAG)



Post MUX SIB

Our solution

- Change SIB architecture in IJTAG network, to:
  - Not provide input data to instrument when SIB is closed
  - Close SIB without shifting data through untrusted instrument

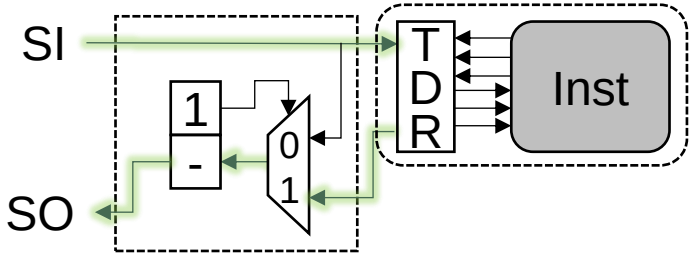


Proposed SIB

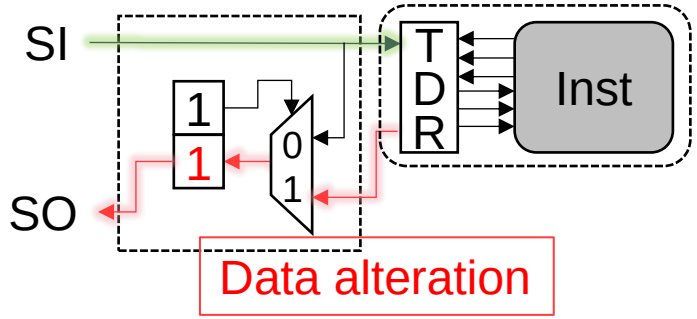
Our solution – Example

- Pre MUX SIB:

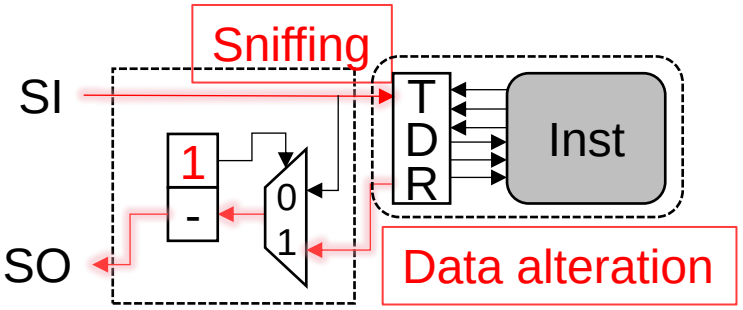
A. SIB is open



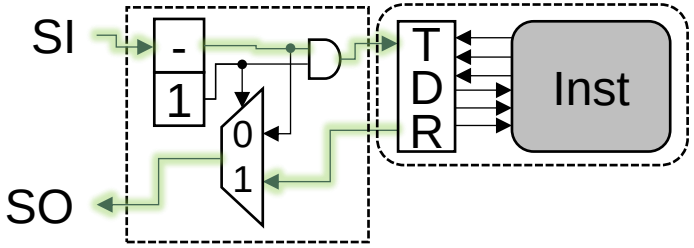
B. Shift in 0 to close SIB

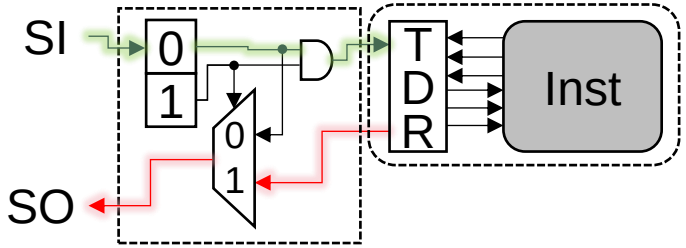


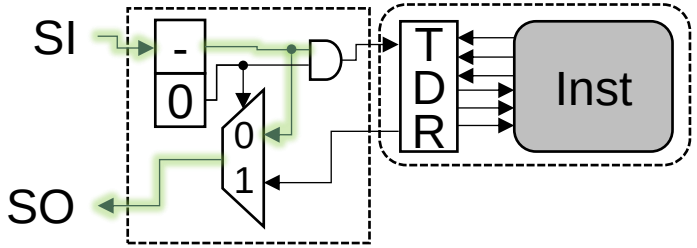
C. SIB should be closed



- Proposed SIB:







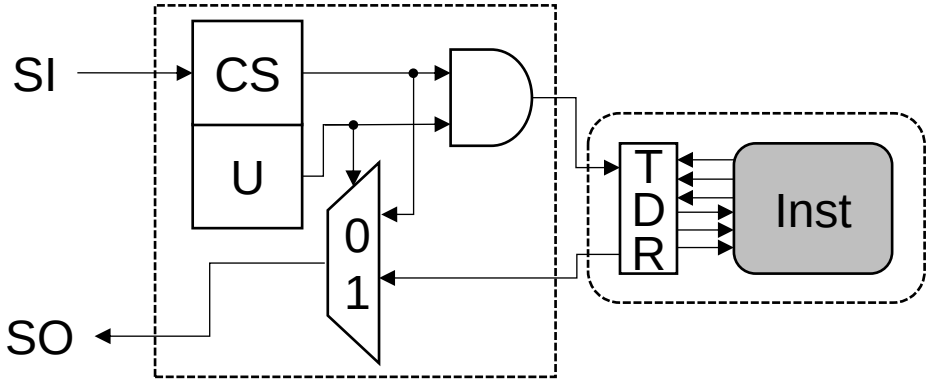
Requirements	STDR with secure wrapper[2]	STDR with control signals[3]	Priority encoder[4]	Isolation scheme[5]	Proposed SIB
IJTAG compliance?	Yes	Yes	Yes, re-arrange test data	Yes, manage control signals	Yes
Scalability issues?	None	Many control signals	None	Many control signals	None
IJTAG EDA tool?	No	No	No	No	Yes
Test time overhead?	Activation sequence	No	No parallel access	No	No
Area overhead?	Large	Large	Medium	Small	Small

IJTAG Benchmark[1]	STDR with secure wrapper[2]	Priority encoder[4]	Isolation scheme[5]	Proposed SIB
TreeFlat	92.46 %	12.40 %	1.50 %	0.66 %
Mingle	96.79 %	15.08 %	0.42 %	0.21 %
TrapOrFlap	-	-	0.10 %	0.06 %
TreeBalanced	73.91 %	1.55 %	0.18 %	0.07 %

1. A. Tšertov, *et al.*, "*A suite of IEEE 1687 benchmark networks*"
2. R. Elnaggar, R. Karri, K. Chakrabarty, "*Security against data sniffing and alteration attacks in IJTAG*"
3. S.-J. Wang, *et al.*, "*Improving IJTAG test efficiency and security*"
4. A. Riaz, G. Kumar, J. Tudu, S. Ahlawat, "*On protecting IJTAG from data sniffing and alteration attacks*"
5. A. Das, N. A. Touba, "*A graph theory approach towards IJTAG security via controlled scan chain isolation*"

Conclusion

- Protection against data sniffing and data alteration attacks in IJTAG, by changing the SIB architecture
  - Easy integration into an EDA tool
  - No extra control signals needed
  - No test time overhead
  - Low area overhead



Proposed SIB

LUND UNIVERSITY

LUND
UNIVERSITY