

Hardware Trojan Detection

Maximilian Heim

University Albstadt-Sigmaringen

May 15, 2022

1 Introduction

- Hardware Trojans
- Relevance

2 Detection

- Destructive detection
- Nondestructive detection

3 Conclusion

What are hardware trojans?

- ❶ Malicious modification of an IC
- ❷ Consists of a trigger and a payload
- ❸ Triggers: Time bombs, combinational, analog ...
- ❹ Payloads: Denial of service, extraction of information, keys

Why is detecting them relevant?

- Military
- Finance
- Energy
- Government agencies
- Surveillance states
- Transport
- The list continues . . .

Reverse Engineering

- Removing the surface layer by layer
- Advantages:
 - ① 100 % detection rate
- Disadvantages:
 - ① Only tests a single chip
 - ② Chip unusable afterwards
 - ③ Very time consuming
- However,

Types of detection