

# Hardware Trojan Detection

Maximilian Heim

University Albstadt-Sigmaringen

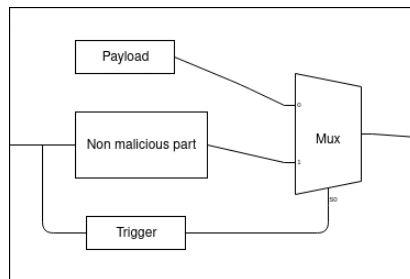
June 20, 2022

- 1 Introduction
  - Hardware Trojans
- 2 Destruktive Detektion
- 3 Nicht-Destruktive Detektion
- 4 Fazit

# Was sind Hardware Trojaner?

- Böartige Modifikation eines Integrierten Schaltkreises
- Trigger (Time bombs, cominational...)
- Payload (Denial of service, keys. . . )

Figure: Theoretischer Aufbau eines HW Trojaners



# Destruktives Reverse Engineering

- Entfernen der Oberfläche
- Visuelle Inspektion
- Vergleich mit Golden Sample
- Vorteile:
  - ① 100 % Erkennungsrate
- Nachteile:
  - ① Testet nur einen Chip
  - ② Destruktiv
  - ③ Zeitaufwändig
- Jedoch: Sinnvoll in Kombination mit anderen Verfahren

# Funktionstests

- Beobachten der Ausgabe bei bestimmten Eingängen
- Vergleich mit Golden Sample
- Problem: Großer Trojan Space
- Vorteile:
  - 1 Sehr einfacher Testaufbau
  - 2 Bei bekannten Testvektoren → 100 % Erkennungsrate
  - 3 Hunderte IC's können parallel getestet werden
- Nachteile:
  - 1 Je nach Komplexität des IC's sehr zeitaufwändig/unmöglich

# Funktionstests: Statistischer Ansatz

- R.S. Chakraborty et al, "MERO: A Statistical Approach for Hardware Trojan Detection"
- [https://link.springer.com/content/pdf/10.1007/978-3-642-04138-9\\_28.pdf](https://link.springer.com/content/pdf/10.1007/978-3-642-04138-9_28.pdf)
- Netzliste → Testvektoren
- Vektoren werden N mal getestet (Kombinatorisch-sequentielle HW Trojaner)
- Reduktion der Testzeit um 85 %

# Seitenkanaltest

- Beobachten der Leistungsaufnahme/Pfadverzögerung
- Vergleich mit Golden Sample
- Vorteile:
  - 1 Erkennung ohne Aktivierung
  - 2 Sehr einfacher Testaufbau
  - 3 Hohe Erkennungsrate
  - 4 Hunderte IC's können parallel getestet werden
- Nachteile:
  - 1 Produktionsvariationen
  - 2 Bei sehr kleinen Trojanern kann die Leakage sehr klein werden

# Seitenkanaltest: Fingerprinting

- D. Agrawal et al, "Trojan Detection using IC Fingerprinting"
- <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4223234>
  - 1 Auswahl zufälliger Schaltkreise
  - 2 Aufnahme von Power Traces
  - 3 Fingerprint erzeugen
  - 4 Destruktives Reverse Engineering der Chips
  - 5 Vergleiche Fingerprints von zu testenden Chips mit Referenz



# Fazit

- Destruktive Detektion ungeeignet für Testen von ICs die verwendet werden sollen
- Gegenüberstellung von Funktionstests und Seitenkanaltests:

	Funktionstests	Seitenkanaltests
Pros	1. Effektiv für kleine Trojaner 2. Produktionstoleranz unabhängig	1. Effektiv für große Trojaner 2. einfache Testerzeugung
Cons	1. Testerzeugung komplex	1. Anfällig für Produktionstoleranzen 2. Detektion von kleinen Trojanern schwierig

- Wie man sieht: Die Verfahren ergänzen sich → Kombination beider Verfahren

# Quellen

- <https://d/dl.acm.org/doi/pdf/10.1145/2906147>
- <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5340158>
- [https://www.fkie.fraunhofer.de/content/dam/fkie/de/documents/HWT-Bericht/HWT-Bericht\\_Cover.pdf](https://www.fkie.fraunhofer.de/content/dam/fkie/de/documents/HWT-Bericht/HWT-Bericht_Cover.pdf)
- [https://en.wikipedia.org/wiki/Hardware\\_Trojan](https://en.wikipedia.org/wiki/Hardware_Trojan)