

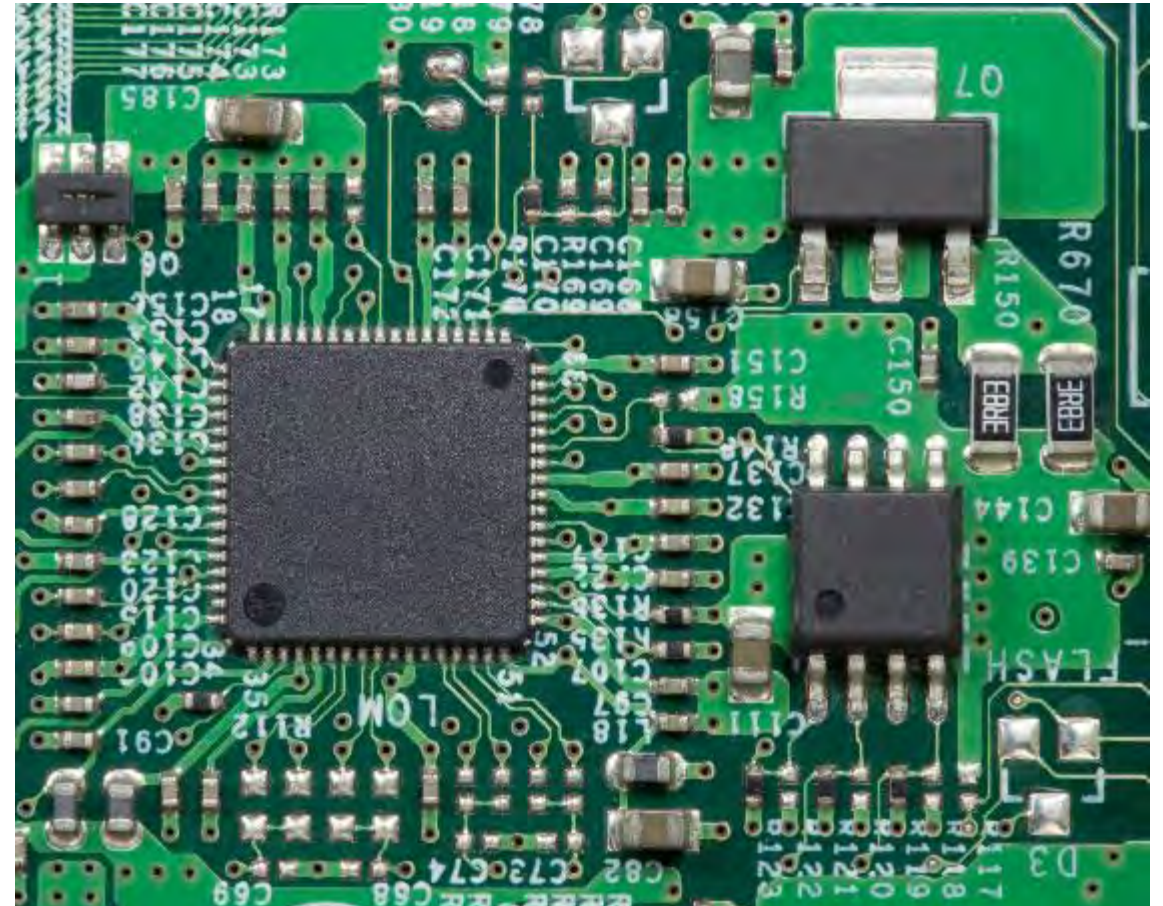
# Hardware-Hacking entschlüsselt

Ein einfacher Leitfaden zu  
Seitenkanal- und Glitching-Angriffen

# Warum Hardwaresicherheit?

## Entwicklersicht

## Hardware wird als digitale **Blackbox** betrachtet



# Warum Hardwaresicherheit?

# Angreifersicht

## Schnittstellen und Zugänge:

- Takt und Spannungsversorgung
- Debug-Schnittstellen

## Bauteile:

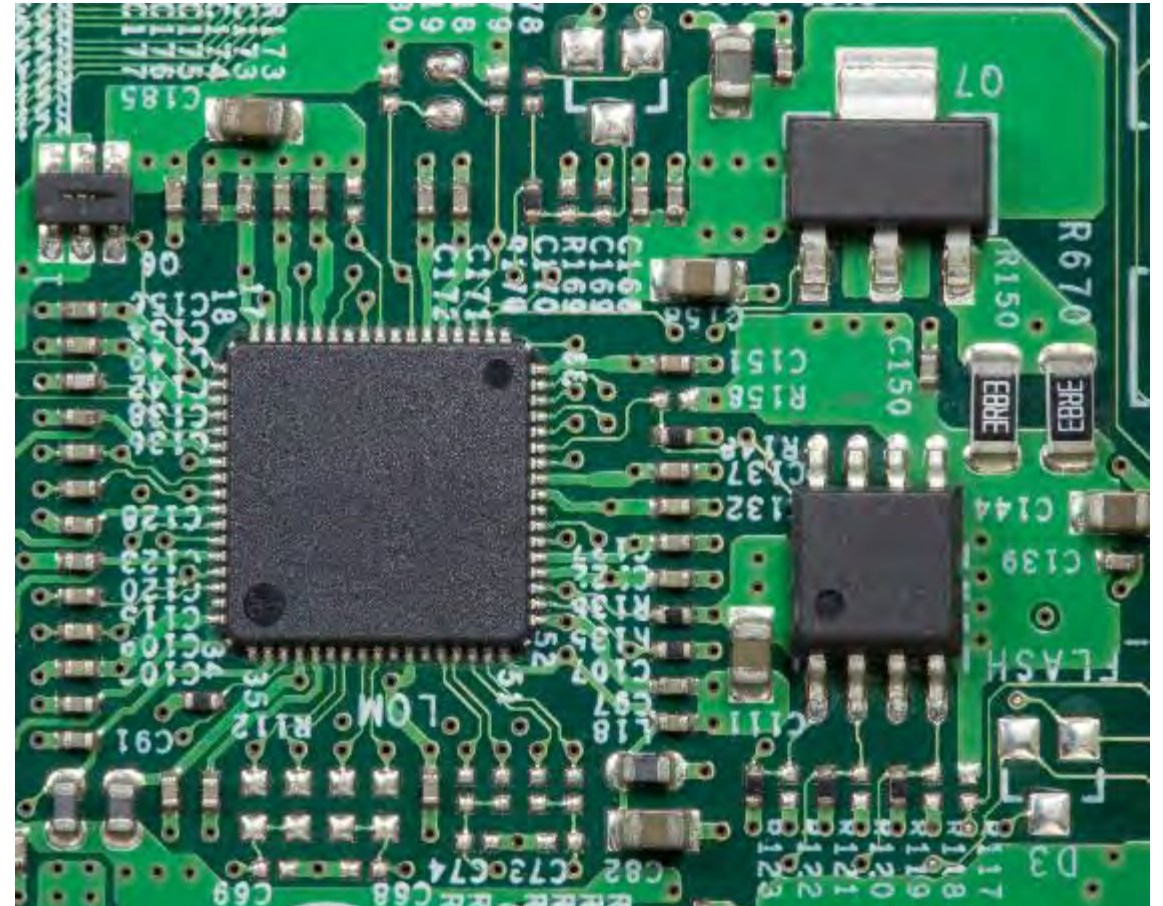
- Speicher

## Beobachten:

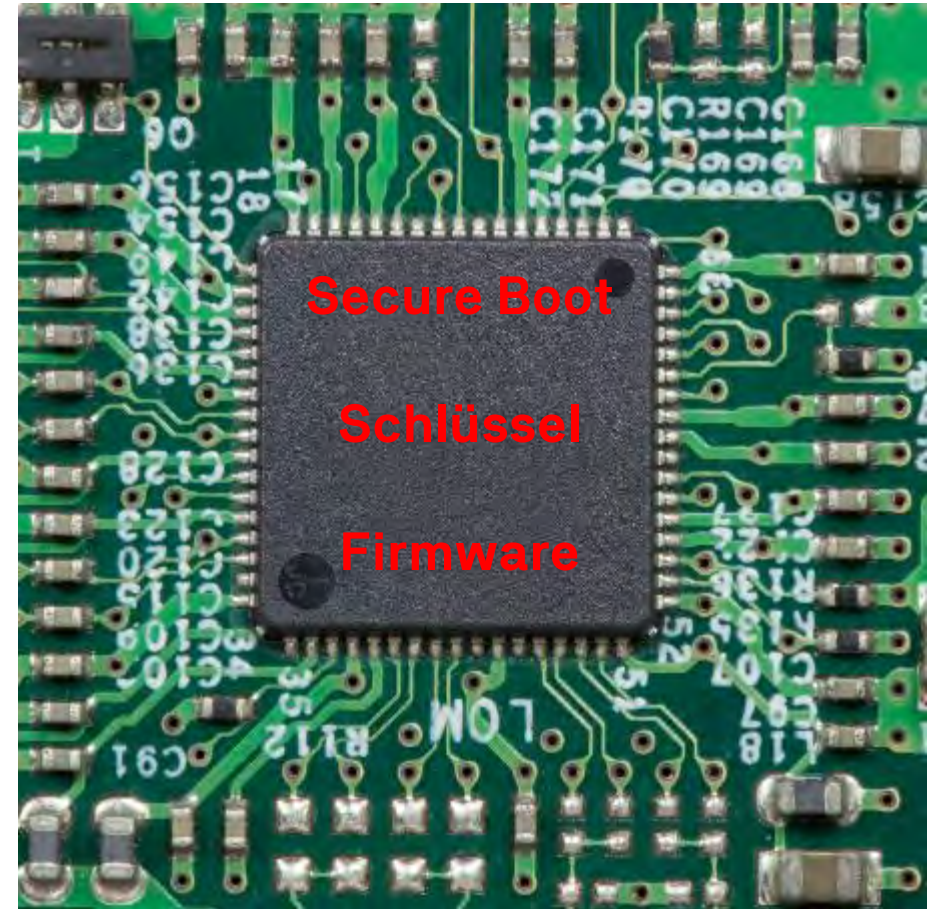
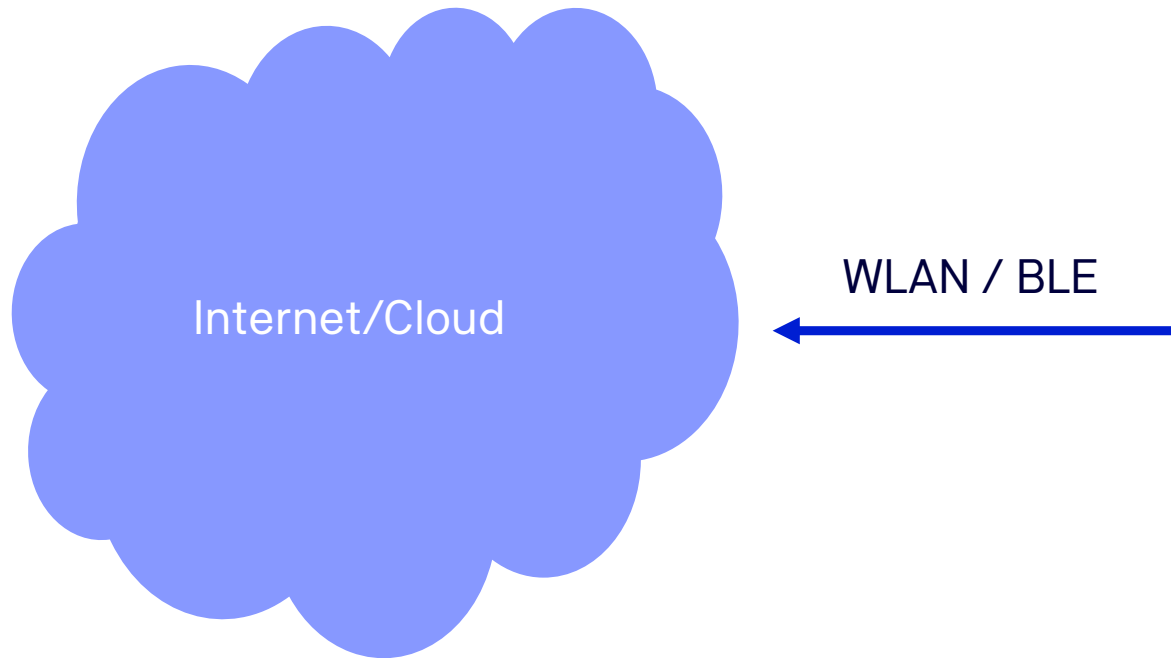
- Seitenkanalangriffe

## Stören:

- Fehlerangriffe



# Warum Hardwaresicherheit?



# Die ersten Angriffspunkte

## Kommunikationsschnittstellen abhören

UART

## Debug-Schnittstellen verwenden

JTAG

## Externe Flash-Chips auslesen

Equipment:

- Datasheet
- Multimeter
- Logic Analyzer
- günstige Debugger
- Low-End-Oszilloskop

**Kosten: wenige hundert Euro**

# Und wenn diese nicht funktionieren?

-  Debug-Port gesperrt
-  Flash Readout Protection aktiv
-  Firmware signiert
-  Secure Boot aktiv
-  Schlüssel nicht direkt auslesbar

Jetzt wird es interessant.

# Seitenkanalangriffe

Was ist ein Seitenkanal?

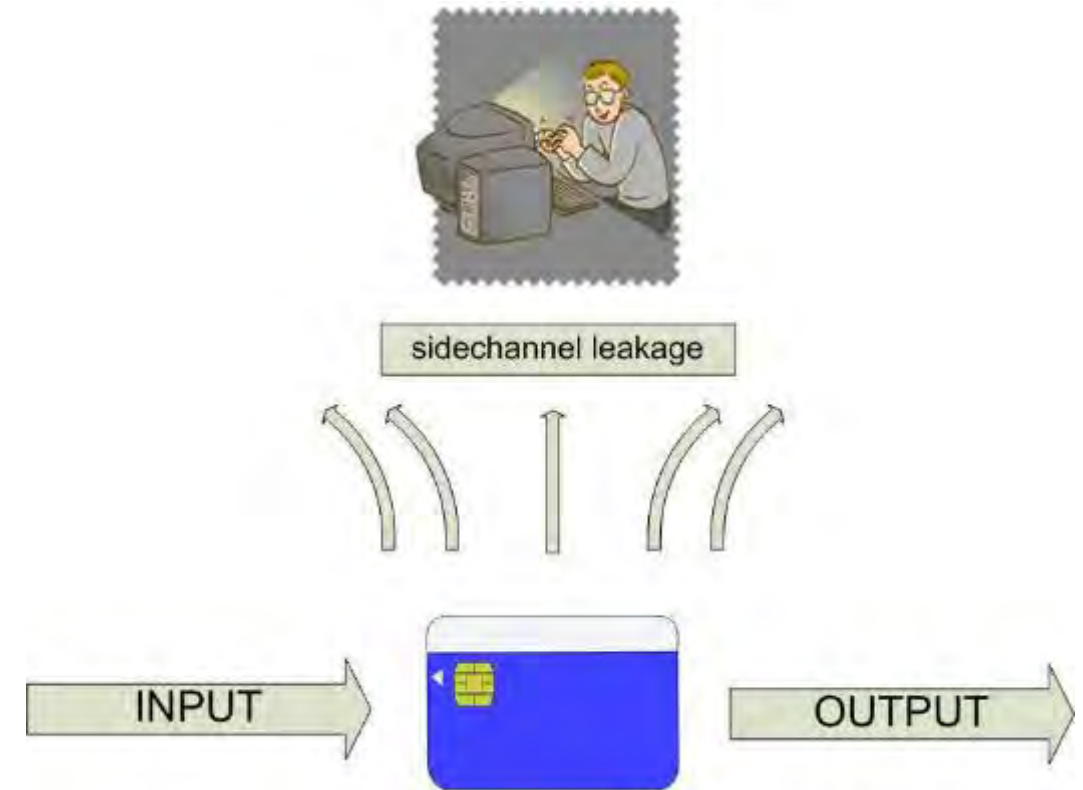
**Seitenkanalangriffe sind passive Angriffe**

**Uns interessiert:**

- Operationsabhängigkeit
- Datenabhängigkeit

**Wir beobachten:**

- Laufzeit
- Stromverbrauch
- elektromagnetische Abstrahlung



# Seitenkanalangriffe

## Laufzeit

```
bool passWordCheck(uint8_t* passwordHash)
{
    uint8_t correctPassword[32] = {0x00, 0x01, 0x02....}

    for (int j = 0; j < 32; j++) {
        if (correctPassword[j] != passwordHash[j]) {
            return false;
        }
    }

    return true;
}
```

# Seitenkanalangriffe

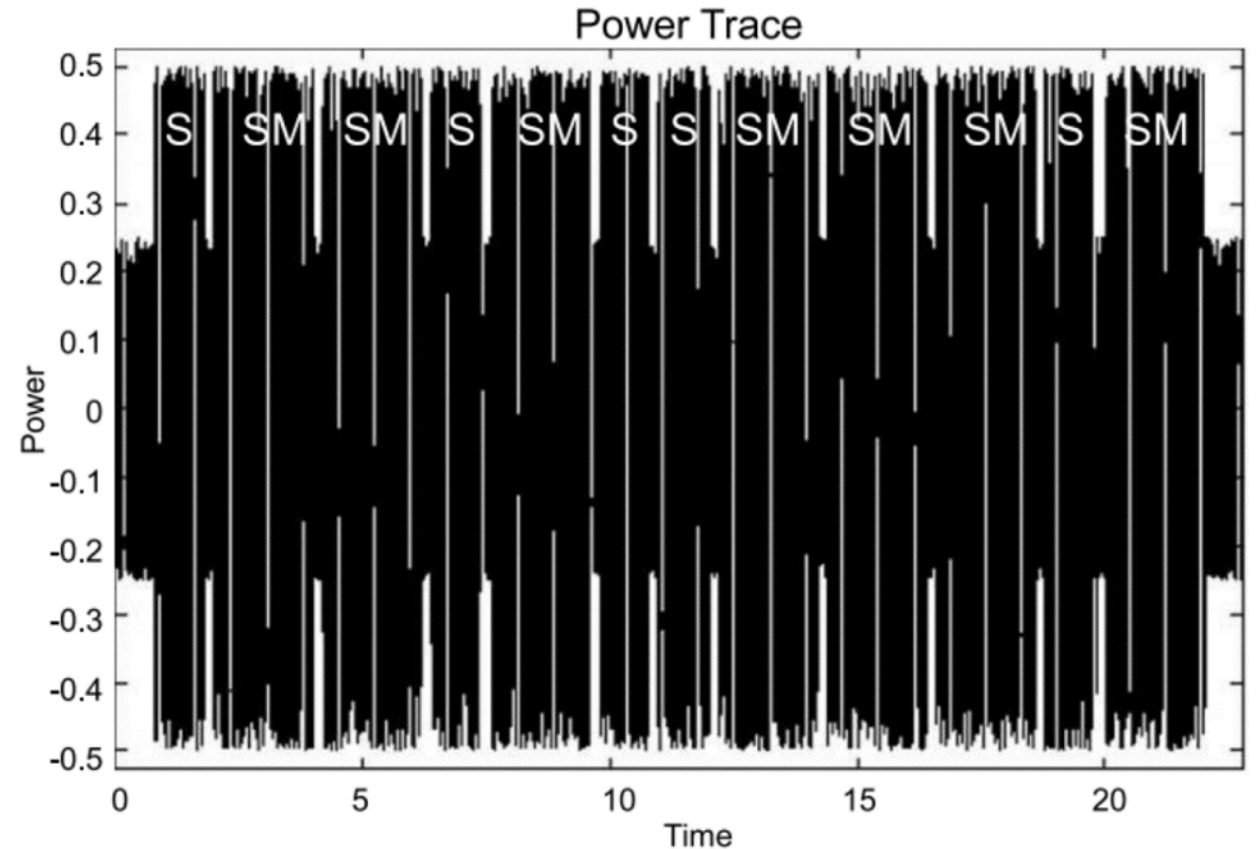
## Operationsabhängigkeit

Operationen unterscheiden anhand von:

- Laufzeit
- Taktzyklen
- Stromverbrauch

In unserem Beispiel:

- S → Binär 0
- SM → Binär 1

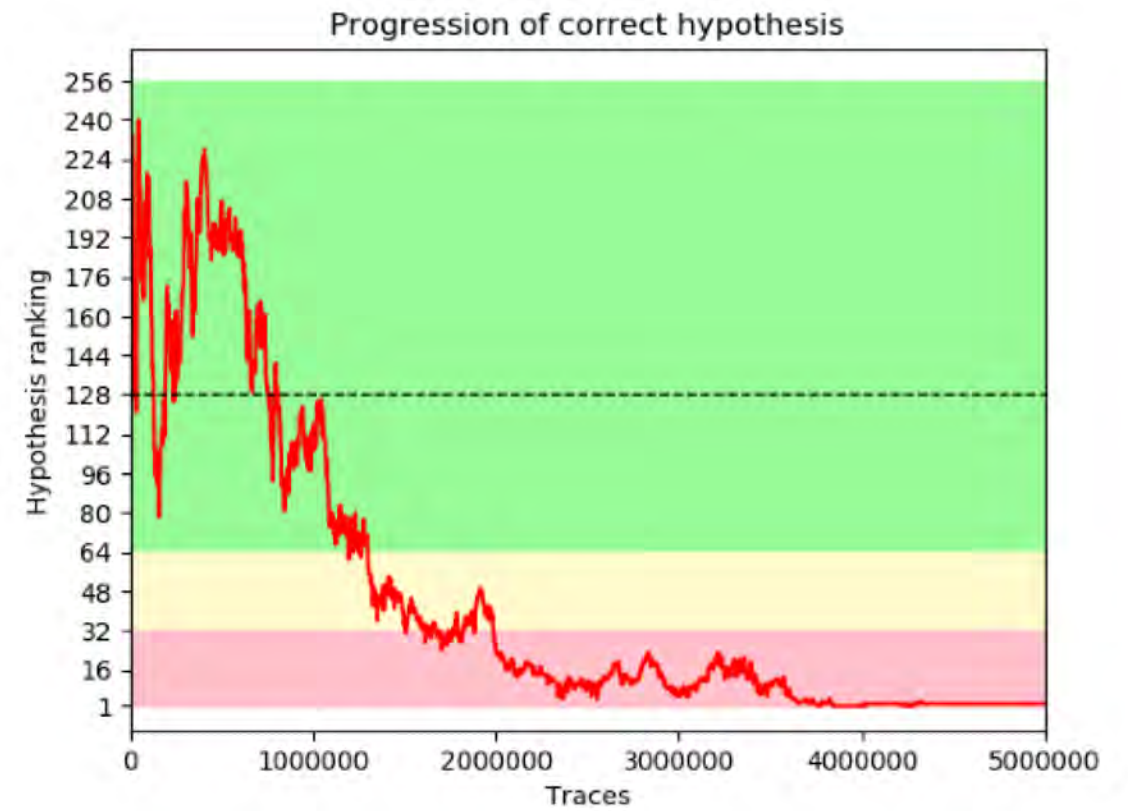
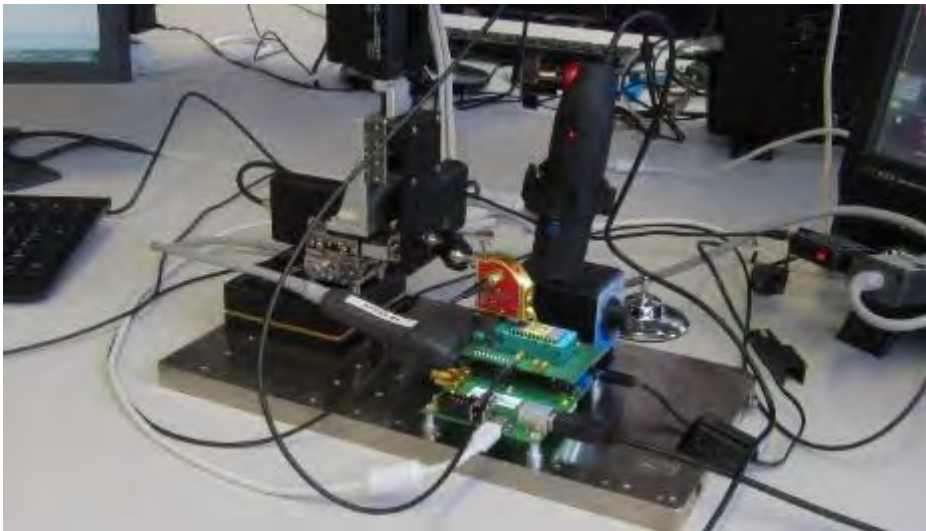


Quelle: *Understanding Cryptography: A textbook for students and practitioners*

# Seitenkanalangriffe

## Symmetrische Verschlüsselung

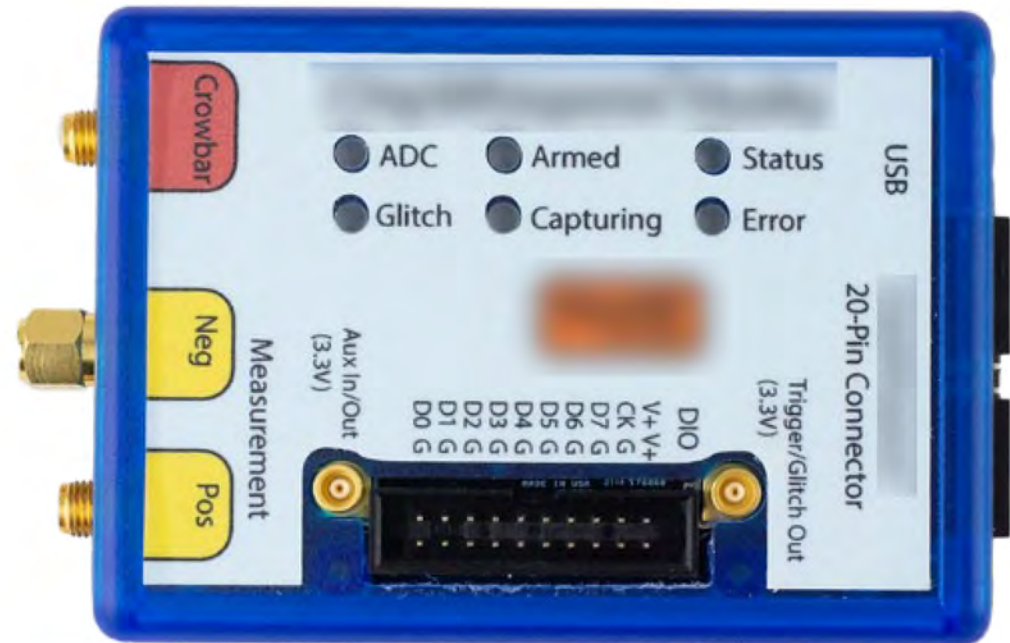
Hunderte bis Tausende Messungen in Kombination mit statistischen Analysen



# Seitenkanalangriffe

Durchführung im Büro

1. Messen und Triggern (**für unter 700 €**)
2. Open-Source-Software
3. Schlüsselextraktion

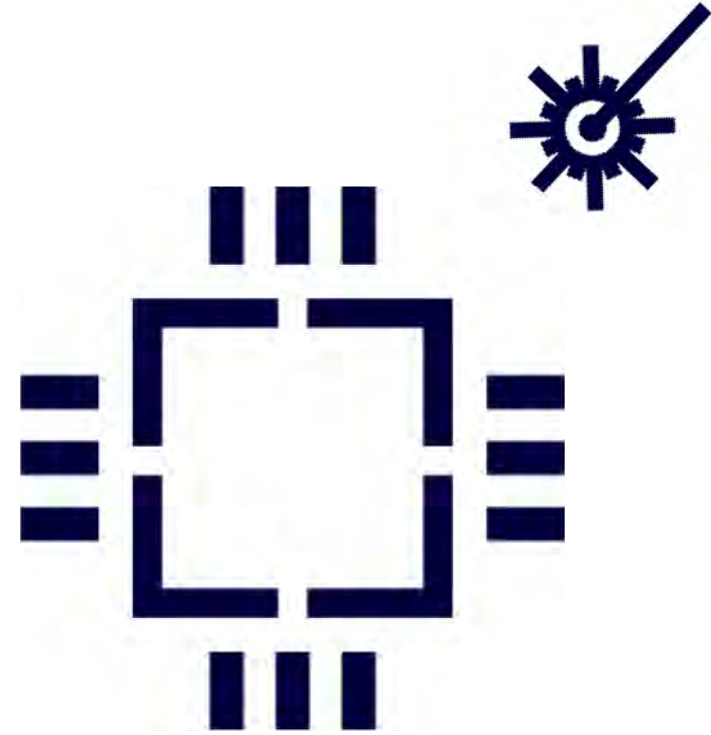


# Fehlerangriffe

## Fehlerangriffe sind aktive Angriffe

Typische Angriffsvektoren sind:

- Spannung
- Takt
- EM
- Laser
- Umgebungstemperatur



# Fehlerangriffe

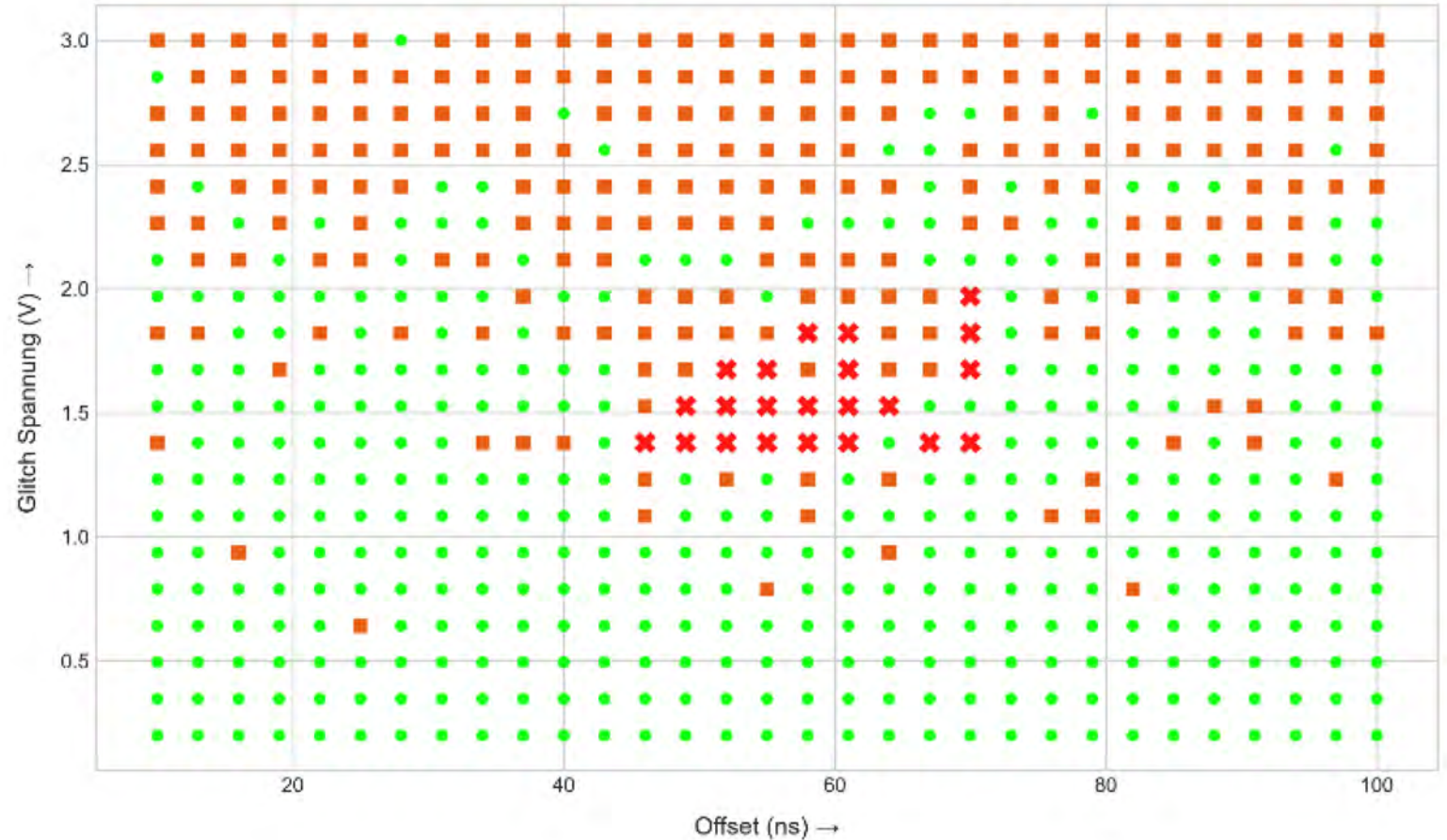
## Kritische Single-Bit-Entscheidungen

```
1  if (firmware_is_valid()) {  
2      boot();  
3  } else {  
4      stop();  
5  }
```

# Wann stören wir die Berechnung?

Verschiedene Parameter testen z. B. :

- Timing
- Pulsdauer
- Pulsstärke



# Von lokalem zu Remote-Angriff

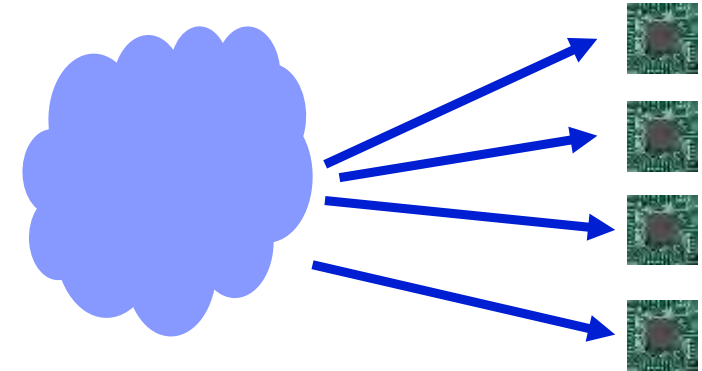
1 Firmware extrahieren



2 Firmware analysieren



3 Remote-Angriff entwickeln



Der Hardwareangriff muss nur auf einem Gerät stattfinden. Das Ergebnis der Analyse kann unter Umständen die gesamte Produktflotte betreffen.

# Gegenmaßnahmen

Ein Auszug

| Seitenkanäle                                                                                                  | Fehlerinjektion                                                                                           |
|---------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• Masking</li><li>• Hiding</li><li>• Konstantes Zeitverhalten</li></ul> | <ul style="list-style-type: none"><li>• Sensoren</li><li>• Redundanz</li><li>• Code-Flow-Schutz</li></ul> |

# In der Entwicklungsphase

- ☐ Sind Debug- und Testschnittstellen im Produktionszustand deaktiviert?
- ☐ Werden kritische Daten auf dem PCB geschützt übertragen?
- ☐ Wie verhält sich das System bei einfachen Glitching-Angriffen?
- ☐ Sind kritische Entscheidungen redundant abgesichert?
- ☐ Wurde der Stromverbrauch auf Seitenkanäle untersucht?
- ☐ Wurde das Laufzeitverhalten auf Seitenkanäle untersucht?

**Kenne ich die Hardwareeigenschaften meines Produktes?**

## **M. Sc. Nick Theisejans**

Produktmanager Hardwaresicherheit

Senior-Experte für Hardware & eingebettete Sicherheit

[N.Theisejans@tuvit.de](mailto:N.Theisejans@tuvit.de)

+49 201 8999-507

