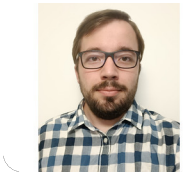
# Fault Detector

## Detektion von Fault-Angriffen auf dem FPGA


Diplomand



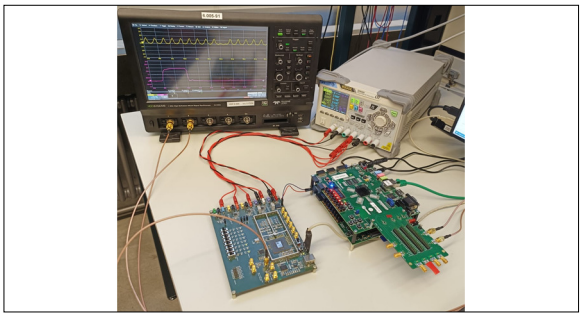
**David Feldmann**


Einleitung: Mit stetig voranschreitender Digitalisierung steigt der Bedarf an spezieller Hardware zur Beschleunigung von kryptographischen Algorithmen. Durch den Einsatz von Fault-Attacken, welche das System manipulieren und in unbeabsichtigte Zustände bringen, wird ebendiese Hardware zum Schwachpunkt der Verschlüsselung. Böswillige Akteure nutzen diese Attacken, um an den Kryptographieschlüssel zu gelangen und sensible Daten zu extrahieren. Um diesen Angriffen entgegenzuwirken, bedarf es nicht nur softwareseitige Erkennung von Fehlkalkulationen, sondern optimalerweise auch einem Detektor, welcher die Attacken frühzeitig, zuverlässig und präzise detektiert. Bei der Entwicklung wurde darauf abgezielt, eine möglichst breite Sparte an Angriffsmethoden abzudecken. Der Fokus lag auf Spannungs- und Takt-Glitches, da diese zu den beliebtesten Attacken gehören. Bei der Implementierung wurde viel Wert auf Kompaktheit, flexible Portierbarkeit und Effizienz gelegt.

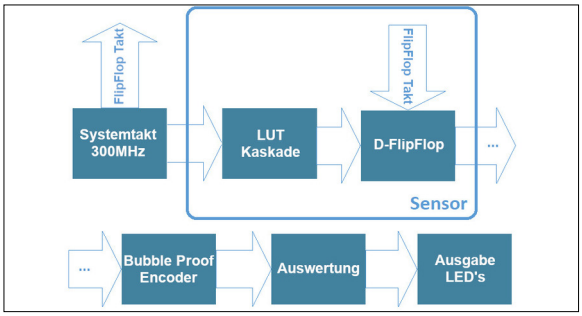
Vorgehen: Zu Beginn wurde ein grobes Verständnis zu den verschiedenen Attacken erarbeitet. Danach wurde der geplante Sensor analog mittels VHDL-AMS simuliert, um dessen Funktionsweise besser zu verstehen und seine Funktion zu bestätigen. Mit neu gewonnen Erkenntnissen ging es danach an die Implementierung mittels der Hardware-Beschreibungssprache VHDL. Für die entwickelten Designs wurden fortlaufend Testbenches geschrieben, um deren Funktionalität zu testen und zu verifizieren. Schlussendlich wurde das fertige Design auf die Hardware geladen, optimiert, getestet und ausgemessen.

Ergebnis: Mittels einer Kette von 52 Verzögerungsgliedern, durch welche der verwendete Takt von 300 MHz hindurchgeschickt wird, konnten sowohl Takt- als auch Spannungs-Glitches erkannt werden. Damit wurden die Forderungen gemäss Aufgabenstellung erfüllt. In den durchgeführten Messungen erwies sich der Detektor als präzise und zuverlässig mit erkannten Glitches bis zu einer minimalen Länge von 1 ns. Auch war es durch gezieltes Platzieren der Logik möglich, ein elegantes, kompaktes und doch flexibles Design zu erstellen.

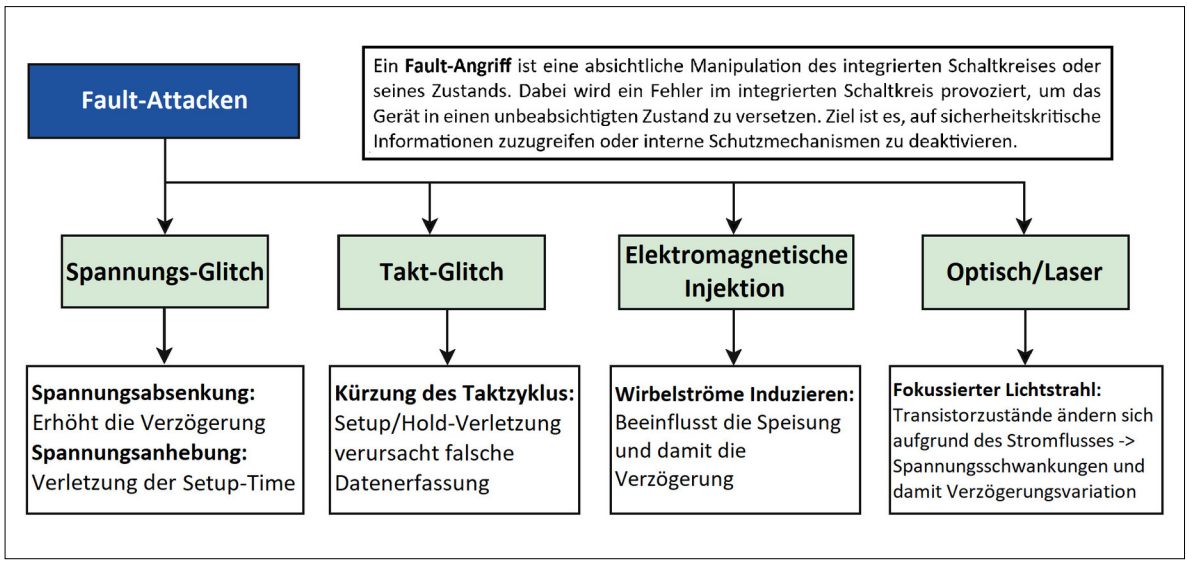
**Messaufbau für Takt-Glitch**
Eigene Darstellung



**Blockschaltbild des implementierten Detektors**
Eigene Darstellung




**Übersicht über populäre Fault-Attacken**
Basierend auf Buch "Hardware Security Training, Hands-on!"




Referenten
**Prof. Dr. Paul Zbinden, Lukas Leuenberger**

Korreferent
**Robert Reutemann, Zürich, ZH**

Themengebiet
**Mikroelektronik**

Projektpartner
**IMES Institut für Mikroelektronik und Embedded Systems, Rapperswil, SG**