# Kurzfassung

## Strukturorientiertes Design von Sicherheitsprimitiven auf rekonfigurierbarer Hardware

**Alexander Wild**

Ein Field Programmable Gate Array (FPGA) ist ein programmierbarer Hardwarebaustein, welcher weitreichende Anwendung in kommerziellen Produkten, wie Satelliten-Receivern, gesicherten Universal Serial Bus (USB) Sticks aber auch in Infrastrukturen, wie Netzwerk-Backbones, findet. Die Popularität dieser Gerätefamilie stützt sich auf die hohe Flexibilität und Programmierbarkeit, kombiniert mit den Vorteilen von Hardwarebausteinen (hinsichtlich der hohen Leistung, niedrigem Energieverbrauch und Sicherheit durch Integration). Somit bietet die Hardwarestruktur von FPGAs eine hervorragende Plattform für schnelle und effiziente Anwendungen mit geringem Entwicklungsaufwand. Dennoch wird von den FPGA-Herstellern kaum Unterstützung geboten, um ihre Geräte gegen die Vielzahl von Angriffsszenarien zu schützen.

Eine Art der Angriffsklassen, gegen die sich jede physikalisch zugängliche Hardware schützen muss, sind physikalische Angriffe. Diese Angriffsklasse ist momentan eines der größten Themen im Bereich der Hardware-Sicherheit. Die aktuellen FPGA-Generationen sind inhärent nicht mit Gegenmaßnahmen gegen diese Angriffsklasse ausgestattet.

Des Weiteren basiert die Mehrheit der auf dem Markt erhältlichen FPGAs auf Static Random Access Memory (SRAM)-Zellen und stellen dadurch keinen sicheren, nicht flüchtigen Speicher im Chipgehäuse für Benutzer bereit. Dadurch ist eine konventionelle Umsetzung von persistenter, interner Schlüsselspeicherung nicht möglich und ein alternatives Schlüsselmanagement erforderlich. Physical Unclonable Functions (PUFs) scheinen eine vielversprechende Lösung für dieses Problem zu bieten, indem ein gerätespezifischer, geheimer Schlüssel während der Initialisierungsphase oder zur Laufzeit des FPGAs generiert wird.

Diese Dissertation behandelt die beiden erwähnten Probleme und konzentriert sich dabei auf die Aspekte und Strukturen der untersten Ebene eines FPGAs. Genauer gesagt wird die Gerätestruktur selbst verwendet, um (i) die Widerstandsfähigkeit gegenüber physikalischen Angriffen zu erhöhen und (ii) um PUF-Konstrukte zu realisieren, welche ohne die Verwendung von zusätzlicher Hardware auf FPGAs umsetzbar sind.

### Schlagworte:

Field Programmable Gate Array (FPGA), Kryptologie, Gegenmaßnahme, Hardware, Implementierung