

Seitenkanalangriff auf verschiedene Speicherkonzepte



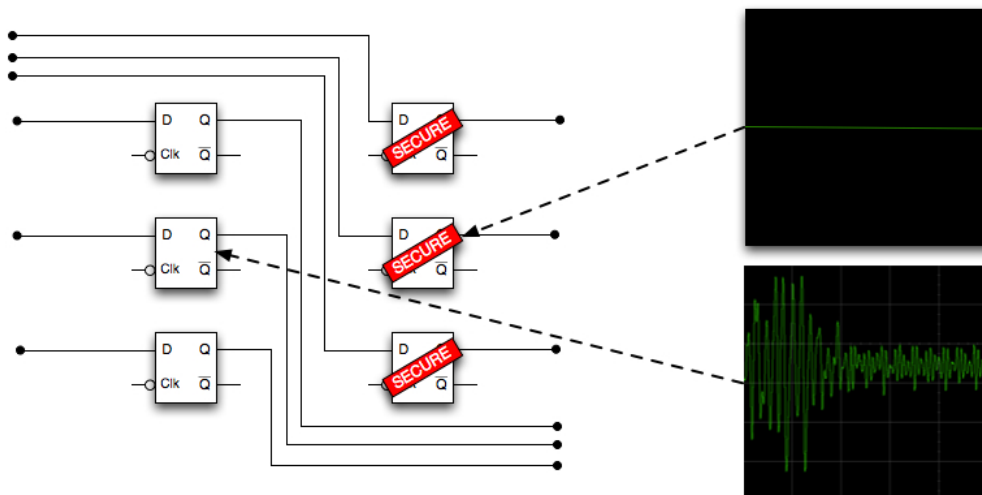
TECHNISCHE
UNIVERSITÄT
DARMSTADT

Fachbereich Informatik
Integrierte Schaltungen und Systeme

Master-/Diplomarbeit

Aufgabenstellung

Seitenkanalangriffe sind ein wichtiges Thema beim Entwurf von sicheren Verschlüsselungsprozessoren. Eines dieser Angriffsverfahren ist die *Differential Power Analysis* (DPA). Diese Angriffstechnik nutzt das zeitliche Verhalten der Leistungsaufnahme der kryptographischen Hardware, um Rückschlüsse auf den Schlüssel zu gewinnen und um diesen zu schätzen.



In dieser Arbeit sollen verschiedene Techniken evaluiert werden, welche Informationsschwachstellen in Speicherelementen vor Seitenkanalangriffen schützen. Die aus der Evaluation gewonnenen Kenntnisse sollen genutzt werden, um eine sichere Speicherarchitektur in VHDL zu implementieren.

Betreuung

Betreut werden können Studenten/Studentinnen aus dem FB Informatik oder FB Elektrotechnik.

Die Arbeit erfolgt in enger Zusammenarbeit mit einem wissenschaftlichen Mitarbeiter. Bei Interesse melden Sie sich bitte direkt bei untenstehendem Mitarbeiter. Ein Informationsblatt mit der detaillierten Aufgabenstellung können Sie per Nachfrage erhalten.

Zur Bearbeitung sind Kenntnisse in VHDL und Speicherarchitekturen notwendig. Kenntnisse im Bereich Schaltungsentwurf sind von Vorteil.