

CUDA vs. FPGA zur beschleunigten Korrelationsanalyse von Seitenkanälen



TECHNISCHE
UNIVERSITÄT
DARMSTADT

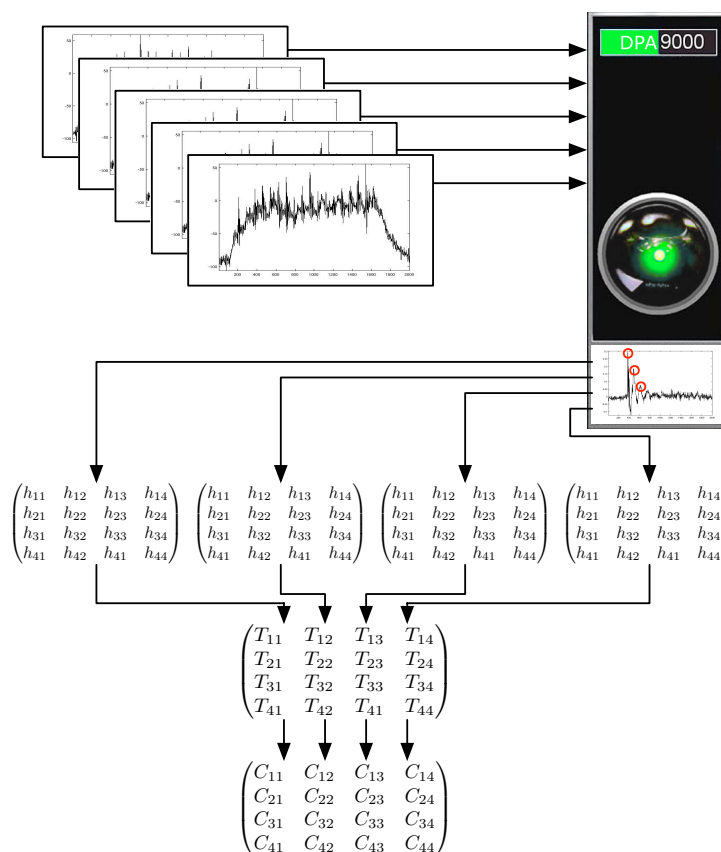
Fachbereich Informatik
Integrierte Schaltungen und Systeme

Diplom-/ Masterarbeit

Aufgabenstellung

Die Methode der *Differential Power Analysis* (DPA) Angriff hat sich im Bereich der Seitenkanalangriffe etabliert. Zur Durchführung dieses Angriffs sind neben der Aufnahme von Leistungskurven des anzugreifenden Devices auch aufwendige und intensive Berechnungen zur Auswertung nötig. Aktuelle Rechenarchitekturen sind stark genug, um diese Aufgaben in einer annehmbaren Zeit zu berechnen, verlangsamen jedoch den Analyse-Prozess.

Im Rahmen dieser Arbeit sollen Verfahren zur Beschleunigung dieser Berechnungen untersucht werden. Bestehende Matlab-Skripte für die Durchführung eines DPA-Angriffs sollen optimiert werden, um diese für parallele Berechnungsprozeduren nutzen zu können. Zur Parallelisierung sollen die Berechnungen für die Korrelationskoeffizienten auf einer leistungsstarken Grafikkarte ausgeführt werden. Aus Performanzgründen soll evaluiert werden, ob es effektiver ist, diese Berechnungen in Hardware auf einen FPGA auszuführen oder auf einer Grafikkarte.



Betreuung

Betreut werden können Student(innen) 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 *Matlab*, *VHDL* und *C/C++* nötig.