
— Master Thesis — (Diplomarbeit)

Side Channel Analysis Acceleration with CUDA and OpenCL

CASED

In CASED (Center for Advanced Security Research Darmstadt) collaborate the Technische Universität Darmstadt, Fraunhofer Institute for Secure Information Technology and the University of Applied Sciences Darmstadt in the fast developing field of IT Security. In a unique cooperation, which combines different areas of expertise from these renowned institutions, progressive IT security solutions are researched, developed and implemented into industrial economy: CASED brings together computer scientists, engineers, physicists, legal experts and business economists. Read more on www.cased.de.

Motivation

The task of the thesis is to accelerate a *Differential Power Analysis* attack by using a GPU based architecture. Therefore the needed algorithms have to be implemented either with the CUDA and the OpenCL framework in C to utilize a Nvidia graphic card for massive parallel computing. The implemented program to speed up the computation should be embedded into a Matlab Toolbox. To improve the performance, different parallelization techniques have to be evaluated to gain the maximum throughput. For benchmarking the implemented algorithms in C via OpenCL and CUDA the original matlab DPA algorithms have to be transferred to GPUmat.

Tasks

- Analyze existing algorithms in Matlab and implement them with CUDA
- Embedding the correlation calculation on the graphic card in the Matlab
- Optimize algorithms for correlation calculation on the graphic card
- Benchmark results against an existing Toolbox

Requirements

- Knowledge in the area of parallel computing
- Experience with Matlab
- Expertise in programming C

Date of entry

As of now

Contact

Dipl.-Ing. Marc Stöttinger
stoettinger@iss.tu-darmstadt.de
CASED - Center for Advanced Security Research Darmstadt
Mornewegstraße 32
64293 Darmstadt