Motivation

ARM processors are flooding the market of routers, smartphones, and wireless devices. Based on a 32-bit architecture, modern CPUs make use of the ARM NEON extension featuring advanced 128-bit instructions. Example devices are the Apple iPad2 or the Samsung Galaxy S2.

ALE is a new lightweight authenticated encryption algorithm based on AES. Based on previous Intel SSE implementations of AES, efficient ARM NEON implementations should be developed. A Samsung Galaxy S2 device will be used to benchmark and improve the implementations.

Goals and Tasks

- Acquire the necessary background on AES implementations and NEON instructions
- Port ALE to ARM using NEON extensions
- Analyze and optimize the C/assembly implementation

Literature


Deliverables

- Project files (.zip, cleaned)
- Documentation (inline)
- Readme (getting started)
- Presentation (10 .ppt slides)

Project Schedule

- Start Immediately
- Month 1 Reading literature
- Month 2 Implementing
- Month 3 Final deliverables

Project

Studies: ☒ INF ☒ SW ☒ TEL ☒ TM

Prerequisites

- C programming

Advisor / Contact

florian.mendel@iaik.tugraz.at
martin.schlaeffer@iaik.tugraz.at