

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.

Grøstl is a candidate algorithm for the new SHA-3 standard and similar to AES. Based on previous Intel SSE implementations of Grøstl, 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 Grøstl implementations and NEON instructions
- ▶ Port Grøstl to ARM using NEON extensions
- ▶ Analyze and optimize the C/assembly implementation



Figure 1: Samsung Galaxy S2 with ARM NEON instructions.

Literature

- ▶ P. Gauravaram, L. R. Knudsen, K. Matusiewicz, F. Mendel, C. Rechberger, M. Schl affer, and S. S. Thomsen.
Grøstl – a SHA-3 candidate.
Submission to NIST, 2008.
Available online: <http://groestl.info>.
- ▶ E. K asper and P. Schwabe.
Faster and Timing-Attack Resistant AES-GCM.
In C. Clavier and K. Gaj, editors, *CHES*, volume 5747 of *Lecture Notes in Computer Science*, pages 1–17.
Springer, 2009.

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

Master Project

Studies: INF SW TEL TM

Prerequisites

- ▶ C programming

Advisor / Contact

martin.schlaeffer@iaik.tugraz.at