Fish and Begol on ARM

Advisor(s): Sebastian Ramacher

Institute for Applied Information Processing and Communications (IAIK)
Graz University of Technology, Austria

Motivation

Fish and Begol are signature schemes that only rely on symmetric-key primitives (block ciphers, hash functions), and are therefore viable candidates for post-quantum security. Since the underlying block cipher consists mostly of AND and XOR operations on wide words, an implementation can leverage the speedup provided by SIMD instruction sets for improved performance.
Recent ARM processors such as the Cortex-A15 used in some smartphones support the NEON instruction set which provides SIMD operations for operands up to 128 bit.

Goals and Tasks

- Get familiar with the signature schemes and the symmetric-key primitives.
- Understand the NEON instruction set.
- Implement the signature schemes optimized for ARM with NEON.

NEON™

ARM NEON.

Literature

- D. Derler et al.
  Digital Signatures from Symmetric-Key Primitives
  preprint

Deliverables

- Project files (zip, cleaned)
- Documentation (pdf)
- Presentation (pdf)

Schedule

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

Studies

☒ INF ☒ TEL ☒ SW ☒ TM

Prerequisites

- Basic cryptographic background
- C/C++ programming

Advisor / Contact

sebastian.ramacher@iaik.tugraz.at.