Cryptography for ARM NEON

The Cortex-A8 is a seventh generation CPU core designed and licensed by ARM. It is widely used on smartphones (Apple iPhone4, Samsung Galaxy S, Google Nexus S), multimedia systems (Apple TV, Apple iPod Touch) and development platforms (BeagleBone). All these electronic devices demand efficient and secure cryptographic libraries for e.g. data encryption or authentication.

Recent research has shown that implementations with variable execution timing may allow attackers to extract secret cryptographic keys stored on the device. Timing variances can occur due to implementation choices (e.g. data-dependent branches) or due to the internal architecture of the processor core (e.g. cache lines). In order to overcome this problem one needs to find alternative implementation strategies that are naturally immune to timing attacks. A possibility is to use bitslicing techniques that ensure independent data flows and avoid the use of look-up tables.

The goal of this thesis is to design and develop bitsliced implementations of block ciphers such as the Advanced Encryption Standard (AES) using an ARM processor with NEON technology. NEON is a vector instruction set extension that features a SIMD (Single Instruction, Multiple Data) engine with its own independent pipeline and 128-bit register file. Software development for NEON can be done directly in assembly language, or in C language through high-level function intrinsics.

The main objective of the thesis is to devise and achieve high-throughput cryptographic implementations, and compare them to state-of-the-art libraries for ARMv7 such as OpenSSL. Depending on the interests of the student it is possible to tweak the focus of the thesis to more practical scenarios, for instance, by devising implementations that provide security against side-channel attacks.

Practicalities

Promotor: Prof. Ingrid Verbauwhede
Daily supervision: Josep Balasch Furkan Turan
Josep.Balasch@esat.kuleuven.be Furkan.Turan@esat.kuleuven.be
office B01.22 office B01.23
Nature of the work: 20% literature, 20% theoretical work, 60% software
Number of students: 1 or 2

Master thesis proposal © 2017-2018 COSIC