Project Phase 1: A Detailed Analysis of SUPERCOP on the Dragonboard APQ8060.

Kevin Burns, Robert Lyerly, Reese Moore, Philip Kobezak
Virginia Polytechnic Institute & State University
1185 Perry Street, Blacksburg VA
{kevinpb, rlyerly, ram, pkobezak}@vt.edu

1 Introduction

Computers are a ubiquitous part of our society. As computers become increasingly connected, more of our daily lives are becoming digitized. As such, it is important that we find new ways to ensure security and privacy. The field of Cryptography involves designing algorithms and protocols as a means of ensuring services interact with each other in a secure, private way. Traditionally, cryptographic theory was used to develop algorithms that were highly efficient and very secure on large desktop CPUs. However, with the dawn of mobile computing there is an increased need for power-aware cryptography. Research in this field seeks to strike a balance, searching for algorithms that can be used in low-power settings while still being strong and secure. New cryptographic algorithms must be evaluated on a wide variety of hardware platforms to understand how they perform in practice.

Hash functions play an important part in cryptography. They are heavily used for authentication and digital signing, two components of cryptography that are necessary for information security. Designing a good hash function is a complex task - the algorithm must have several characteristics such as uniformity, efficiency and infeasability of reversing the hash. The National Institute of Standards and Technology (NIST) is responsible for maintaining many cryptographic algorithms, including hash functions. NIST recently held a competition to generate an alternative to SHA-1 and MD5 because of known attacks for these hash functions. Many different researchers submitted implementations to the competitions, and the Keccak algorithm was chosen as the official implementation for SHA-3 on October 2, 2012. However, the software hosted at http://bench.cr.yp.to contains all the SHA-3 implementations submitted to NIST so that anybody may test them. In the first phase of our project, we were tasked with benchmarking these submissions.

1.1 Hardware Overview

Our platform for the first phase of the project was a Snapdragon S3 APQ8060-based Dragonboard, used for prototyping and developing for the Android plat-

form (hereafter referred to as "the Dragonboard"). The Dragonboard implements a complete wireless phone system, including a wireless RF card, a sensor card (with accelerometer and gyroscope) and a touchscreen. The Snapdragon S3 APQ8060 contains several cores for computation and processing:

1. ARM1136J-S 384 MHz embedded microprocessor
2. Qualcomm dual-core Scorpion microprocessor (up to 1.7 GHz), which has the ARM NEON SIMD extensions
3. Qualcomm QDSP6000 and QDSP4000 DSP cores
4. ARM7 resource and power management microprocessor
5. Adreno 220 GPU

Most compute-intensive tasks are run on the larger Scorpion cores (which are designated as "application cores"), the QDSP6000 DSP and the Adreno 220 GPU. The ARMv7 instruction set architecture (ISA) is the 7th-generation of the ARM ISA. It is a RISC ISA and contains a standardized 3-stage pipeline (although implementations may contain longer pipelines) and 16 x 32-bit registers. ARMv7 also defines the NEON SIMD extensions which specify the interface to a 128-bit SIMD core with an independent pipeline and register file. It can perform basic arithmetic and logic operations on varying size data types, including signed/unsigned 8-bit, 16-bit, 32-bit or 64-bit words. The QDSP6000 (or "Hexagon") DSP is a programmable DSP designed for application use. It has several features which make it a flexible platform, including symmetric multiprocessing and VLIW/SIMD instructions (in fact, Linux has been ported to run on the Hexagon). The Adreno 220 GPU is used for 2D and 3D rendering on Android. It implements several graphic APIs and can be used concurrently by several of the other cores for interleaving CPU, DSP and graphics operations.

1.2 Problem Statement

The objective of the first phase of the project was to do a detailed perfomance profiling for a set of hash algorithms provided by the SUPERCOP testsuite. The analyses should try to determine why each algorithm implementation excelled, compared to other implementations, on the target platform (Dragonboard APQ8060).