Embedded SIMD Architecture Extensions and its Applications in Cryptography

With mobile devices on the rise, and mobile internet becoming cheaper and faster all the time, communication over the Internet is increasing rapidly. The aim of mobile computing is to offer as much performance as possible, while at the same time maximising battery life. This combination of factors means that software has to become optimised in order to use as little of the sparse resources on these devices as possible.

In order to provide secure communication on these devices, cryptographic operations have to be carefully developed to prevent needless computing cycles - and hence decreased battery life. Some of the most common processors available in the mobile segment offer hardware cryptographic engines for common used protocols such as AES. However, these hardware units are not programmable and using different algorithms than the one provided by the hardware vendor is not possible. Furthermore, most hardware vendors offer different blocks of functionality, meaning it is not easy to develop a single application across multiple vendors – increasing development costs.

Another trend in mobile computing is the use of specific co-processors commonly known as Single Instruction Multiple Date (SIMD) units or vector engines. These can be used to execute certain operations in a parallel way, effectively doing more work with less clock cycles – especially useful for multimedia. This paper deals with how we can use those SIMD engines to take on an inherent non-trivial parallelizable problem such as cryptographic operations. The added benefit of having similar SIMD engines available across the mobile processor spectrum, and compiler support for these engines, means lower development costs and easier porting between platforms.