

INSTRUCTION SET ARCHITECTURE FOR
ACCELERATING CRYPTOGRAPHIC PROCESSING IN
WIRELESS COMPUTING DEVICES

A. Murat Fiskiran

A DISSERTATION
PRESENTED TO THE FACULTY
OF PRINCETON UNIVERSITY
IN CANDIDACY FOR THE DEGREE
OF DOCTOR OF PHILOSOPHY

RECOMMENDED FOR ACCEPTANCE
BY THE DEPARTMENT OF
ELECTRICAL ENGINEERING

September 2005

Abstract

Two main classes of cryptography algorithms used to protect digital data on computer systems and communication networks are *symmetric-key* and *public-key* ciphers. Used with appropriate security protocols, symmetric-key ciphers provide data *confidentiality*, while public-key ciphers provide *authentication* and *digital signatures*. As network connectivity proliferates, processing of both symmetric-key and public-key ciphers will be an increasing part of the workload of programmable networked devices, from servers to smartcards and sensors.

This thesis explores instruction set architecture (ISA) techniques to accelerate cryptographic processing in programmable processors. We select a representative suite of ciphers, including older, well-entrenched ciphers like DES and 3DES, as well as newer ciphers like AES and ECC, which are more efficient for constrained environments. We perform a detailed workload characterization of this cipher suite to characterize the common and frequent operations in both symmetric key ciphers and public-key ciphers. We propose new instructions to accelerate the performance-critical operations. Examples are ISA enhancements for fast parallel table lookups in symmetric-key ciphers, and multi-precision polynomial arithmetic in public-key ciphers. We synthesize these ISA proposals in PAX, a tiny crypto-processor for very high-performance yet low-cost cryptographic processing. The ISA extensions used in PAX can also be added to any microprocessor or embedded processor. We verify the versatility of these ISA extensions by showing their usefulness in accelerating other applications, such as binary field arithmetic and error correction coding.

A distinctive property of PAX is *wordsize scalability*: the same instruction set can be synthesized into processors with different word sizes. This allows the performance and cost of PAX processors to be scaled and targeted for platforms with different levels of computational resources, ranging from smartcards to handheld wireless devices to servers. Combined with wordsize scaling, the novel ISA features in PAX provide huge speedups, up to 41.4× for AES, a symmetric-key cipher, and 27.8× for ECC, a public-key cipher, compared to a basic RISC processor.