A Generic Approach to the Development of Coprocessors for Elliptic Curve Cryptosystems

ECE Ph.D. Seminar
By
Rabia Shahid

Ph.D. Advisor:
Dr. Kris Gaj

Monday, July 24th, 2017
10:00 – 11:00 AM

ENGR 3507

Abstract

Cryptographic engineering is a field that combines cryptology, algebraic geometry, and number theory with methods from computer arithmetic, digital system design, and computer architecture. Unfortunately, most of the researchers working in this area are either mathematicians/cryptographers or computer engineers, specializing in their respective fields. The theoretical complexities related to number theory and abstract algebra in the majority of public-key cryptosystems can easily prevent computer engineers from fully optimizing their designs.
In this talk, we describe a possible bridge between these two domains, demonstrated using a family of Elliptic Curve Cryptosystems (ECC). We present the design of a configurable and generic execution unit for ECC that serves as a coprocessor to perform operations involved during a scalar multiplication. The execution unit is supported by a software static scheduler to automate the cumbersome process of manual scheduling of operations involved in ECC. The arithmetic unit performs the operations at the lowest level of hierarchy, i.e., prime field arithmetic. We focus on optimizing the overall performance of the cryptoprocessor by using an optimal number of multiplier units, capable of taking full advantage of the parallelism present in the algorithm and a single modular adder/subtractor, working in parallel with multipliers. An instruction set architecture capable of supporting all required instructions is designed, along with the coprocessor that can process multiple batches of instructions using the arithmetic unit. We report results for an entire scalar multiplication in terms of latency in clock cycles and in absolute time units. We also demonstrate that the entire setup is generalizable to any cryptosystem that involves modular multiplications and modular additions/subtractions at the lowest level of hierarchy.