Notice and Invitation

Oral Defense of Doctoral Dissertation
The Volgenau School of Engineering, George Mason University

Rabia Shahid
Bachelor of Science, COMSATS Institute of Information Technology, 2007
Master of Science, George Washington University, 2010

A NEW APPROACH TO THE DEVELOPMENT OF COPROCESSORS FOR PAIRING-BASED CRYPTOSYSTEMS

July 31, 2017, 2:00-4:00pm
Engineering Building, Room 3507
All are invited to attend.

Committee
Dr. Kris Gaj, Chair
Dr. Jens-Peter Kaps
Dr. Houman Homayoun
Dr. Massimiliano Albanese

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. One of the most established state-of-the-art solutions is Elliptic Curve Cryptography (ECC). One of the most promising emerging approaches is Pairing-Based Cryptography (PBC). PBC-based security services, such as non-interactive key agreement, identity-based encryption (IBE) and short signatures, solve problems beyond the range of traditional cryptographic schemes, and make cryptographic solutions less costly, less cumbersome, and easier to deploy. The broad spectrum of ECC and PBC schemes available in the literature and a wide-range of possible parameter choices requires deep understanding of the possible trade-offs and dependencies among the parameter values and efficiency of the corresponding hardware implementations.

In this research, we describe a possible bridge between the aforementioned two domains, demonstrated using selected families of Elliptic Curve and Pairing-Based Cryptosystems. We present the design of a configurable and generic execution unit that serves as a coprocessor to perform operations involved in these cryptosystems. The execution unit is supported by a software static scheduler to automate the cumbersome process of manual scheduling of operations required by these algorithms. The arithmetic unit performs the operations at the lowest level of hierarchy, i.e., at the level of prime field arithmetic. We focus on optimizing the overall performance of the crypto-processor by using an optimal number of multiplier units, capable of taking full advantage of the parallelism present in an implemented 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 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.