1

Introduction

This chapter presents a complete outline for this Book. It explains the main goals pursued, the strategies chosen to achieve those goals, and a summary of the material to be covered throughout this Book.

1.1 Main goals

The choice of reconfigurable logic as a target platform for cryptographic algorithm implementations appears to be a practical solution for embedded systems and high-speed applications. It was therefore planned to conduct a study of high-speed cryptographic solutions on reconfigurable hardware platforms.

Both efficient and cost effective solutions of cryptographic algorithms are desired on reconfigurable logic platform. The term "efficient" normally refers to "high speed" solutions. In this Book, we do not only look for high speed but also for low area (in terms of hardware resources) solutions.

Our main objective is therefore to find high speed and low area implementations of cryptographic algorithms using reconfigurable logic devices. That implies careful considerations of cryptographic algorithm formulations, which often will lead to modify the traditional specifications of those algorithms. That also implies knowledge of the target device: device structure, device resources, and device suitability to the given task. The design techniques and the understanding of the design tools are also included in the implications imposed by efficient solutions. An optimized cryptographic solution will be the one for which every step; starting from its high-level specification down to the physical prototype realization is carefully examined.

It is known that the final performance of cryptographic algorithms heavily depends on the efficiency of their underlying field arithmetic. Consequently, we begin our investigation by first studying the algorithms, solutions and corresponding architectures for obtaining state-of-the-art finite field arithmetic

realizations. Our study was carried out for both, prime and binary extension finite fields. We investigated field arithmetic algorithms for the operations of field addition, multiplication, squaring, square root, multiplicative inverse and exponentiation among others.

Thereafter, we selected a set of three of the most important cryptographic building blocks, for their implementation on reconfigurable logic devices: hash functions, symmetric block ciphers and public key cryptosystems in the form of elliptic curve cryptography.

We described first the basic principles for attaining efficient hardware implementation of hash functions. In the subject of symmetric ciphers, we study the two most emblematic algorithms, namely, the Data Encryption Standard (DES) and the Advance Encryption Standard (AES). In the case of asymmetric cryptosystems we analyze fast implementations of Elliptic Curve operations defined over binary extension fields.

Several considerations were made to achieve high speed and economical implementations of those algorithms on reconfigurable logic platforms. One of them was to exploit high bit-level parallelism where and whenever it was possible. Similarly, we employed design techniques especially tailored for exploiting the structure of the target devices.

A variety of hash function algorithms were studied first. Emphasis was made on MD5, by providing a step-by-step analysis of its algorithm flow. An explanation of the SHA-2 family was also included. In our descriptions we pondered hardware implementation aspects of the hash algorithms.

DES was the second cryptographic building block studied in this Monograph. The basic primitives involved in block ciphers specifically for DES were analyzed for their implementations on reconfigurable logic platform. A compact one round FPGA implementation of DES was carried out exploiting high bit-level parallelism. Experiments were made for optimizing the proposed FPGA architecture with respect to hardware area.

A more detailed study was planned regarding AES due to its importance for the current security needs in the IT sector. Each step of the algorithm was investigated looking for improvements in the standard transformations of the algorithm and for an optimal mapping to the target device. Both, iterative and pipeline approaches for encryption were used for AES FPGA implementation. We attempted to reduce the critical paths for encryption/decryption by sharing common resources or optimizing the standard transformations of the algorithm.

In the case of Elliptic Curve Cryptography (ECC), we utilized a hierarchical six-layer model, but only the lower three layers were addressed in this Book. The first layer of the model deals with the efficient implementation of finite field arithmetic. The Second layer makes use of the underlying arithmetic for implement elliptic curve arithmetic main primitives: point addition and point doubling. The third layer implements elliptic curve scalar multiplication which is achieved by adding n copies of the same point P on the curve. Both the point addition and doubling operations from the second layer serve

as building blocks for the third layer. We strived for using parallel techniques for all the three layers. This way, a generic architecture for the elliptic curve scalar multiplication was proposed and implemented on the FPGA platform. We also presented parallel formulations of the scalar multiplication operation on Koblitz curves an architecture that is able to compute the elliptic curve scalar multiplication using the half-and-add method. Additionally, we presented optimizations strategies for computing a point addition and a point doubling using LD projective coordinates in just eight and three clock cycles, respectively.

1.2 Monograph Organization

Next chapters present a short introduction to the cryptographic algorithms chosen to illustrate the design strategies discussed previously as well as the mathematical background required for the correct understanding of the material to be presented. Design comparisons and conclusion remarks are presented at the end of each Chapter. A short summary of each chapter is given below.

In Chapter 2, a brief review of modern cryptographic algorithms is given. Topics addressed include: Secret-key and public-key cryptography, hash functions, digital signatures, an so forth. Furthermore, we also discuss in this Chapter potential real-world cryptographic applications and the suitability of reconfigurable hardware devices for accommodate them.

In Chapter 3 a brief introduction to reconfigurable hardware technology is given. We explain the historical development of FPGA devices and include a detailed description of the FPGA families of two major manufacturers: Xilinx and Altera. We also cover reconfigurable hardware design issues, metrics and security.

In Chapter 4, some important mathematical concepts are presented. Those concepts are particularly helpful for the understanding of cryptographic operations for AES and elliptic curve cryptosystems. Key mathematical concepts for a class of elliptic curves are also described at the end of this Chapter.

In Chapter 5, we discuss state-of-the-art arithmetic algorithms for prime fields. We present efficient hardware design alternatives for operations such as adders, modular adders, modular multipliers and exponentiation among others. We give at the end of each Section a comparison analysis with some of the most significant works reported in this topic.

In Chapter 6, state-of-the-art algorithms for binary extension fields are studied. We discuss relevant algorithms for performing efficiently field multiplication, squaring, square root, inversion and reduction among others. We give at the end of each Section a comparison analysis with some of the most significant works reported in this topic.

In Chapter 7, we study efficient reconfigurable hardware implementations of hash functions. Specifically, we carefully analyze MD5, arguably the most studied hash function ever. We give at the end of each Section a comparison analysis with some of the most significant works reported in this topic.

In Chapter 8, a general guideline for implementing symmetric block ciphers is described. Basic primitives involved in block ciphers are listed and design tips are provided for their efficient implementations on reconfigurable platform. DES is presented as a case of study. A compact and fast DES implementation on reconfigurable platform is explained. We give at the end of this Chapter a comparison analysis with some of the most significant works reported in this topic.

In Chapter 9, we explore multiple architectures for AES. Several efficient techniques for AES implementation are described. Several efficient AES encryptor and encryptor/decryptor cores based on those techniques are presented on reconfigurable platforms. The benefits/drawbacks of all AES cores are examined. We give at the end of this Chapter a comparison analysis with some of the most significant works reported in this topic.

In Chapter 10 we discuss several algorithms and their corresponding hardware architecture for performing the scalar multiplication operation on elliptic curves defined over binary extension fields $GF(2^m)$. By applying parallel strategies at every stage of the design, we are able to obtain high speed implementations at the price of increasing the hardware resource requirements. Specifically, we study the following four different schemes for performing elliptic curve scalar multiplications,

- Scalar multiplication applied on Hessian elliptic curves.
- Montgomery Scalar Multiplication applied on Weierstrass elliptic curves.
- Scalar multiplication applied on Koblitz elliptic curves.
- Scalar multiplication using the Half-and-Add Algorithm.

1.3 Acknowledgments

We would like to thank to all the long list of people who contribute to the material presented in this Book, needless to say that all of them are worthy to be mentioned. We gratefully thank our former Master's students: Juan Manuel Cruz-Alcaraz, Sabel Mercurio Hernández-Rodríguez and Emmanuel López-Trejo who contribute with their hard work and talent to the design and testing of several architectures presented in Chapters 6, 9 and 10. We would also like to thank our colleagues Guillermo Morales-Luna, Julio López-Hernández, Nareli Cruz-Cortés, Tariq Saleem, Shamim Baig, Habeel Ahmed, Erkay Savas, Tugrul Yanik, Luis Gerardo De-La-Fraga and Carlos Coello Coello who provided priceless comments and advice which greatly helped us to improve the

contents of this Book. We also acknowledge valuable contributions from Karla Gómez-Avila, Marco Negrete-Cervantes, Víctor Serrano-Hernández, Alejandro Arenas-Mendoza, Guillermo Martínez-Silva and Carlos López-Peza. We gratefully acknowledge our Springer editor, Jason Ward, for his diligent efforts and support towards the publication of this Work.

Last but not least, the first and third authors acknowledge support from CONACyT through the NSF-CONACyT project number 45306. The second author acknowledge support from the faculty and staff members of the Centre for Cyber Technology and Spectrum Management (CCT & SM), National University of Sciences and Technology (NUST), Islamabad-Pakistan.