Chapter 1:

INTRODUCTION

1-1. Motivation

Efficient hardware implementation of elliptic curve cryptosystems (ECCs) in resource-constrained devices is important in many applications on small devices such as smart cards, radio-frequenciy identification (RFID), and wireless sensor networks. Computations in finite fields combined with low-hardware-complexity architectures are important in many areas, including coding theory, computer algebra systems, and public-key cryptosystems (e.g., ECCs). Although all finite fields of the same cardinality are isomorphic, their arithmetic efficiency depends greatly on the basis used for field element representation. The most commonly used are polynomial basis (PB) and normal basis (NB).

Polynomial basis: **PB** may also refer to a basis of the extension of the form {1, α,……., α^{m-1} } where α is the root of a primitive polynomial of degree m equal of the degree of the extension.

Normal basis: NB GF(2^m) is a basis of the form $\left(\beta.\beta^2.\beta^4.\beta^8.\ldots\ldots\beta^{2^{(m-1)}}\right)$, where $\beta \epsilon GF(2^m)$.

Arithmetic over NB finite fields GF(2^m) has recently been used in many significant applications, including error-correcting codes, cryptography, digital signal processing, switching theory and pseudorandom number generation. Addition, multiplication, exponentiation, and inversion are the most important computations in finite field arithmetic. Therefore, fast multiplication algorithms with low circuit complexity are much desired. Because such computations cannot be performed in real time on general-purpose computers, hardware-efficient architectures for multiplication in GF(2^m) are highly desirable.

1-2. Main Contribution

The contributions in this thesis are as follows:

- We propose a new compact optimal normal basis field arithmetic unit (FAU).
- We reduce the area cost in terms of NAND gates compared to a standard FAU.
- We reduce the area cost in terms of NAND gates compared to the research done in 3.1.
- We reduce the number of slice regiters and slice lookup tables compared to a standard FAU.
- We model the proposed design using VHDL and Implement it on Xilinx Artix7 XC7A200T FPGA over GF(2^{173}, 2^{233}, 2^{350}, 2^{515}),

1-3. Thesis Organization

The remainder of this thesis is organized as follows: Chapter 2 introduces the required background on the field of arithmetic operations and optimal normal basis. Chapter 3 presents the literature review. Chapter 4 describes the design methodology of the FAU proposed in this thesis. Chapter 5 shows the results of implementing the design and comparing it to the standard FAU. Chapter 6 concludes the thesis and discusses future work.

1-4. Chapter Summary

In this Chapter, we mentioned the motivation for the thesis and what contributaions were made. Also the whole structure of the thesis was explained. In the next Chapter we mention some background information regarding field arithmetic and optimal normal basis.