Table of Contents

Chapter 1: Introduction……………………………………………………………...…12

1.1 Motivation……………………..……………….……….…....…..12

1.2 Main Contribution………………………………………………. .13

1.3 Thesis Organization …………………………………………………13

1.4 Chapter Summary……………………………………………………13

Chapter 2: Background Information…………………………………………..…..14

2.1 Finite Field Arithmetic……………………...…………...…...…14

2.2 Arithmetic Logic Unit ………..………..…………...……..……15

2.3 GF(2^m) Arithmetic……………………..…………………..……..16

2.4 Optimal Normal Basis…………………………………..………..16

2.5 Types of Optimal Normal Basis…………………………………......18

2.6 Elliptic Curve Cryptography………………….……..……..…….19

2.7 Chapter Summary………………………………………...………19

Chapter 3: Literature Review……………………………...…………….……..20

3.1 Pipelined Multiplicative Inverse Architecture for AES……..…..….20

3.2 Low-complexity Hardware Architecture of Gaussian Normal Basis Multiplication over GF(2^m) ……………………………...……...22

3.3 Massey-Omura multiplier ……….…….…………..………………23

3.4 Itoh-Tsuji inversion algorithm…….……………………………..……25

3.5 Fast Inversion in GF(2^m) with Normal Basis Using Hybrid-Double Multipliers. ……………………….…………………………26

3.6 Small FPGA based Multiplication-Inversion Unit for Normal Basis Representation in GF(2^m)…………………………………….…..…..27

3.7 Chapter Summary ………………….……..………………………28

Chapter 4: Methodology ………………..……………….…………………..……29

4.1 The Proposed Design…………………………..……..…………..……29

4.2 Operations of the Proposed FAU……………………..……….......….30

4.3 Chapter Summary…………………………………….…………..…..32

Chapter 5: Implementation Results …………..……………………..……...........…....33

5.1 Evaluating the Proposed Design……………………..…….............…33

5.2 Implementing the Design in VHDL……….…………….………......35

5.3 Comparing Slice Registers and LUTs with the Standard Design…......36

5.4 Running the Design on Different Numbers of Bits.............................37

5.5 Analyzing the results……………………………………….....……38

5.6 Chapter Summary...…..42

Chapter 6: Conclusion……………………………………………………..…...…43

References ……………………………………………………..……………......…..44

List of Tables

Table 1. Area cost of proposed design in terms of NANDs ………..……………….…..….34

Table 2. Comparing area cost of pipelined multiplicative Inverse with our design ...…35

Table 3. Synthesize results of 173-bit input……………………………………….....…35

Table 4. Comparison of slice registers in LUTs of 173-bit design…………………….36

Table 5. Comparing the proposed and standard design for different numbers of bits....37

List of Figures

Figure 1. Multiplicative inverse gate implementation over GF$(2^4)^2$ using a pipeline...21

Figure 2. Proposed structure of the digit-serial GNB multiplier over GF(2^7)…..……..22

Figure 3. 5-bit Massey-Omura Multiplier Circuitry …...…..…………….....…….……....24

Figure 4. The proposed inverter architecture using a hybrid-double multiplier……......27

Figure 5. Architecture of the multiplication-inversion unit (MIU)………….……...…28

Figure 6. Proposed FAU design…………………….………………………...…..30

Figure 7. Comparing slice registers of the standard and proposed design……………..38

Figure 8. Comparing LUTs of the standard and proposed design……………....…...38

List of Algorithms

Algorithm 1: Massey-Omura multiplication …………..……………………………….24

Algorithm 2: Itoh-Tsujii inversion…………………………………………………..26

Algorithm 3: Itoh-Tsuji inversion in the proposed FAU……………………..………..31