**A HEXAR ITOH-TSUJII INVERSION ALGORITHM OVER TRINOMIAL GALOIS FIELD FOR CRYPTOGRAPHIC APPLICATIONS**

# D78 Project

*Submitted in partial fulfillment for the requirement of B.E. degree in Electronics and Communication Engineering of Anna University*

#### Submitted by

##### R.MEENA

***(Reg. No: 13D46)***

***N.MEENAKSHI***

***(Reg. No: 13D47)***

#### Guided by

## ***Dr.V.R.VENKATASUBRAMANI***



# *Department of Electronics and Communication Engineering*

### **THIAGARAJAR COLLEGE OF ENGINEERING**

(An Autonomous Institution Affiliated To Anna University, Chennai)

**MADURAI – 625 015**

***November 2016***

###### **THIAGARAJAR COLLEGE OF ENGINEERING**

**(An Autonomous Institution Affiliated to Anna University, Chennai)**

**MADURAI – 625 015.**



BONAFIDE CERTIFICATE

This is to certify that the D78 Project entitled “A HEXAR ITOH-TSUJII INVERSION ALGORITHM FOR TRINOMIAL GALOIS FIELD FOR CRYPTOGRAPHIC APPLICATIONS”, being submitted by *R.MEENA*(13D46) and *N.MEENAKSHI* (13D47) in partial fulfillment for the requirement of Bachelor of Engineering Degree in Electronics and Communication Engineering, is a record of bonafide work done by them during the year 2016-2017 under my supervision. The results embodied in this report have not been submitted to any other university or institute for the award of any degree or diploma.

Dr.V.R.Venkatasubramani,M.E.,Ph.D Dr.Mrs.R.Sukanesh, M.E.,Ph.D

Assistant Professor, Professor and Head,

Department of ECE, Department of ECE,

Station: Madurai Date:

Certified that the Candidate was examined in the Viva-Voce Examination held at Thiagarajar College of Engineering, Madurai on \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

INTERNAL EXAMINER EXTERNAL EXAMINER HDECE.

ACKNOWLEDGEMENTS

We express our heartfelt thanks to Dr.V.ABHAIKUMAR, Principal of Thiagarajar College of Engineering for providing all the facilities and allowing us to do the project in the college campus.

We express our heartfelt thanks to Dr.Mrs.R.Sukanesh , Head of ECE Department for allowing us to use the necessary facilities in the lab to successfully complete this project in the campus itself.

We wish to express our profound gratitude and heart thanks to Dr.S.Rajaram ,VLSI head and our guide Dr.V.R.Venkatasubramani, Assistant Professor, ECE department for the able guidance, immense help, encouragement and providing us the necessary facilities throughout the project.

We convey our sincere thanks to all the staff members , parents and friends who guided us throughout our B.E course.

R.MEENA

N.MEENAKSHI

## **LIST OF CONTENTS**

|  |  |
| --- | --- |
| **Item** | **Page No.** |
| Title Page | i |
| Certificates | ii |
| Acknowledgement | iii |
| List of contents | iv |
| List of figures | vi |
| List of tables | vii |
| Abstract | viii |
| CHAPTER.1.INTRODUCTION   * 1. Introduction   2. Cryptology   3. Security goals | 1  1  1  4 |
| CHAPTER.2.MATHEMATICAL BACKGROUND  2.1. Abstract algebra  2.1.1 Groups, Rings and Fields  2.2. Binary Finite Field | 6  6  6  8 |
| CHAPTER.3.LITERATURE REVIEW | 13 |
| CHAPTER.4.METHODOLOGY.  4.1 Multiplicative Inverse Algorithm  4.1.1 The Itoh Tsujii Algorithm  4.1.2 Quad Itoh Tsujii Algorithm  4.2 Finite Field multipliers  4.2.1 Karatsuba multiplication  4.2.2 The Hybrid Karatsuba multiplier | 16  16  16  19  22  23  24 |
| CHAPTER.5.PROBLEM DESCRIPTION | 27 |
| CHAPTER.6.PRESENT WORK  6.1 Hexar Itoh Tsujii Algorithm  6.1.1 Proposed Hexar structure  6.1.2 Hardware Architecture | 28  28  30  34 |
| CHAPTER.7. RESULTS AND DISCUSSIONS | 39 |
| CHAPTER.8. CONCLUSION AND FUTURE WORK | 41 |
| REFERENCES | 42 |

**LIST OF FIGURES**

|  |  |  |
| --- | --- | --- |
| **Figure No.** | **Description** | **Page No.** |
| 1.1 | Communication model | 5 |
| 2.1 | Squaring circuit | 10 |
| 2.2 | Modular reduction with trinomial x233+x74+1 | 11 |
| 4.1 | 233 Hybrid Karatsuba Multiplier tree | 25 |
| 6.1 | Hexar block Design: Raises the Input to the Power of 16k | 35 |
| 6.2 | Hexar-ITA Architecture for GF (2233) with the Addition Chain | 36 |
| 7.1 | Multiplicative inverse of (x8+x7+x6+x5+x4+x3+x2  +x+1) in GF(2m) | 40 |

**LIST OF TABLES**

|  |  |  |
| --- | --- | --- |
| **Table No.** | **Description** | **Page No.** |
| 4.1 | Brauer addition chain for 233 | 18 |
| 4.2 | Inverse of a ∈ GF (2233) using ITA | 19 |
| 4.3 | Inverse of a ∈ GF (2233) using Quad ITA | 21 |
| 6.1 | LUTs for Hexar block | 31 |
| 6.2 | Comparison of LUTs Required for a Squarer, Quad and Hexar Circuit for GF (29) | 32 |
| 6.3 | Inverse of a ∈ GF (2233) using Hexar ITA | 33 |
| 6.4 | Control Word for GF (2233) Hexar ITA | 37 |
| 7.1 | Comparison of Quad and Hexar circuits | 39 |
| 7.2 | Comparison on the performance of Quad and Hexar | 39 |

**ABSTRACT**

With the development in internet and communication technologies the need for security in sharing private information. Public key cryptography is widely used in establishing secure communication channels between the users on the internet.Public key cryptography relies on algorithms from computer arithmetic,number theory and algebra. Elliptic curve cryptography (ECC) has become major focus of research attention because of its short key sizes and security. Multiplicative inverse is a major part in the public key generation .Also it is considered complex in nature due to the number of arithmetic operations .Hence there are several algorithms in optimizing the operation .One such algorithm is Itoh-Tsujii algorithm. However ,to match the ever increasing requirement for the speed in today’s applications ,further optimizations are necessary . We have presented the Hexar ITA for trinomial Galois Field (GF) which reduces the arithmetic operations and hardware requirement for the computation of inverse compared to the existing algorithms.It has been implemented on a Xilinx Virtex 4 FPGA.