INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume3, Issue2)
Available online at www.ijariit.com

A Comparative Study of RSD Based ECC Processor Using Karatsuba Algorithm and Vedic Multiplier

Mitha Raj
Cochin College of Engineering and Technology
mitharaj12@gmail.com

Amarjith Singh
Cochin College of Engineering and Technology
amarjith@cochincet.ac.in

Abstract: Elliptic curve cryptography is the most secure public key encryption technique public key encryption means different keys for encoding and decoding. The processor based on RSD (redundant signed digit). The processor employs Karatsuba of man method and Vedic multiplier for multiplication purpose. The processor can do all the arithmetic operation using an ALU (arithmetic logic unit). A comparative study between these algorithms to achieve high throughput multiplication. The implementation result based on Xilinx Spartan 3E XC3S1600E shows that the proposed algorithm can do scalar point multiplication p256.

Keywords: Redundant Signed Digit Elliptic Curve Cryptography.

INTRODUCTION

Elliptic curve cryptographic system is an asymmetric cryptographic system. It offers same security to RSA whereas in RSA larger keys are used. Scalar point multiplication is the basic operation. For carrying free arithmetic redundant signed digit can be used.

Cubic equation for the elliptic curve

$$Y^2 + AXY + BY = X^3 + CX^2 + DX + E$$

This equation is known as wier strass equation where A, B, C, D, E are real numbers and X and Y take on the values in real numbers.

General equation is

$$Y^2 = X^3 + AX + B$$

The smoothness of curve and distinct roots can be explained using $4A^3 + 27B^2 \neq 0$

The points on the curve (p, q). The coordinates of the point addition results a= (p1, q1) and b= (p2, q2). Therefore the resultant R =a +b = (p3, q3)

$P3 = ((q2-q1)/ (p2-p1))^2 - p1 - p2$

$Q3 = ((q2-q1)/ (p2-p1)) (p1 - p3) - q1$

CONTENTS

1.1 REDUNDANT SIGNED DIGIT

The redundant signed digit representation is a carry free arithmetic. It can avoid lengthy data path. The integers are represented by using the difference of two other integers. One integer P is represented by the difference of P^+ and P^- components. The main advantage is that it can avoid lengthy data path and performing addition and subtraction without the use of two's complement representation. The integers are 1, 0,-1.

1.2 KARATSUBA ALGORITHM

This algorithm is a fast multiplication algorithm. Multiplication using the school book method of O (n^2) and its complexity is O ($n^{1.58}$).

Let X and Y represented as n digits strings in base B.

$$X = X1B^M + X0$$

$$Y = Y1B^M + Y0$$

Then multiplication of operands

$$XY = (X1B^M + X0)(Y1B^M + Y0)$$

$$XY = Z2\ B^{2M} + Z1\ B^M + Z0$$

Where $Z2 = X1Y1$

$Z1 = X1Y0 + X0\ Y1$

$Z0 = X0\ Y0$

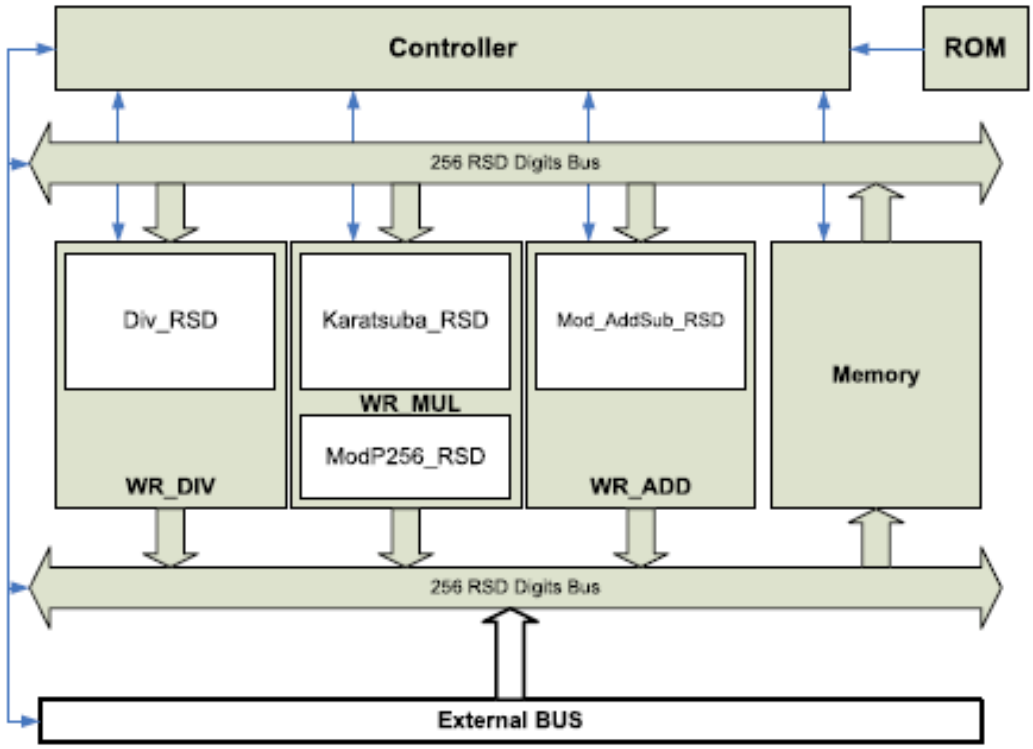
This method reduces 4 steps into 3 steps.

1.3 VEDIC MULTIPLIER

The Vedic multiplier is based on 16 sutras. For multiplication purpose, Urdhava Tribhagyam and Nikhilam Sutras are used. It is based on vertical and crosswise. The main advantage of Vedic multiplier is reduced complexity in calculations.

1.4 OVERALL PROCESSOR ARCHITECTURE

The ECC processor consists of an arithmetic unit, memory, and two data buses. Arithmetic unit includes modular addition or subtraction, multiplication block, modular division block. For division extended eucleadian algorithm is used. For addition purpose, new adder is proposed. The adder consist of two layers .layer 1 generate the carry and interim sum and layer 2 generates the only sum.



Overall Processor Architecture Using Karatsuba Algorithm

RESULTS

RESULTS OF KARATSUBA ALGORITHM

Number of IOs	1028
Number of LUTs	512
Combinational path delay	94.95ns

RESULTS OF VEDIC MULTIPLIER

Number of IOs	1024
Number of LUTs	9312
Combinational path delay	463.664

CONCLUSION

This paper concluded that Karatsuba multiplier is faster than Vedic multiplier. Vedic more multiple carries large combinational path delay.

