ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Comparative Analysis of Arithmetic Operations in an ECC Processor using RSD and CSD based Representation

Gayathri Devi R

PG Scholar, Dept. of ECE, TKM Institute of Technology, Kollam, Kerala, India

ABSTRACT: Nowadays, secure information exchange is an important issue for the communication network. Elliptic curve cryptography (ECC)s is a type of cryptography which can provide same level of security but with much shorter key size. The main operation in ECC is scalar point multiplication in which a point on the curve is multiplied by a scalar. This scalar point multiplication is done through point additions and point doubling which in turn is done through series of multiplications, additions, and subtraction and division operations. Various ECC processors that target prime fields, binary fields are there which depends on the modulus they take. In prime field ECC processors the carry propagation can be limited by using the RSD based representation in which the digits are represented by difference of its positive component and negative components. A modular adder unit along with a modular subtraction unit was done in which the RSD digits were given as the input .And also Karatsuba multiplier along with recursive and iterative was done. The same units were done with the CSD representation and a comparison of both representations was done.

KEYWORDS: Elliptic curve cryptography (ECC) ; Redundant signed digit (RSD) ; Canonical Signed Digit(CSD).

I. INTRODUCTION

Elliptic curve cryptography (ECC) is an asymmetric key cipher adopted by the IEEE and NIST as it offers more security per key bit compared to other contemporary ciphers. Security in ECC based cryptosystems is achieved through elliptic curve scalar multiplication. ECC offers the highest strength per bit and the smallest key size when compared with other public-key cryptosystems by exploiting the mathematical basis of ECC.

Although elliptic curves (ECs) can be defined on a variety of different fields, only finite fields are employed for cryptography. Among them, prime fields F_p and binary extension fields are considered to be the ones that offer the most efficient and secure implementations. The operands of ECC operations are large finite field elements. A point scalar multiplication is performed by calculating a series of point additions and point doublings. By their geometrical properties, points are added or doubled through series of additions, subtractions, multiplications and divisions of their respective coordinates.

Redundant signed digits can be used to perform the arithmetic operations in ECC processor. Redundant signed digit representation is a signed digit representation in which the integers are represented by the difference of its positive and negative components. It uses the set of digits {1,0 -1} . Another representation which can be used is the CSD representation or the Canonical signed digit representation in which the numbers are represented using the digits { 1,0,-1}

II. RELATED WORK

A.ECC processor using carry save arithmetic

Carry save addition can be used in modular addition operation in an ECC processor in which outputs two sequence of numbers ; one a sequence of partial sum bits and another a sequence of carry bits .But it cannot be used for modular addition or subtraction since we do not know that the intermediate result is greater or lesser than

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

B. Modular multiplication using Montgomery method

Modular multiplication in an ECC processor can be done using transforming the operand into Montgomery domain .But the transformation is a difficult process . So we opt for Karatsuba multiplication in which the operands are To be multiplied are splitted into two equal halves and then multiplied.

III. METHODOLOGY

A.ECC processor

Arithmetic operations in ECC processor includes Modular addition, multiplication subtraction . RSD based and CSD based addition and multiplication can be done.RSD based representation is the redundant signed digit representation In which the integers are represented by the difference of its positive components and negative components. In CSD based representation the integers are represented by the digits {1,0,-1} but it has minimal non zero digits.

i) RSD based modular addition

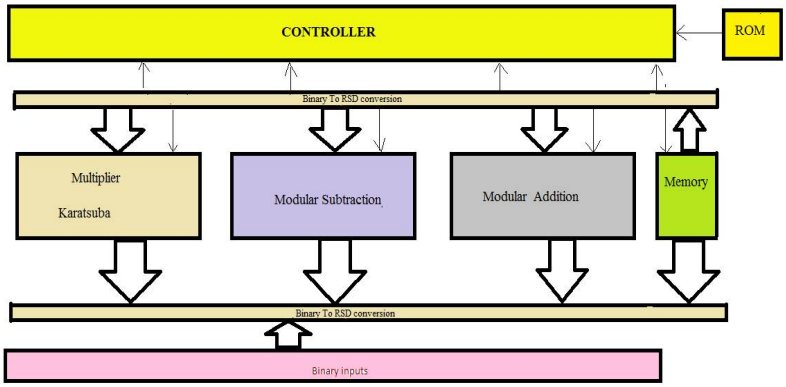

Fig 1. Architecture of ECC

i) RSD based modular addition

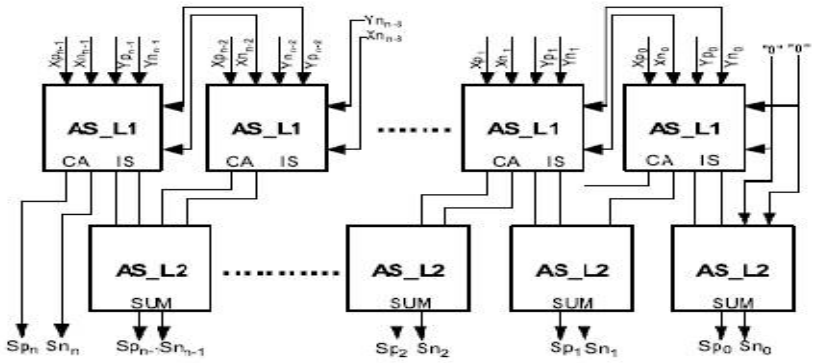

Fig 2. RSD adder

An RSD adder consists of two layer . Layer 1 generates the interim sum and the carry and layer 2 generates the sum.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

The same adder can be used for CSD addition. Layer1 works by ensuring that layer 2 does not generate any overflow by using the values from layer 1. The *n*-digits modular addition is performed by three levels of RSD addition. Level 1 performs the basic addition of the operands which produces $n + 1$ digits as a result. If the most significant digit (MSD) of level 1 output has a value of 1/−1, then level 2 adds/subtracts the modulus from the level 1 output correspondingly. The result of level 2 RSD addition has $n + 2$ digits; however, only the $n + 1$th digit may have a value of 1/−1.

Algorithm for modular addition

Input : $A = a_{n-1}\ldots a_0$ *and* $B = b_{n-1}..b_0$ *and* $M = m_{n-1}\ldots m_0$ *and Add Sub 1-bit*

Output : $S = s_{n-1}\ldots..s_0$

if Add sub=0 then

T1=A+B;

else

T1=A-B;

end if

$$T2 = \begin{cases} T1 & T1[n] = 0 \\ T1 - M & T1[n] = 1 \\ T1 + M & T1[n] = -1 \end{cases}$$

$$T3 = \begin{cases} T2 & T2[n] = 0 \\ T2 - M & T2[n] = 1 \\ T2 + M & T2[n] = -1 \end{cases}$$

Return S←T3

The modular subtraction can be dine by using the same algorithm by just inverting the operand to be subtracted.

2.Modular multiplication.

Karatsuba and Ofman proposed a methodology to perform a multiplication with complexity by dividing the operands of the multiplication into smaller and equal segments. Having two operands of length *n* to be multiplied, the Karatsuba–Ofman methodology suggests to split the two operands into high-*(H)* and low-*(L)* segments as follows .

$$a_H = (a_{[n-1]}, \ldots a_{[n/2]}) \quad a_L = (a_{[n/2-1]}, \ldots a_0)$$

$$b_H = (b_{[n-1]}, \ldots, b_{[n/2]}), \quad b_L = (b_{[n/2-1]}, \ldots, b_0)$$

where $a = a_L + a_H\beta^{n/2}$ *and* $b = b_L + b_H\beta^{n/2}$

$$C = AB = (a_L + a_H\beta^{n/2})(b_L + b_H\beta^{n/2})$$

$$= a_Lb_L + ((a_L + a_H)(b_L + b_H) - a_Hb_H - a_Lb_L)\beta^{n/2} + a_Hb_H\beta^n$$

Consider β as the base for the operands, where β is 2 in case of integers and β is x in case of polynomials.

Karatsuba recursive multiplication

Operands of size *n*-RSD digits are divided into two (low and high) equal sized *n*/2-RSD digits branches. The low branches are multiplied through an *n*/2 Karatsuba multiplier and the high branches are multiplied through another *n*/2 Karatsuba multiplier. Implementation difficulties arise with the middle Karatsuba multiplier when multiplying the results of addition of the low and high branches of each operand by itself. The results of the addition are of size *n*/2+1RSD digits so that an unbalanced Karatsuba multiplier of size $n/2 + 1$ is required. Hence, the carry generated by the middle addition operation needs to be addressed to avoid implementation complexities of the unbalanced Karatsuba multiplier. The *n*/2-digit Karatsuba block is used to multiply the middle summations, excluding the carry. A 1-digit RSD multiplier is used to multiply the carry digits. The cross multiplication is simply performed by checking the carry in the other middle summation.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

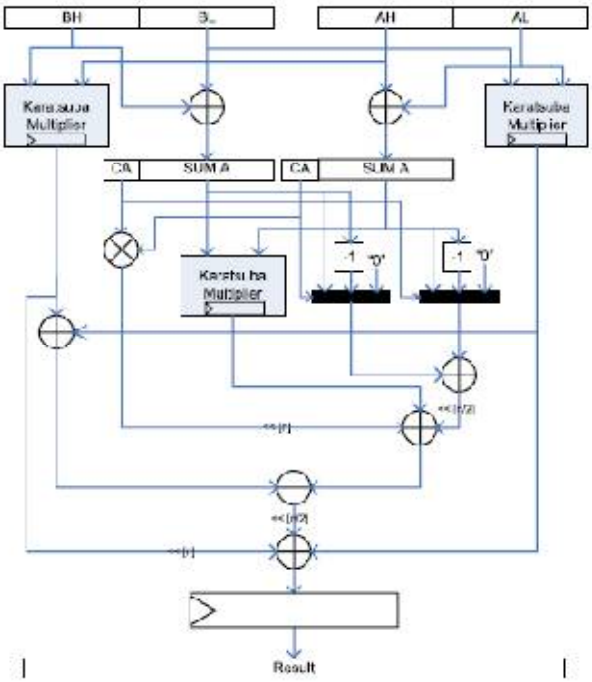

Fig 3. Block diagram of recursive multiplication

III. SIMULATION RESULTS

Her in the simulation results waveforms of RSD based and CSD based arithmetic operations is shown. When compared to RSD based operations CSD based operations have less non zero digits and it is unique .Also it has comparatively less delay when compared to RSD based operations

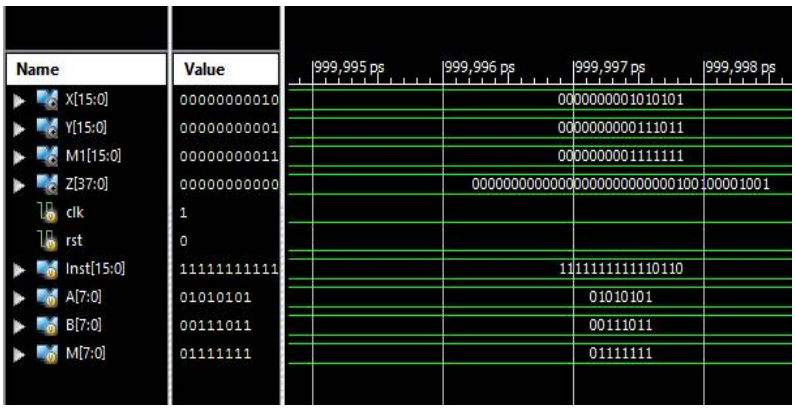

Fig 4.Output of rsd addition

Fig4 shows the output waveforms of RSD based modular addition. The inputs given are X and Y in RSD format as 85 and 59 and modulus given is 127 and output got is Z as17.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

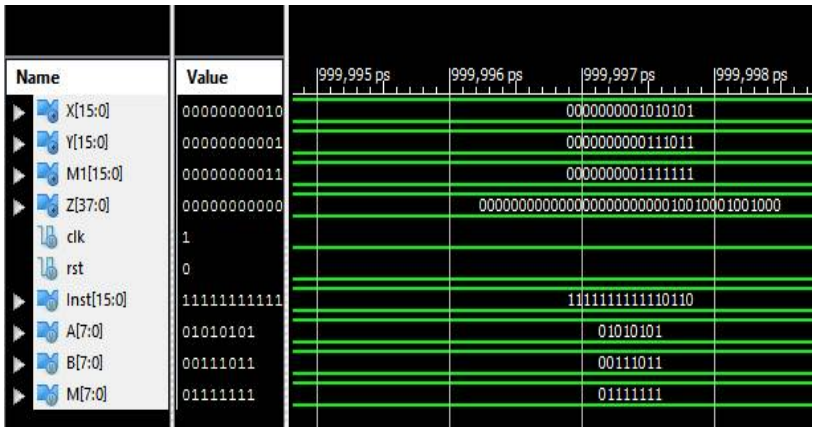

Fig 5. Output of rsd subtraction

Fig 5 shows output waveforms of RSD based modular subtraction .The inputs given are X and Y are 85 and 59 and modulus as 127 and the output got is z as 26.

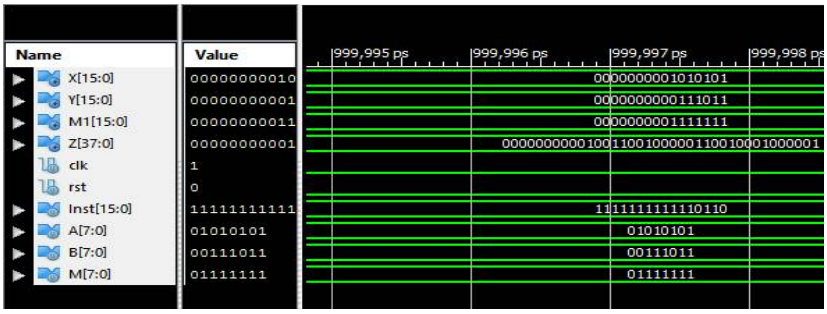

Fig.6 Output of RSD based multiplication

Fig 6 shows output waveforms of RSD based Karatsuba multiplication. In this the given inputs are X, Y in RSD format and the input is of 16 bit since its is redundant and the output got is 5015.

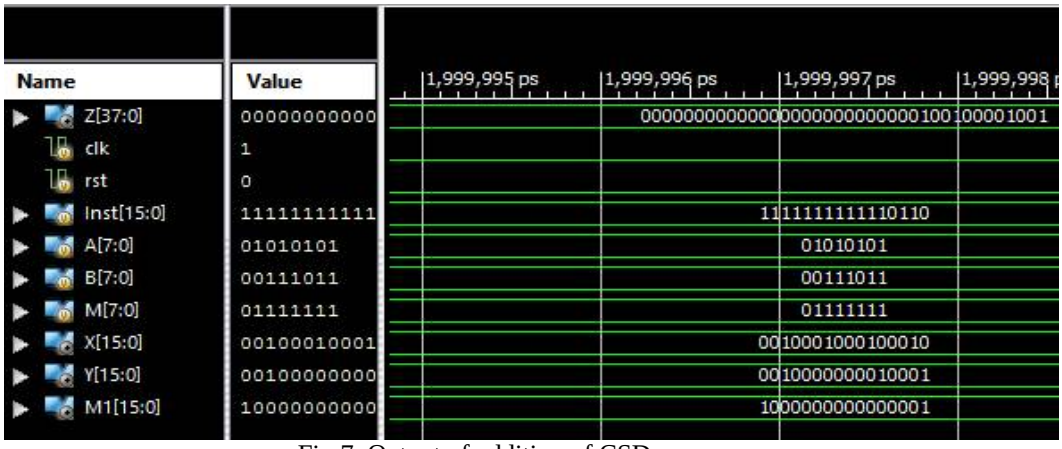

Fig 7 .Output of addition of CSD processor

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Fig7 shows output waveforms of CSD based modular addition. In this the inputs given are X ,Y, M in RSD form as 85,59, and 127 and the output obtained is z as 17.

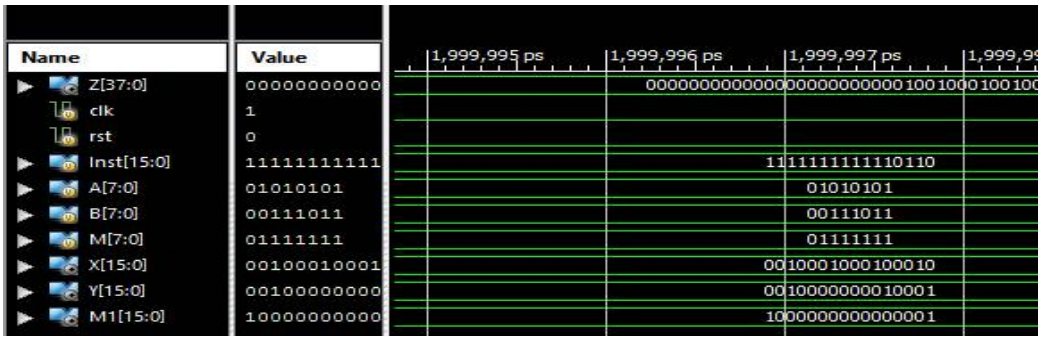

Fig.8 Output of csd based subtraction

Fig 8 shows output waveforms of CSD based modular subtraction. In this the inputs given are X, Y and M1 as 85,59 and 127 in CSD digits format and the output got is z as 26.

Fig 9 Output of CSD based multiplication

Fig 9 shows output waveforms of CSD based Karatsuba multiplication. The inputs given are X Y, as 85 and 59 in CSD format and the output given is 5015.

IV. CONCLUSION AND FUTURE WORK

This paper presented the comparison between a CSD and RSD based arithmetic operations in an ECC processor .The main characteristics of an RSD representation is that it is not unique and it has maximal number of non zero digits. If we use CSD based representation instead of RSD based representation we can reduce the delay and also in CSD based representations the number of nonzero digits is minimum.

REFERENCES

1. Hamad Marzouqi, Mahmoud Al-Qutayri, Khaled Salah, and Dimitrios Schinianakis, "A High-Speed FPGA Implementation of an RSD-Based ECC Processor," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., January 2015.
2. N. Koblitz, "Elliptic curve cryptosystems," Math. Comput., vol. 48, no. 177, pp. 203–209, Jan. 1987.
3. W. Stallings, Cryptography and Network Security: Principles and Practice, 5th ed. Englewood Cliffs, NJ, USA: Prentice-Hall, Jan. 2010.
4. D. Hankerson, A. Menezes, and S. Vanstone, Guide to Elliptic Curve Cryptography, 1st ed. New York, NY, USA: Springer-Verlag, Jan. 2004.
5. Sun and L. Chen, "Design of scalable hardware architecture for dualfield Montgomery modular inverse computation," in Proc. Pacific-Asia Conf. Circuits, Commun., Syst. (PACCS), May 2009, pp. 409–412.
6. S. Yazaki and K. Abe, "VLSI design of Karatsuba integer multipliers and its evaluation," Electron. Commun. Jpn., vol. 92, no
9. J.-Y. Lai and C.-T. Huang, "Energy-adaptive dual-field processor for high-performance elliptic curve cryptographic applications," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 19, no. 8, pp. 1512–1517, Aug. 2011.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

10.S.-C. Chung, J.-W. Lee, H.-C. Chang, and C.-Y. Lee, "A highperformance elliptic curve cryptographic processor over GF(p) with SPA resistance," in Proc. IEEE Int. Symp. Circuits Syst. (ISCAS), May 2012, pp. 1456–1459.
11. J.-Y. Lai and C.-T. Huang, "Elixir: High-throughput cost-effective dualfield processors and the design framework for elliptic curve cryptography," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 16, no. 11, pp. 1567–1580, Nov. 2008.

BIOGRAPHY

Gayathri Devi R is a PG scholar in Electronics and Communication Department, TKM Institute of Technology, Kollam, Kerala, India. She received Bachelor of Technology (B Tech) degree in 2015 from Sree Buddha college of engineering for Women , Pathanamthitta, Kerala, India.