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 6, June 2017

Elliptical Curve Cryptography Using RSD

Ashish S.Yadav

Student (VLSI and Embedded Systems), Department of E&TC, Sinhgad College of Engg. Pune, Maharashtra, India

ABSTRACT: cryptography is a scientific art of providing encryption and decryption. In this paper a novel way of cryptography to generate secret key using RSD is presented. In this, a problem of security is formulated using elliptical curve method. First, a algorithms based on Karatsuba-Ofman and RSD methods helps us to generate the 8 bit key or introducing encryption. Finally, a simulation results has shown the accuracy of karatsuba algorithm and has the reduced the complexity from n^2 to $n^{1.58}$. Further the performanceis enhanced by using RSD algorithm for addition and subtraction.

I.INTRODUCTION

Cryptography is the science of transforming messages. It makes them secure depending on the algorithm used for encryption and decryption. For example, for 80 bit information RSA algorithm gives 1024 bit key size. In this data, containing information is converted into encrypted data. The encrypted data consists of cipher text and data containing information.. Hence Cryptography provides a fair unit of confidentiality, authentication, integrity, access control and availability of data is maintained. Cryptography is portioned into two types Symmetric and asymmetric cryptography. Symmetric cryptography is also known as secret Key cryptography. Here same key is being used for encryption and decryption process, whereas same algorithm encrypts and decrypts the data, i.e. the keys are shared between the sender and receiver. The key must be kept secret. Asymmetric Cryptography is known as Public Key Cryptography. Here different keys are being used by sender and receiver for encryption and decryption process.

Elliptical curve cryptography is public key cryptography. It requires smaller key size as compared to non-ECC cryptography to provide equivalent security. For example, RSA requires 1024 bit key size whereas ECC needs only 160 bit key size for 80 bit information. For example, it provides equivalent security to RSA framework with smaller key sizes. Elliptical curve cryptography consists of two major operations Point Addition and Point Doubling, these two major operations are called as scalar point calculations. Points are doubled and being added through the series of operations like additions, subtractions and multiplications performed on the respective co-ordinates using geometrical properties.

A Redundant Signed Digit (RSD) is a numeral system. It uses more bits than required to represent a single binary digit. Hence most numbers will have several representations. For example radiax-2 RSD number is represented by {-1, 0, 1). RSD properties are different from the regular binary representation systems. Here RSD allows addition without using a typical carry. RSD makes bitwise logical operation slower, as it contains positive as well as negative values. Carry free addition is an attractive property of RSD as it do not generate carry while addition.

For reducing the multiplication complexity used by us during school days is given by $O(n^2)$. The methodology proposed by Karatsuba and Ofman gives the complexity $O(n^{1.58})$ for performing multiplication. Here the numbers to be multiplied are divided into smaller and equal segments. Recursive karatsuba produces three half-word instead of four half-word multiplications, with some addition and subtractions. In this for finding the points on the elliptic curve multiplication process is required which is given by karatsuba and ofman algorithm. The RSD numerical system used to represent the key in different polarities.

II. LITERATURE SURVEY

An elliptical curve cryptography designed by Neal Koblitz and Victor Miller achieves better security and enhancement in the parameters like key findings and data encryption [1][2].The author has the elliptical curve defined by weierstrass equation helps to find the points of the curve by performing the operations like point addition and point doubling.

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 6, June 2017

This chapter gives information about the recent work going on the elliptical curve cryptography:
The author has proposed a P256 NIST (National Institute of Standards and Technology) curve processor with efficient modular addition, subtraction, multiplication and division operations. The author has also introduced an adder with carry free addition. The proposed adder works with 3 layers. The layer 1 gives result as (n+1). The layer 2 gives result as (n+2) and the layer 3 finalizes the output as (n+1) in order to eliminate carry. Author has proposed his work on Xilinx Virtex 5(XC5VLX110T) FPGA. The maximum frequency obtained is 160MHz and to find the coordinates 2.26ms time is required. [5]
The author has described a method to reduce the multiplication steps. Author performed multiplication of multi-digit numbers by reducing the computational complexity to a great extent. The author splits the two operands into low (L) and high (H) segments. It reduces the complexity from $O(n^2)$ to$O(n^{1.58})$. [3].
The author has explained not only theoretically but also simulation based result to estimate the modular division. Author has also given the architecture for the modular division. Here the author sets two flags ρ and δ which first check for the odd or even for the dividend. The simulation gives results as -1 or +1. [10]
The author had come up with hardware as well as as software for the modular multiplication. On the other hand the for hardware implementation he came up with a hardware algorithm for modular multiplication. [9]
The author has described VLSI design for the multipliers where we can use karatsuba algorithm and simulation based results are shown to estimate the multiplication result. [8]
The author has proposed a processor for the elliptical curve cryptography with a radiax-4 unified division unit. On the other hand the processor proposed is hardware and simulation based, he has proposed 160-bit and 256-bit DECP with $0.29mm^2$ and $0.45mm^2$ for the silicon area in 90nm.[6].
The author has proposed a co-processor for increasing the computational speed of the elliptical curve scalar multiplications. The scalar multiplication here is introduced with point addition and point doubling operations. The author has showed the latency under $20\mu s$ for a 2^{80} bit security.
The author has explained theoretically the concepts of cryptography and about the advantages and limitations of the cryptography techniques. [4]

III. BACKGROUND

A. Elliptical Curve Cryptography
Elliptical curve cryptography is public key cryptography. It requires smaller key size as compared to Non-ECC cryptography to provide equivalent security. For example, it provides equivalent security to RSA framework with smaller key sizes. Elliptical curves are defined over a field K by the reduced Weierstrass equation given in equation (1)[1]. The further points of the curve are obtained by the point addition and point doubling operation in which point addition is the basic operation.

$$E: y^2 = x^3 + ax + b \quad (1)$$

The smoothness of the curve and the distinct roots are defined by $4a^3 + 27b^2 \neq 0$. The curve obtained by th e equation by performing the modulo a prime number. Such elliptical curves are called as prime field elliptical curves. The coordinates of the point addition and point doubling is calculated as follows, assuming P=(x_1, y_1), Q=(x_2, y_2) and R=$(P + Q)$=(x_3, y_3):
The conditions defined below to perform point addition and point doubling in equation (2) [3]:

$$\text{Point addition }: S = \frac{y2-y1}{x2-x1} mod\ p \qquad if\ p \neq q$$
$$\text{Point doubling: } S = \frac{3x^2+a}{2y}\ mod\ p \qquad if\ p = q \quad (2)$$

Here according to above condition point addition and point doubling operation is performed, then for point addition the coordinates for R(x_3, y_3) is obtained as in equation (2) [3]:

$$x_3 = (\left(\frac{y_2-y_1}{x_2-x_1}\right) \text{^}2) - x_1 - x_2$$
$$y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1 \quad (3)$$

Whereas the point doubling operation is obtained as follows in equation (2) [3]:

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 6, June 2017

$$x_3 = \left(\frac{3x_1^2+a}{2y_1}\right) - 2x_1$$

$$x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3) - y_1 \quad (4)$$

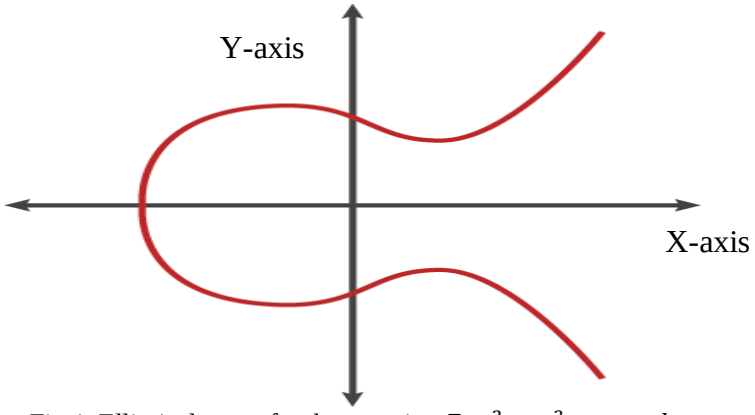


Fig.1. Elliptical curve for the equation $E: y^2 = x^3 + ax + b$

The two operations point addition and point doubling is also called as point scalar multiplication. Here point scalar multiplication is the operation of multiplying a point P on the elliptic curve by an integer scalar k.

B. Redundant Signed Digit

A Redundant Signed Digit (RSD) is a numeral system. It uses more bits than required to represent a single binary digit. Hence most numbers will have several representations. In effect it is called as redundant. RSD properties are different from the regular binary representation systems. Here RSD allows addition without using a typical carry.

When compared to non-redundant representations, RSD makes bitwise logical operation slower, but arithmetic operations are faster when a greater bit width is used. Carry free addition is an attractive property of RSD.

A non-redundant radiax-r number has digits from the set {0, 1,……, r-1}, where r is any number. Here the numbers can be represented in a unique way. Whereas, radiax-r RSD number is based on the digit set 'S'in equation (5) [11].

$S = \{-\beta, -(\beta - 1), \ldots\ldots, -1,0,1, \ldots \alpha\}$ (5)

Where $1 \leq \beta, \alpha \leq r - 1$. A symmetric signed digit has $\alpha = \beta$.

A symmetric signed digit representation uses the digit set given below. Where r is the radiax and α is the largest digit in the set given in equation (6)[11].

$D_{<r,\alpha>} = \{-\alpha, \ldots\ldots - 1,0,1, \ldots . \alpha\}$ (6)

A number in this representation is written as in equation (7) [11]:

$X_{<r-\alpha>} = X_{W-1}.X_{W-2}.X_{W-3}.X_{W-4} \ldots\ldots X_0 = \sum X_{W-1-i}\, r^i$ (7)

C. Karatsuba-Ofaman Multiplication

Multiplication is the basic step required in several advanced field like cryptography, where several multiplication steps are required for every process. When multiplying two N digit numbers we need $N * N = N^2$ multiplication steps [3]. Here first n-digit number is split into two (the first part of the number is multiplied with some base and with the second part). With the help of intermediate products and base number final product is obtained. The complexity of addition operations is usually less than the complexity of multiplication operations. Henceforth the usage of Karatsuba algorithm is increased in several advanced fields.

Having two operands of length n to be multiplied, the Karatsuba-Ofman methodology suggests to split the numbers into high (H) and low (L) as in equation (8) [3]:

$$a_H = (a_{n-1}, \ldots\ldots, a_{\frac{n}{2}}), \quad a_L = (a_{\left(\frac{n}{2}\right)-1}, \ldots\ldots, a_0) \quad (8)$$

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 6, June 2017

$$b_H = (b_{n-1}, \dots\dots, b_{\frac{n}{2}}), b_L = (b_{(\frac{n}{2})-1}, \dots\dots, b_0)$$

Consider β as the base for the operands, where β is 2 in case of integers and β is x in case of polynomials. Then, the multiplication of both operands is performed a follows: $a = a_L + a_H\beta^{\frac{n}{2}}$ and $b = b_L + b_H\beta^{\frac{n}{2}}$

Four half-sized duplications are required, where Karatsuba procedure reformulatein equation (9) [5] :

$$C = AB = \left(a_L + a_H\beta^{\frac{n}{2}}\right)\left(b_L + b_H\beta^{\frac{n}{2}}\right)$$
$$= a_L b_L + (a_L b_H + a_H b_L)\beta^{\frac{n}{2}} + a_H b_H(\beta\text{^}n). \quad (9)$$

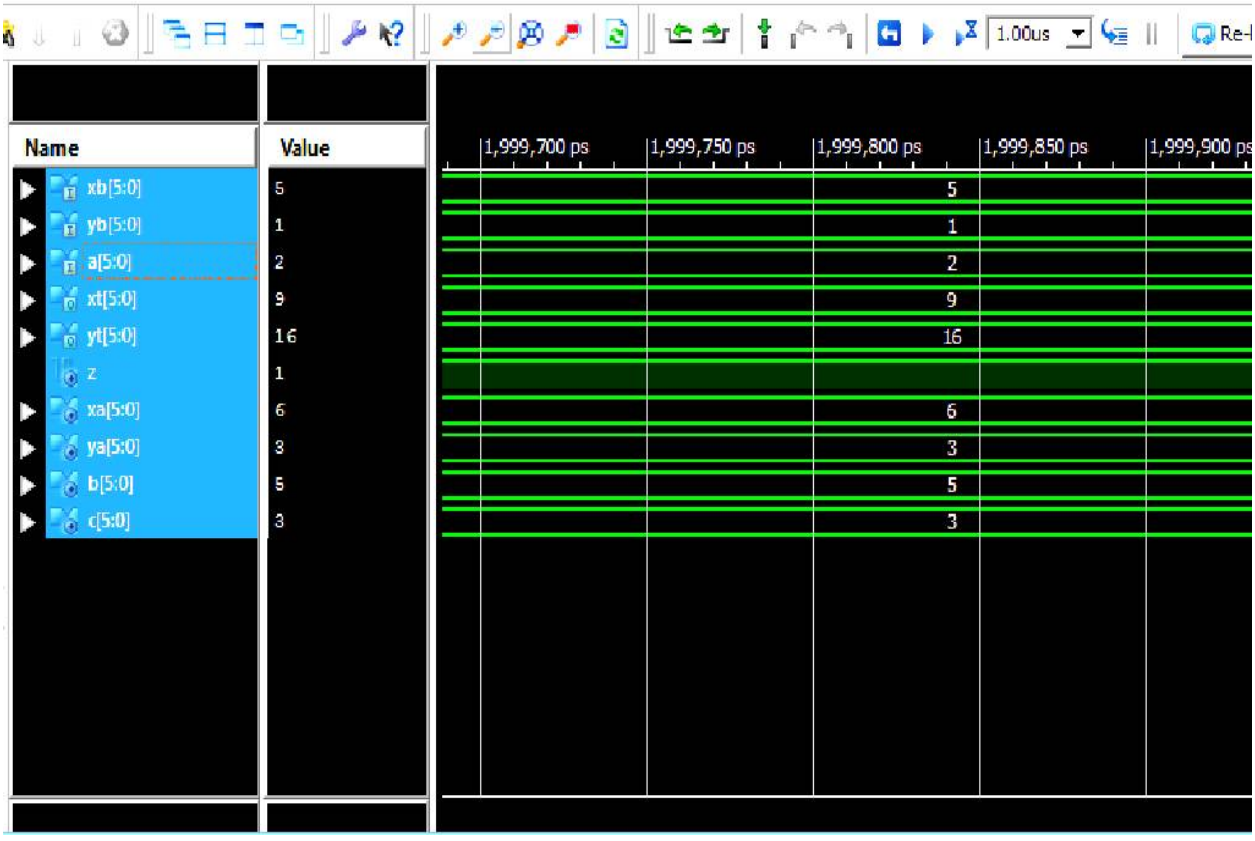
Therefore only three half-sized multiplication are needed. Karatsuba algorithm is performed recursively, where the operands are segmented into smaller parts until a reasonable size is reached and the regular multiplication with smaller segments is performed.

IV. SIMULATION OF ELLIPTICAL CURVE CRYPTOGRAPHY USING RSD

The elliptical curve cryptography by using RSD is used to generate the key which are nothing the points of the elliptic curve. This can be achieved by using the modular arithmetic operation. Here we are performing multiplication by using Karatsuba algorithm which reduces the multiplication steps and hence increases the speed of the multiplication. For key generation an equation of the curve is defined and the points are generated by the scalar operations and a LUT based structure for the curve is proposed which enhances the performance of the key generation.

V. RESULTS

1. Key Generation:



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 6, June 2017

Here xa andxb are the initial points of the elliptic curve. Here $a$reprents the points on the elliptic curve, basically a tells us the point number to be obtained. xt and $yt$are the next co-ordinates on the curve.

Initial points	Obtained points
xb = 5	xt = 9
yb = 1	yt = 16

VI. CONCLUSION

The work generates the key, as the elliptic curve is defined as LUT based. The multiplication used for the point doubling operation has time complexity $n^{1.58}$ which reduces the multiplication steps. The key is generated and the LUT slices are used and maximum operating frequency is 169MHz. RSD as a carry free representation is used which results in short datapaths and increase in frequency.

REFERENCES

[1] N. Koblitz, "Elliptic curve cryptosystems," Math. Comput., vol. 48, no. 177, pp. 203–209, Jan. 1987.
[2] W. Stallings, Cryptography and Network Security: Principles and Practice, 5th ed. Englewood Cliffs, NJ, USA: Prentice-Hall, Jan. 2010.
[3] A. Karatsuba and Y. Ofman, "Multiplication of multidigit numbers on automata," Soviet Phys. Doklady, vol. 7, p. 595, Jan. 1963.
[4] Ç. K. Koç, Ed., Cryptographic Engineering, 1st ed. New York, NY, USA: Springer-Verlag, Dec. 2008.
[5] HamadMarzouqi, Mahmoud Al-Qutayri "A High Speed FPGA Implementation of an RSD based ECC Processor", IEEE trans.2016
[6] Y.-L. Chen, J.-W. Lee, P.-C. Liu, H.-C. Chang, and C.-Y. Lee, "A dualfield elliptic curve cryptographic processor with a radix-4 unified division unit," in Proc. IEEE Int. Symp. Circuits Syst. (ISCAS), May 2011, pp. 713–716
[7] N. Guillermin, "A high speed coprocessor for elliptic curve scalar multiplications over Fp," in Proc. 12th Int. Workshop Cryptograph. Hardw. Embedded Syst. (CHES), vol. 6225. Jan. 2010, pp. 48–64
[8] S. Yazaki and K. Abe, "VLSI design of Karatsuba integer multipliers and its evaluation," Electron. Commun. Jpn., vol. 92, no. 4, pp. 9–20, 2009.
[9] G. Chen, G. Bai, and H. Chen, "A new systolic architecture for modular division," IEEE Trans. Comput., vol. 56, no. 2, pp. 282–286, Feb. 2007.
[10] N. Nedjah and L. de MacedoMourelle, "A reconfigurable recursive and efficient hardware for Karatsuba–Ofman's multiplication algorithm," in Proc. IEEE Conf. Control Appl. (CCA), vol. 2. Jun. 2003, pp. 1076–1081.