International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 07 | July-2016 www.irjet.net p-ISSN: 2395-0072

A VLSI implementation of RSD based high speed ECC processor using arithmetic operations

Sahana G D[1], Vishwanath B R[2]
[1] PG Student, Dept. of Electronics and Communication Engineering, Rajeev Institute of Technology Hassan, Karnataka
Email: sahanagdsana@gmail.com
[2] Asst. Professor, Dept. of Electronics and Communication Engineering, Rajeev Institute of Technology Hassan, Karnataka
Email: vishwa_br@yahoo.co.in

Abstract - *Elliptic Curve Cryptography is a standout amongst the most interested exploration themes in VLSI. System security is turning out to be increasingly significant as the volume of information being traded on the Internet increments. Point addition and doubling are key operations of ECC which choose the Performance of ECC. Here the design with the information way which can perform either prime field G(p) operations or binary field G(2m) operations for arbitrary prime numbers has been proposed. Utilizing this design we can accomplish the high throughput of the both fields that is prime and binary fields. The examination of speed and area overhead among various ECC plans legitimizes the cost-adequacy of the proposed ECC architecture with its design procedure. The Xilinx virtex 5 field programmable gate array has been utilized. The usefulness of the FPGA will be checked by utilizing chip scope pro analyzer. Further the processor is actualized in ASIC CMOS innovation.*

***Key Words*: Point addition, Point doubling, prime field Binary field.**

1. INTRODUCTION

Cryptography is about developing and breaking down conventions that anticipate outsiders or people in general from perusing private messages. Different angles in data security, for example, information privacy, information respectability, verification, and non-repudiation are key to current cryptography. There are two sorts of cryptosystems: symmetric and asymmetric. In symmetric frameworks the same key that is the mystery key is utilized to encode and decode a message. Because the key is shorter in length in symmetric systems, they are speed in data manipulation compared to asymmetric systems[4]. Open key is utilized to encrypt a message and private key is utilized to unscramble it by asymmetric systems. Protection to communication can be increased by using asymmetric systems. In early stages different methods like enigma encryption machine, one-time pad, pseudo random generator, diffie-helman key exchange, and steganography were used in cryptography. The most recent method in cryptography is elliptic curve cryptography.

While performing multiplication, addition is utilized in the accumulation procedure [1], and also in one type of algorithm known as binary modular divider algorithm which will be employed in an asymmetric Cryptographic system called as Elliptic curve cryptographic system. In order to stay away from lengthy data paths due to carry propagation, carry free arithmetic is utilized in prime field ECC processors [2]. A Redundant Signed Digit (RSDs) has been used in different outlines. It is important to fabricate fast effective expansion data path since it is a central operation utilized in other modular arithmetic operations. Measured duplication is a crucial operation in ECC. Cellular automata multiplier and Fermat algorithm for inversion has been to outline the arithmetic unit in the finite field GF (2^{163}) [5].

This paper proposes another RSD-based Modular Addition/Subtraction and Multiplier for ECC processor with fast working recurrence. The RSD representation is a carry free arithmetic in which numbers are spoken to by the distinction of two different numbers. The way of the RSD representation has the upside of performing expansion and subtraction without the need of the two's supplement representation. On the other side, because of redundancy in the representation of integers an overhead is introduced. The novelty of our processor evolves around the following.

- Literature survey to be carried out in the area of implementation of ECC processor using VLSI technology. Survey includes studies on different techniques and different algorithm.
- Studies to be carried out on different existing technique and also existing algorithms to achieve the objectives like addition without inversion in mixed co-ordinate, multiplication within shortest period of time, highest operating frequency, transferring capability to other FPGA and ASIC technologies.
- To perform point expansion and point multiplying over binary field using the algorithm that has been developed based on karastuba and Vedic multiplication.

- To perform point expansion and point multiplying over prime field using the algorithm that has been developed based on karastuba and Vedic multiplication.
- Then the verilog code will be written for algorithms of key operations of ECC processor and implemented in virtex 5 FPGA board.
- Then the ASIC implementation will be done by using same verilog code.

2. ELLIPTIC CURVES OVER DUAL FIELD

Elliptic curve serves as good trapdoor function that is an algorithm which is simple in one direction and hard in another direction. The curves are named as elliptic curves as they are illustrated by equations which are in cubic form, which are taken for calculating the circumference. Elliptic bends are simple capacities which can be drawn as smooth circling lines in (x,y) plane. By and large, cubic condition for elliptic bend can be given by utilizing summed up Weierstrass equation as given in 2.1.

$$y^2 + m_1xy + m_3y = m_2x^2 + m_4x + m_6 \quad (1)$$

Where $m_1, m_2, m_3, m_4, m_5, m_6 \in F_p$ and p is a prime integer.

An elliptic bend with group of points (x,y) over the real numbers forms a abelian group if it satisfy the condition as shown in equation 2.2

$$y^2 = x^3 + mx + n \quad (2)$$

Where m and n are real numbers, x and y use the values in the real numbers.

The two finite fields over which the elliptic curves are mainly defined are:

- Binary field *GF(2^n)*
- Prime field GF(P)

For prime field the elliptic curve equation is given by,

$$y^2 \bmod p = (x^3+cx+d) \bmod P \quad (3)$$

Where

$$4c^3 + 27d^2 \neq 0 \bmod p \quad (4)$$

Is a condition to form an abelian group. The adding procedure in an elliptic group over prime field is very similar to operations performed over the real numbers with elliptic curve. The only difference is that all the tasks are performed modulo p.

Elliptic curve equation over Binary field is given by

$$y^2+xy=x^3+ax^2+b \quad (5)$$

ECC over binary field achieves the high performance without considering the carry and modular reduction. These fields are ideal for the utilization in equipment as far as speed and area.

2.1 BINARY FIELD

The most imperative elliptic curve conditions are $Y^2 + XY = X^3 + cX^2 + d$ (Weierstras condition in GF (2^m)) for binary field. In binary field, addition is XOR operation and multiplication is polynomial based, and the result is reduced by using the irreducible polynomial. Squaring is achieved by shift operation. So multiplication is performed based on the hybrid Karastuba multiplier. Here primary focus is on ECC over binary field based on the short weierstrass equation.

2.1.1 Point Addition over Binary field

In this method, one point is in projective Co-ordinate and another point is an affine Co-ordinate. The output point that results will appear in projective Co-ordinate so that the operation like inversion will be avoided.

Algorithm 1:

Inputs: A(x_2, y_2), $Q(X_4,Y_4,Z_4)$.

Outputs: $R(X_3,Y_3,Z_3)$.

$A=Y_4+y_2*Z_4^2$;
$B=X_4+x_2*Z_4$;
$C=B*Z_4$;
$Z_3=C*C$;
$D=x_2*Z_3$;
$E=A+B*B+aC$;
$X_3=A*A+C*E$;
$I=D+X_3$;
$J=A*C+Z_3$;
$F=I*J$;
$K=Z_3*Z_3$;
$Y_3=F+x_2*K+y_2*K$

2.1.2 Point doubling over binary field:

Adding the point over the elliptic curve to itself is known as point doubling. In these equations 'a' & 'b' are considered as parameters of elliptic curve.

Algorithm 2:

Inputs:*(X1, Y1, Z1).*

Outputs:*(X4, Y4, Z4)*

$$Z_4=Z_1^2*X_1^2,$$
$$X_4=X_1^4+bZ_1^4,$$
$$Y_4=(Y_1^2+aZ_4+bZ_1^4)*X_4+Z_4*bZ_1^4.$$

2.2 Prime Field

The most imperative elliptic curve conditions are y2=x3+cx+d (Weierstrass condition in GF (p)) for prime field. The fixed number of modular multiplications, squares, additions, shifts, and basic arithmetic operations are required while performing addition and doubling over each elliptic curve. The real number of these operations relies on upon the way the bend is spoken to; as a rule it is multiplications and squaring operations that rule the running time, and the running the reality of the situation will become obvious eventually precisely with the quantity of arithmetic operations required. Here primary focus will be on ECC over prime field based on the short weierstrass equation.

2.2.1. Point addition over Prime field:

The elliptic curve considered in $GF(p)$, has the general elliptic point (x,y) which is projected to (X_1,Y_1,Z_1), where $x=X/Z^2$, and $y=Y/Z^3$ and the second point considered is affine point that is (x_2,y_2). So that the point addition will be shown as below:

Algorithm 3:

Input: $Q=(X_4,Y_4,Z_4)$, $A=(x_2,y_2)$
Output: $R=(X_3,Y_3,Z_3)=P+Q$;
$A=X_4$;
$B=x_2*Z_1^2$;
$C=A-B$;
$D=Y_1$;
$E=y_2*Z_1^3$;
$F=D-E$;
$G=A+B$;
$H=D+E$;
$Z_3=Z_1*C$;
$X_3=F^2-G*C^2$;
$I=G*C^2-2*X_3$;
$Y_3=(I*F-H*C^2)/2$;

2.2.1 Point doubling over Prime field:

Over $GF(P)$, the point doubling will be indicated as:

Algorithm 4:

Input: $P=(X_1,Y_1,Z_1)$,a
Output: $Q=(X_4,Y_4,Z_4)=2P$;
$A=3*X_1^2+a*Z_1^4$;
$B=4*X_1*Y_1^2$;
$X_4=A^2-2*B$;
$Z_4=2*Y_1*Z_1$;
$C=8*Y_1^4$;
$Y_4=A*(B-X_4)-C$;

3. DUAL FIELD ARCHITECTURE

The discussion about the architecture of the ECC processor is done in this section. The ECC processor discussed here contains all the basic EC arithmetic, point double, point addition, and point scalar multiplication over both G (2^m) and G (P) along with arbitrary elliptic bends stated in IEEE 1363 standard.

Figure 1 visualizes the entire ECC Dual field architecture having input/output buffers, control unit, Data selector, Register file and ECC scalar multiplication. Via the I/O interface Data are sent into the Input Buffer and read out from the Output Buffer. Before the computation itself the ECC parameters are going to be written into the buffers. All operations will controlled by control unit. Control register will stores the control instruction and main controller will decode it.

Architecture of ECC Arithmetic units as shown in figure 1.It consists of Control unit, Input/output Buffers, Multiplier block, addition block and Register block. Where multiplier block consists of the Karastuba and normal multiplier which is used to perform point addition and doubling for both fields. Finally the register files will contain the results.

The point and scalar multiplication are needed by the elliptic curve cryptographic scheme which is defined as follows:

$$F=kE=E+E+\ldots+E \text{ (k times)} \quad (7)$$

Where E represents a point over the elliptic curve and the random integer is k. The operations which play a key role in scalar multiplication are point addition and point doubling.

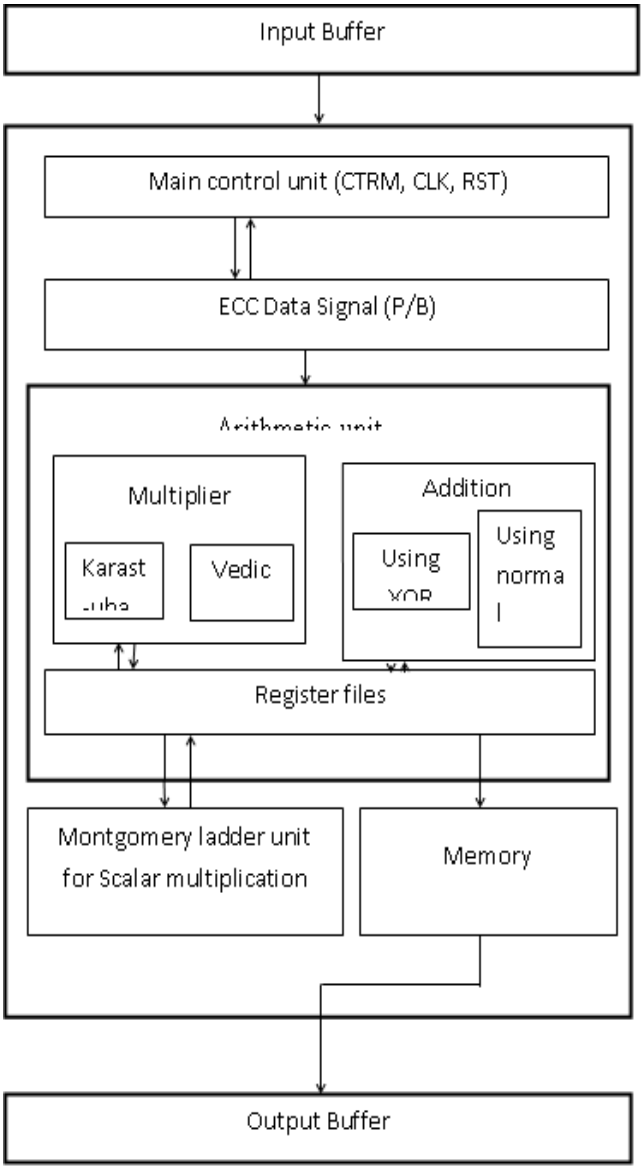

Fig 1: ECC Dual field Processor Architecture

4. RESULTS AND DISCUSSIONS

We have presented the Dual field ECC architecture, which is scalable for field size, which is 8 bit size for Binary field and for Prime field. The proposed Dual field architecture facilitates the design exploration of a large variety of applications with heterogeneous throughput/area requirements. So our Dual field ECC processor and its design methodology are very cost-effective and flexible.

Xilinx ISE 14.7 Tool has been used, for the design and testing of point addition, point doubling and Scalar multiplication for ECC. Multiplications and squaring is done using Vedic Mathematics, Additions & subtractions done in an normal method. Coding is done using Verilog-HDL. Simulations and synthesis results are tested and verified on Virtex xc5vlx110t-1ff1136 as target device.

4.1 SIMULATION RESULTS IN FPGA

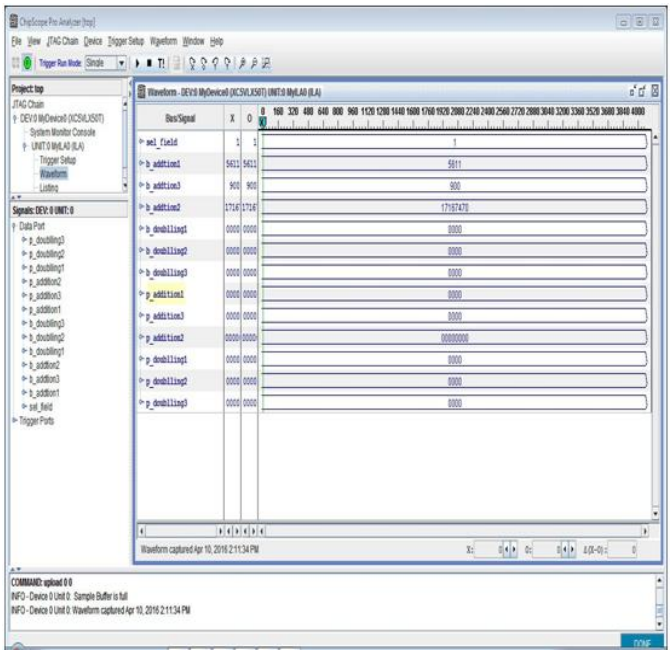

Fig 2: 8 bit point addition (mixed co-ordinates) over binary field

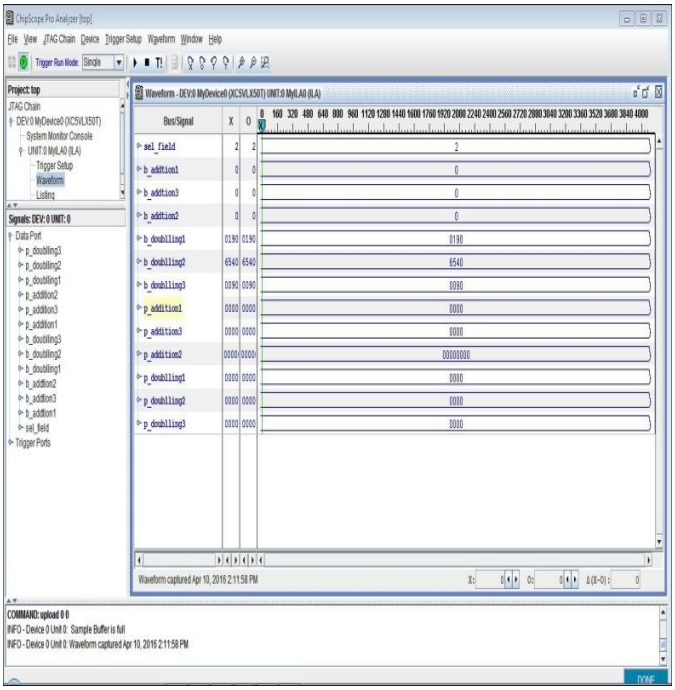

Fig 3: 8 bit point doubling (pure- projective) over binary field

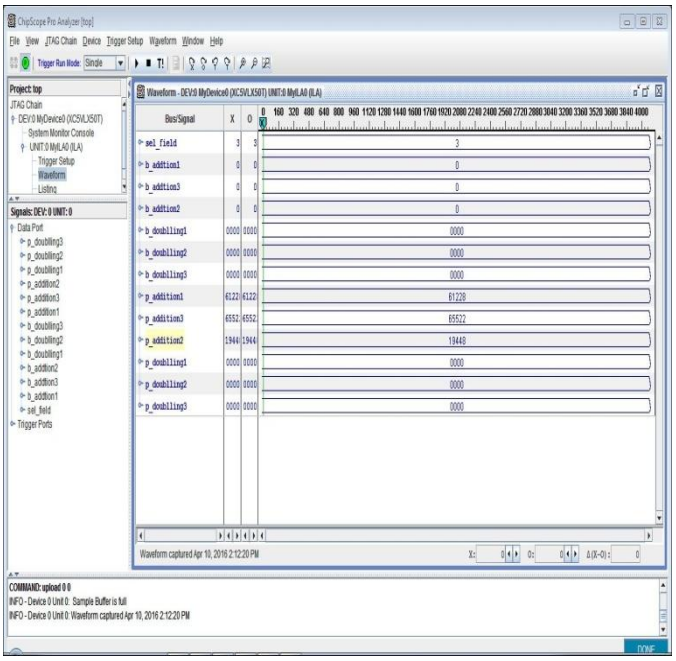

Fig 4: 8 bit point addition (mixed co-ordinates) over prime field

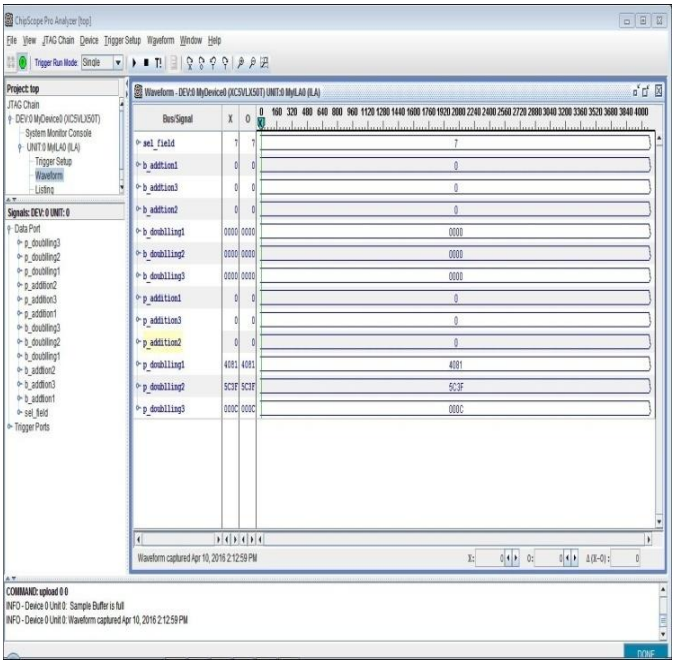

Fig 5: 8 bit point doubling (pure- projective) over prime field

4.2 RESULTS OF SYNTHESIS

The results of synthesis of point addition, point doubling over binary GF (2^m) and primary field GF (p) using mixed co-ordinates is shown in table 1.

8 bits	No. of slice LUT's	Delay(ns)
Point addition over binary field	520	39.039
Point doubling over binary field	485	22.745
Point addition over prime field	417	44.514
Point doubling over prime field	299	22.373

4.3 SYNTHESIS RESULTS IN ASIC

Cadence incisive tool can be used to synthesize the program as per the design specifications.

Table 2: Synthesis report in ASIC

Parameters	Before	After
Area	159981.16	50730.52
Gates	26886	7693
Power	9021576.17	5227563.44

In the synthesis result of ASIC, comparison of the area, gates and power, before synthesis and after synthesis will be done.

Table 1: Synthesis results in FPGA

4.2 ENCOUNTER RESULT UPTO GDSII LAYOUT

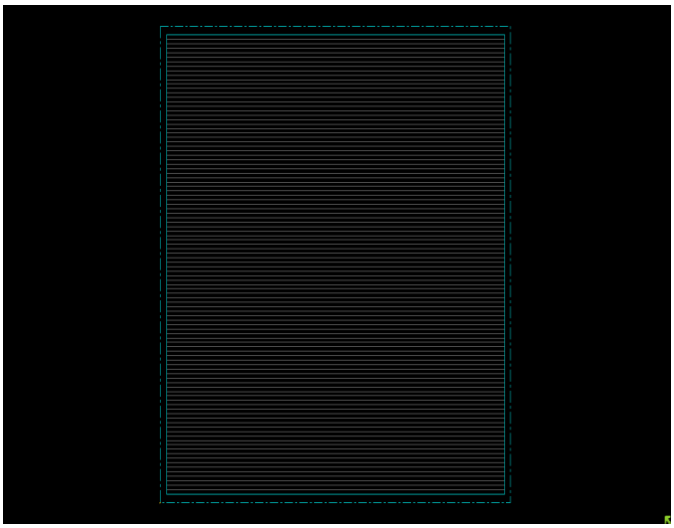

Fig 6: Floor planning of dual field ECC architecture

Floor planning is the first step in the encounter operation. And in the floor planning it will generates the basement for placing components. Figure 6 shows the floor planning of the dual field ECC architecture.

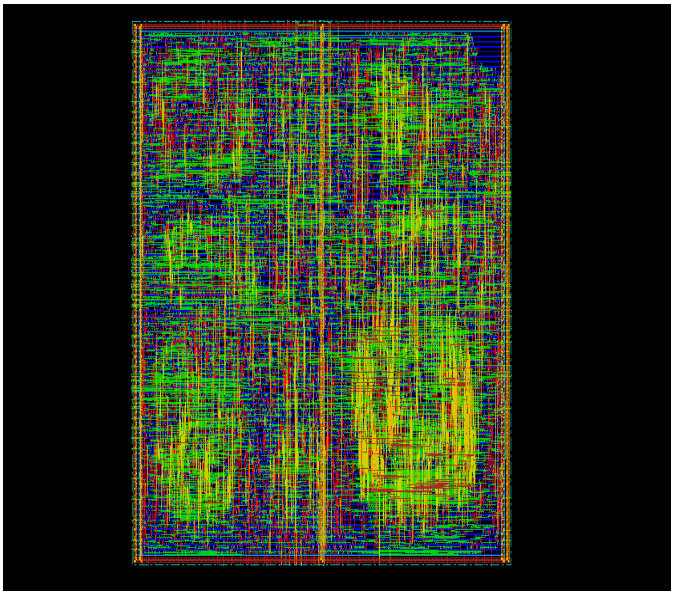

FIG 7: Placement of dual field ECC architecture

Second step is placement, in placement it decides and places all the components in the appropriate places.

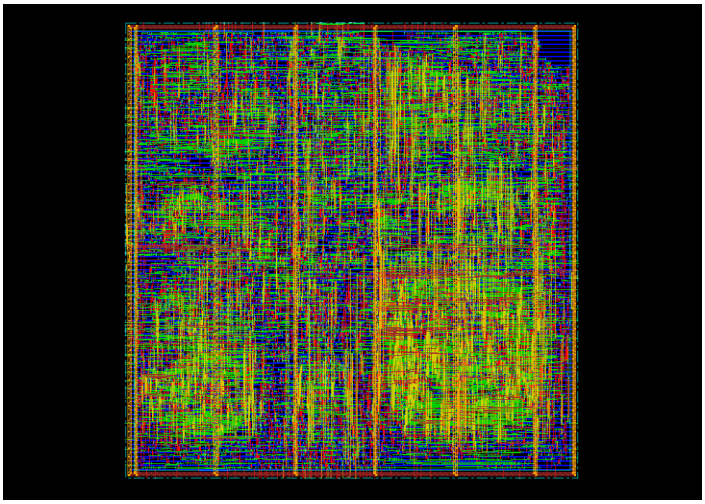

FIG 8: Routing of dual field ECC architecture

Third step is routing, the encounter operation of the dual field ECC architecture, in this it will provide all the interconnection between all the components and it optimizes the area and interconnection as shown in figure 8.

The report of power analysis is produced by the Xilinx power analyzer programming. The aggregate power usage is evaluated to be 0.448W if there should be an occurrence of virtex5 FPGA board as appeared in figure 9.

On-Chip	Power (W)	Used	Available	Utilization (%)
Clocks	0.000	4	--	--
Logic	0.000	1751	28800	6
Signals	0.000	2642	--	--
DSPs	0.000	14	48	29
IOs	0.000	283	480	59
Leakage	0.448			
Total	0.448			

Supply Summary		Total	Dynamic	Quiescent
Source	Voltage	Current (A)	Current (A)	Current (A)
Vccint	1.000	0.288	0.000	0.288
Vccaux	2.500	0.062	0.000	0.062
Vcco25	2.500	0.002	0.000	0.002

	Total	Dynamic	Quiescent
Supply Power (W)	0.448	0.000	0.448

Fig 9: Power analysis report in virtex5 FPGA

TABLE 3: Comparison of dual field architecture in FPGA and ASIC

Power summary	FPGA	ASIC
Total estimated power consumption	44.8 mW	5.22 mW

5. CONCLUSION

We have exhibited the Dual field ECC design, which is versatile for field size of 8 bits in binary and prime field. Our processor can be adjusted both prime field and binary field, and gives a high throughput and range. The test result demonstrates that the EC point scalar duplication of both field GF (P) and GF (2^m) should be possible with Xilinx stage.

The result of experiment demonstrates that our outline creates high throughput and power effectiveness of 44.8 mW in FPGA and 5.22 mW in ASIC. The proposed Dual field engineering encourages the design exploration of a substantial assortment of utilizations with heterogeneous throughput/area prerequisites. So Dual field mixed co-ordinate ECC processor and its configuration system are exceptionally financially savvy and adaptable.

Karastuba multiplication and Vedic multiplication and adders are used in the calculations while performing point addition and multiplying. Xilinx ISE 14.7 Tool has been utilized, for the configuration and testing of point addition, point multiplying for ECC. Multiplications and squaring is done utilizing Vedic Mathematics, Additions and subtractions done in an ordinary strategy. Coding is done utilizing Verilog-HDL.

- FUTURE WORK

  Power utilized can be further reduced. Number of multiplications and squaring operations in the algorithm to perform point addition and point doubling can be further reduced. A suitable algorithm for the transformation of the last result back to affine co-ordinates must be actualized.

REFERENCES

[1] Hamad Marzouqi, Mahmoud Al-Qutayri, Khaled Salah, Dimitrios Schinianakis, Thanos Stouraitis, "A NIST 256 prime field RSD based ECC processor implementation in FPGA", IEEE transactions on very large scale integration systems,2015.

[2] Ciaran J. McIvor, Maire McLoone and John V. McCanny, "Hardware Elliptic Curve Cryptographic Processor Over GF(p)", IEEE transactions on circuits and systems-I: regular papers, vol. 53, no. 9, september 2006.

[3] Sandeep S, Hameem shanavas I, V.Nallusamy, Brindha M, "Design of Hardware Implementation of Elliptic Curve Cryptography Over Binary Field", International journal vol. 2, no.2 , pp.(78-82), 2012.

[4] Z. Guitouni1,R.Chotin-Avot, M. Machhout, H. Mehrez and R. Tourki, "High Performances ASIC based Elliptic Curve Cryptographic Processor over GF(2m)," IJCA Special Issue on "Network Security and Cryptography" NSC, 2011.

[5] Mohsen Machhout, Zied Guitouni1, Kholdoun Torki , Lazhar Khriji and Rached Tourki "coupled FPGA/ASIC implementation of elliptic curve crypto-processor", International Journal of Network Security & Its Applications (IJNSA), Volume 2, Number 2, April 2010.

[6] C. Rebeiro, S. S. Roy, and D. Mukhopadhyay, "Pushing the limits of high-speed GF(2m) elliptic curve scalar multiplication on FPGAs," in Proc. Cryptograph. Hardw. Embedded Syst. (CHES), vol. 7428. Jan. 2012, pp. 494 511.

[7] T. Güneysu and C. Paar, "Ultra high performance ECC over NIST primes on commercial FPGAs," in Proc. 10th Int. Workshop Cryptograph. Hardw. Embedded Syst. (CHES), 2008, pp. 62–78.

BIOGRAPHY

Sahana G D, pursuing M.Tech in VLSI Design and Embedded Systems at Rajeev Institute of Technology, Hassan. Completed B.E. in Electronics and Communication Engineering from Govt. Engineering College, Hassan.

Vishwanath B R, pursuing Ph.d at P.E.S college of engineering, Mandya. Completed M.Tech in VLSI design and Embedded systems in P.E.S college of engineering, Mandya. Completed B.E in ghousia college of engineering, Ramanagara.