IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 8, August 2015.
www.ijiset.com
ISSN 2348 – 7968

Low Power Elliptic Curve Scalar Multiplication Using Hybrid Karatsuba Multipiler with Less Area Utilization

Jayalakshmi K R
M-Tech student,
ECE Department,
Mangalam College of Engineering,
Kottayam, India

Ms. Hima Sara Jacob
Assistant Professor,
ECE Department,
Mangalam college of engineering,
Kottayam,India

***Abstract*—**Art of keeping messages secure is cryptography.Elliptic curve cryptography (ECC) has become popular due to its superior strength- per-bit compared to existing public key algorithms. Multiplication is frequently used operation which is currently implemented in many processors.Elliptic curve scalar multiplication (kP), where k is a scalar (integer) and P is a point on the curve, is the most important operation in elliptic curve cryptosystems.In this paper elliptic curve scalar multiplication is performed by using a hybrid karatsuba multiplier.Synthesis report shows that hybrid karatsuba multiplier has less utilization of area.simulation was done in Modelsim 6.4a.

Keywords:
Elliptic curve cryptography(ECC),Karatsuba multiplication,Point addition,Doubling,ECSMA

1.INTRODUCTION

In many digital system designs Multiplier unit is the main block. Multipliers are the basic and essential building blocks of many high performance systems. Multiplication is frequently used operation which is currently implemented in many processors. In today's market there is a huge demand for high speed multipliers, since these are the slowest elements in the systems. The speed of the multiplier decides the speed of the system, hence the speed of the multiplier has to be improved.

The performance of the system depends on the multiplier's speed which is optimized by the proposed multiplier.Cryptology is science concerned with providing secure communications. The goal of cryptology is to construct schemes which allow only authorized access to information. There are two types of cryptographic algorithms such as symmetric key and asymmetric key algorithms. Symmetric key cryptographic algorithms have a single key for both encryption and decryption.It can be used only when the two communicating parties have agreed on the secret key.In asymmetric key cryptographic algorithms two keys are involved-a private key and a public key. The private key is kept secret while the public key is known to everyone.

Elliptic Curve Cryptography (ECC), which is an asymmetric algorithm ,is gaining attraction as with their high level of security with low cost, small key size and smaller hardware realization.Elliptic curve scalar multiplication (kP), where k is a scalar (integer) and P is a point on the curve, is the most important operation in elliptic curve cryptosystems. Scalar multiplication consists of elliptic curve group operations such as point addition and point doubling. The elliptic curve group operations perform finite field operations like field addition, filed multiplication, field squaring, field division and modular reduction.

In this paper a hybrid karatsuba multiplier for the field multiplication is proposed.Both hybrid karatsuba multiplier and the recursive karatsuba multiplier was simulated and synthesized.

2. LITERATURE REVIEW

The use of Recursive karatsuba multiplier for field multiplication in ECC improves speed and reduces the power.Bt by using Hybrid karatsuba multiplier in ECC ,Further reduction in power and area is possible.So a low power ,less area elliptic curve scalar multiplier can be designed by using a hybrid karatsuba multiplier.

3. ECSMA

Elliptic curve scalar multiplication means, a point on the elliptic curve known as base point P is multiplied by a scalar k and output is the scalar product kP.An elliptic curve is the set of points that satisfy a specific mathematical equation.Equation for an elliptic curve looks something like this:$y^2 = x^3 + ax + b$.

ISSN 2348 – 7968

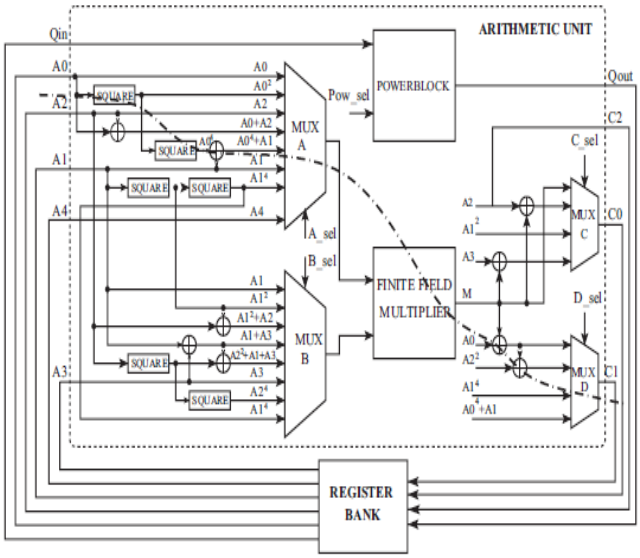

Fig. 1.ECSMA [1]

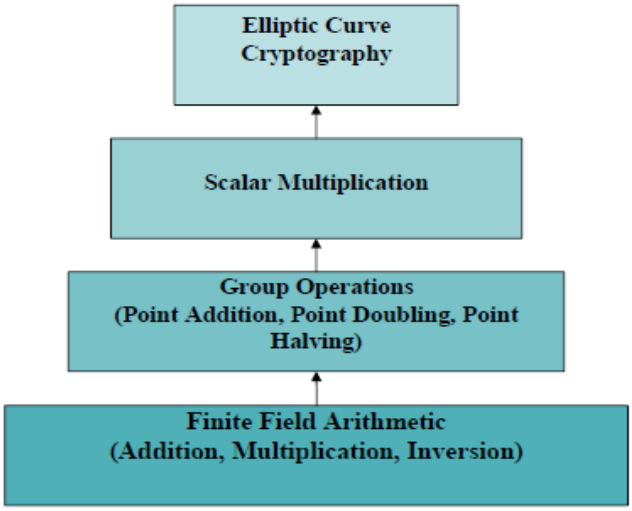

Fig. 2. ECSMA operations[3]

In ECSMA processor organization the main units are register bank and an arithemetic unit. The register bank has eight registers, each capable of holding one field element. Since, each slice contains an equal number of LUTs and flip-flops (FFs), use of slice FFs results in increased utilization of slices. Input multiplexers are used to select the input for each registers. Similarly, output multiplexers are used to select proper registers for each output. The main component of the arithmetic unit is the field multiplier. This has the largest area and also maximum delay compared to other field primitives. the sequence of operations during the scalar multiplication is designed to ensure maximum utilization of the multiplier. Squarers, adders, and multiplexers have very small area.Therefore several instances of these components are used in the arithmetic unit.

Elliptic curve scalar multiplication (kP), where k is a scalar (integer) and P is a point on the curve, is the most important operation in elliptic curve cryptosystems. Scalar multiplication consists of elliptic curve group operations such as point addition and point doubling.

Table.1. Binary field arithemetic operations[4]

Polynomial elements	Binary Form	Operation
$A = X^3 + X^2$ $B = X^2 + X + 1$	A = 1100 B = 0111	**Addition** $A + B = X^3 + X^2 + X^2 + X + 1$ $= X^3 + X + 1$ $A + B = 1100 \oplus 0111$ $= 1011$
$A = X^3 + X^2$ $B = X^2 + X + 1$	A = 1100 B = 0111	**Multiplication** $A \bullet B = X^5 + X^4 + X^3 + X^4 + X^3 + X^2$ $= X^5 + X^2 \bmod X^4 + X + 1$ $A \bullet B = 1100 \bullet 0111$ =100100 (reduction step) 100100 mod 10011 = 1011
$A = X^3 + X^2$	A = 1100	**Squaring** $A^2 = X^6 + X^4$ $A^2 = \sum a^i x^{2i} = 1010000$
$A = X^3 + X^2 + 1$	A = 1101	**Inversion** $A^{-1} = X^2$, Since $(X^3 + X^2 + 1) \bullet (X^2) \bmod (X^4 + X + 1) = 1$ $A^{-1} = 00100$

ISSN 2348 – 7968

4.KARATSUBA MULTIPLICATION

Karatsuba multiplication algorithm multiplies every digit of a multiplicand by every digit of the multiplier and adds the result to the partial product. Classic or binary Karatsuba multiplier is more efficient if we truncate them at n-bit multiplicand level and use an efficient classic algorithm which called hybrid Karatsuba multiplier.The normal multiplication was performed as below,

$$P = A \cdot B = (AH^{2n} + AL) \cdot (BH^{2n} + BL)$$

$$= AH \cdot BH.2^{2n} + (AH \cdot BL + AL \cdot BH)2^{n} + AL \cdot BL.$$

It results four multiplications and three additions.hence large area.Use of karatsuba multiplier reduces the multiplication and hence reduces the area.Kartsuba multiplication shows below contain three partial products ,four additions and two subtractions,hence lesser area.

$$P = A \cdot B = (AH^{2n} + AL) \cdot (BH^{2n} + BL)$$

$$= AH \cdot BH.2^{2n} +((AH – AL).(BL - BH) + (AH.BH) + (AL.BL))A2^{n} + AL \cdot BL.$$

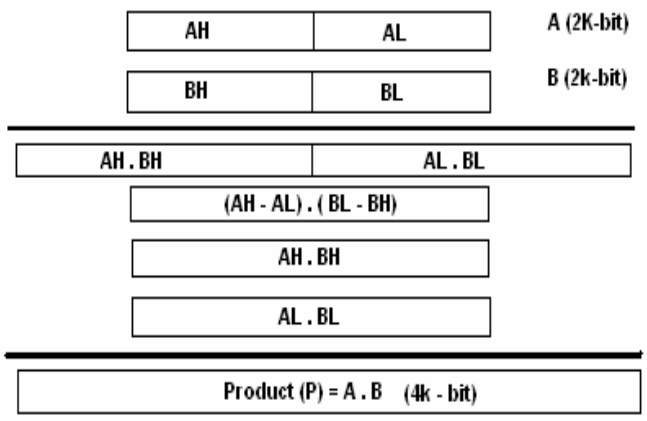

Fig. 3.Karatsuba multiplication[1]

In karatsuba multiplication, If *n* is four or more, the three multiplications in Karatsuba's basic step involve operands with fewer than *n* digits. Therefore, those products can be computed by recursive calls of the Karatsuba algorithm. The recursion can be applied until the numbers are so small that they can (or must) be computed directly.

4.1. HYBRID KARATSUBA MULTIPLIER

Hybrid karatsuba multiplier is a combination of general and simple karatsuba multipliers.In simple karatsuba multipliers we are splitting the inputs in to two,while in general karatsuba multiplier Instead of splitting into two, splits into more than two.For example, an m bit multiplier is split into m different multiplications. For all recursions less than 29 use the General Karatsuba Multiplier. For all recursions greater than 29 use the Simple Karatsuba multiplier.This is hybrid karatsuba multiplier.

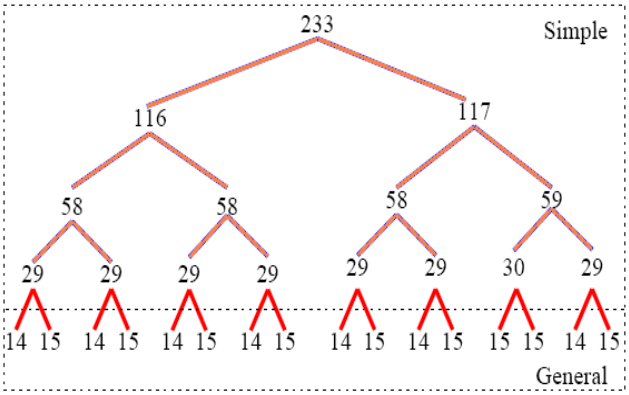

Fig. 4 .233 bit hybrid karatsuba multiplier[4]

5.POINT ADDITION AND DOUBLING

Scalar multiplication consists of elliptic curve group operations such as point addition and point doubling. The elliptic curve group operations perform finite field operations like field addition, filed multiplication, field squaring, field division and modular reduction.Let P = (x1 , y1)is a point on the elliptic curve and Q = (x 2, y 2) is another point on the curve,then point addition and doubling is computed by using the formulae as below,

Point Addition $(P+Q)$	$x_3 = \lambda^2 + \lambda + x_1 + x_2 + a$ $y_3 = \lambda(x_1 + x_3) + x_3 + y_1$ $\lambda = (y_1 + y_2)/(x_1 + x_2)$	Point Doubling $(2P)$	$x_3 = \lambda^2 + \lambda + a$ $y_3 = \lambda(x_1 + x_3) + x_3 + y_1$ $\lambda = x_1 + y_1 / x_1$

ISSN 2348 – 7968

6.SCALAR MULTIPLICATION

Elliptic curve scalar multiplication (kP), where k is a scalar (integer) and P is a point on the curve.Scalar multiplication of point P is computed using algorithm 1.

Algorithm 1: Elliptic Curve Scalar Multiplier

Input : An integer $k \neq 0$ of length l bits and base point P

Output : $Q = kP$

```
1.  begin
2.    Q = O
3.    for i = l − 2 downto 0 do
4.      Q = Double(Q)
5.      if k_i = 1 then
6.        Q = Add(Q, P)
7.      end
8.    end
9.  end
```

Fig..5.ECSMA Algorithm1[3]

7. ELLIPTIC CURVE KEY EXCHANGE

Asymmetric algorithms use a pair of keys for encryption and decryption . Encryption is done by a public key which is known to everyone. Decryption can be only done using the corresponding private key. Given the private key, the corresponding public key can easily be derived. However, the private key cannot be efficiently derived from the public key.

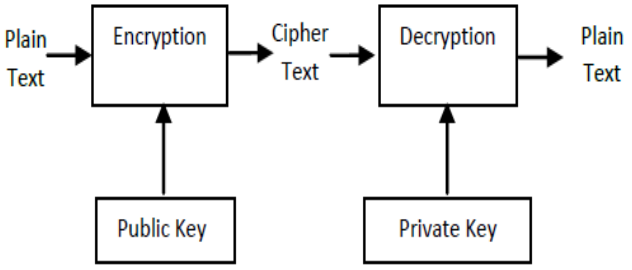

Fig..6. Public key cryptosystem[4]

8.RESULTS

8.1 SYNTHESIS REPORT

Elliptic curve scalar multiplication using both recursive karatsuba multiplier and hybrid karatsuba multiplier are implemented in Xilinx Virtex6 FPGA and the synthesis report shows that Elliptic curve scalar multiplier using hybrid karatsuba multiplier has less power and less usage of hardware resources than scalar multiplication using recursive karatsuba multiplier.

```
'
------------------------------------------------------------------
-------------
|        On-Chip        | Power (mW) |  Used  | Available |
Utilization (%) |
------------------------------------------------------------------
-------------
| Clocks                |       1.27 |      4 |    ---    |
---       |
| Logic                 |       1.15 |   9081 |     46560 |
20 |
| Signals               |       1.23 |  11524 |    ---    |
---       |
| IOs                   |       0.45 |    330 |       360 |
92 |
| Quiescent             |    1569.91 |        |           |
|
| Total                 |    1574.01 |        |           |
|
------------------------------------------------------------------
```

Fig. 7.Synthesis report showing power of Recursive Karatsuba multiplier

```
------------------------------------------------------------------
-------------
|        On-Chip        | Power (mW) |  Used  | Available |
Utilization (%) |
------------------------------------------------------------------
-------------
| Clocks                |       1.21 |      3 |    ---    |
---       |
| Logic                 |       0.99 |  13117 |     46560 |
28 |
| Signals               |       1.03 |  17950 |    ---    |
---       |
| IOs                   |       0.49 |    330 |       360 |
92 |
| Quiescent             |    1569.91 |        |           |
|
| Total                 |    1573.63 |        |           |
|
------------------------------------------------------------------
```

Fig. 8. Synthesis report showing power of Hybrid Karatsuba multiplier

ISSN 2348 – 7968

Number of slice registers		Number of Slice LUT's		Number of Bonded IOB's	
Used	Available	Used	Available	Used	Available
2720	93120	16746	46560	493	360

Fig. 9. Device utilization of recursive karatsuba multiplier

Number of slice registers		Number of Slice LUT's		Number of Bonded IOB's	
Used	Available	Used	Available	Used	Available
2812	93120	10094	46560	493	360

Fig. 10. Device utilization of Hybrid karatsuba multiplier

8.2 SIMULATION RESULT

Simulation was done using modelsim 6.4a

.

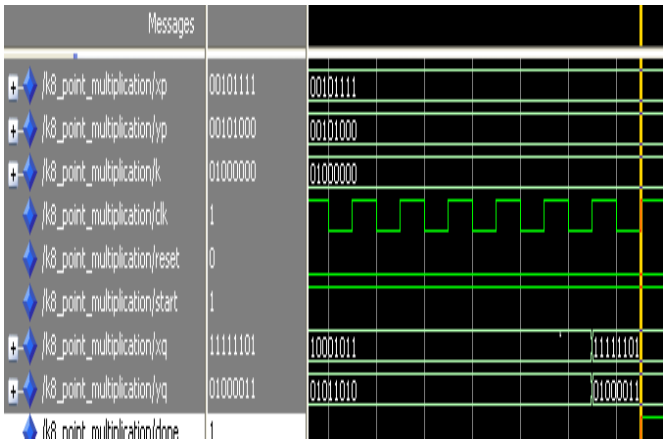

Fig. 11. 8 bit Elliptic curve scalar multiplication

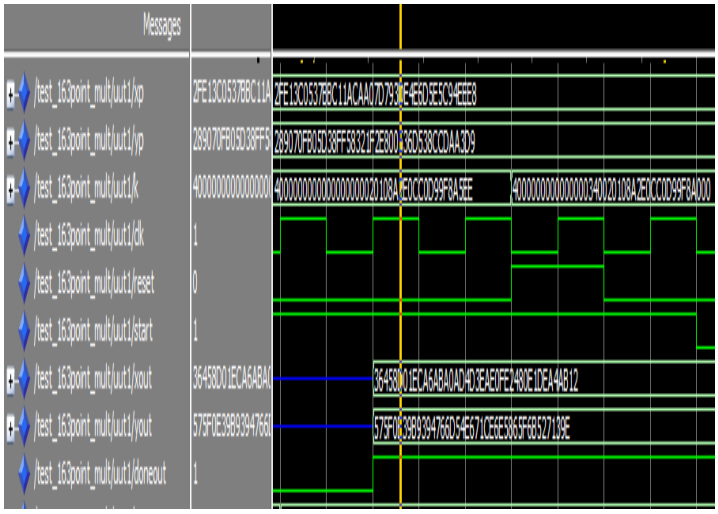

Fig. 12.163 bit elliptic curve scalar multiplication

9. COMPARISON OF RECURSIVE AND HYBRID KARATSUBA MULTIPLIERS

Table 2. Comparison of power and area of Hybrid &Recursive Karatsuba Multipliers

POWER(mw)	Recursive karatsuba multiplier	Hybrid karatsuba multiplier
	1574.01	1573.6
AREA	21327	15350

10. CONCLUSION

Elliptic curve scalar multiplication (kP), where k is a scalar (integer) and P is a point on the curve In this paper elliptic curve scalar multiplication is performed by using a hybrid karatsuba multiplier.Both Recursive and Hybrid kartsuba multipliers are simulated in Modelsim and synthesized in Xilinx ISE 14.1 xc6vlx75t-3ff784.Synthesis report shows that scalar multiplication using hybrid karatsuba multipliers have low power and less area utilization than Recursive karatsuba multiplier.

ISSN 2348 – 7968

11. REFERENCES

[1] Sujoy Sinha Roy, Chester Rebeiro, and Debdeep Mukhopadhyay" Theoretical Modeling of Elliptic Curve Scalar Multiplier on LUT-Based FPGAs for Area and Speed" IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, VOL. 21, NO. 5, MAY 2013

[2] G. Orlando and C. Paar, "A high performance reconfigurable elliptic curve processor for GF(2m)," in Proc. 2nd Int. Workshop Cryptographic Hardw. Embedded Syst., 2000, pp. 41–56.

[3] N. Gura, S. C. Shantz, H. Eberle, S. Gupta, V. Gupta, D. Finchelstein, E. Goupy, and D. Stebila, "An end-to-end systems approach to elliptic curve cryptography," in Proc. 4th Int. Workshop Cryptographic Hardw. Embedded Syst., 2003, pp. 349–365.

[4] en.wikipedia.org/wiki/Hybrid karatsuba multipliers

BIOGRAPHY

Ms.Jayalakshmi K R, received her BTech degree in Electronics and Communication Engineering from Mangalam College of Engineering, Kottayam,India in 2013 and pursuing MTech in VLSI And Embedded system in Mangalam College Of Engineering, Kottayam,India.

Ms.Hima Sara Jacob, Assistant professor at Mangalam College of Engineering,Kottayam,India.She completed her B-Tech in applied electronics and instrumentation from Saint Gits college of engineering,Kottayam,India and Received her M.Tech in VLSI and Embedded system from SaintGits college of engineering,Kottayam,India.