International Journal of Advanced Computer Technology (IJACT)

ISSN:2319-7900

AN EFFICIENT DESIGN OF LOW POWER,FAST ELLIPTIC CURVE SCALAR MULTIPLIER IN ECC USING KARATSUBA MULTIPLIERS

Jayalakshmi K R, M.Tech student, Mangalam college of engineering,Kottayam,India;
Ms.Hima Sara Jacob, Assistant professor, Mangalam college of engineering, Kottayam,India;
Ms.Jyothisree K R, Assistant professor ,Mangalam college of engineering, Kottayam,India

Abstract—Cryptography is where security engineering meets mathematics. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it.ECC is an alternative mechanism for implementing public-key cryptography.In this paper high speed and low power elliptic curve scalar multiplication is done using Karatsuba multipliers.Various types of karatsuba multipliers are implemented and compared.

Keywords :

Cryptography,Hybrid karatsuba multiplier,Elliptic curve cryptography(ECC),Point addition,Doubling.

I. INTRODUCTION

Cryptography provides us with the tools that underlie most modern security protocols. It is probably the key enabling technology for protecting distributed systems, yet it is surprisingly hard to do right.It is a mathematical based technology to ensure the information security over a public channel. In 1985, Neal Koblitz and Victor Miller independently proposed ECC using elliptic curves to design public key cryptographic systems. In the late 1990`s, ECC was standardized by a number of organizations and it started receiving commercial acceptance. Nowadays, it is mainly used in the resource constrained environments, such as adhoc wireless networks and mobile networks. There is a tend that conventional public key cryptographic systems are gradually replaced with ECC systems.As computational power evolves, the key size of the conventional systems is required to be increased dramatically.

In ECC Elliptic curve scalar multiplication is (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. Elliptic curves are not ellipses. They are so named because of the fact that ellipses are formed by quadratic curves. Elliptic curves are always cubic and have a relationship to elliptic integrals in mathematics where the elliptic integral can be used to determine the arc length of an ellipse.

In this paper Karatsuba multipliers are used for elliptic curve scalar multiplication. Hence there is low area and power consumption. Elliptic curve scalar multiplication using both hybrid karatsuba multipliers and recursive karatsuba multipliers are simulated and implemented.

II.ELLIPTIC CURVE CRYPTOGRAPHY(ECC)

ECC offers the smallest key size and the highest strength per bit of any known public-key cryptosystem. This stems from the discrete logarithm problem in the group of points over an elliptic curve. Given a curve, *E*, defined along some equation in a finite field (such as E: $y^2 = x^3 + ax + b$), point multiplication is defined as the repeated addition of a point along that curve. Denote as $nP = P + P + P + \ldots + P$ for some scalar (integer) *n* and a point $P = (x, y)$ that lies on the curve, *E*. This type of curve is known as a Weierstrass curve. The security of modern ECC depends on the intractability of determining *n* from $Q = nP$ given known values of *Q* and *P*. It is known as the elliptic curve discrete logarithm problem.

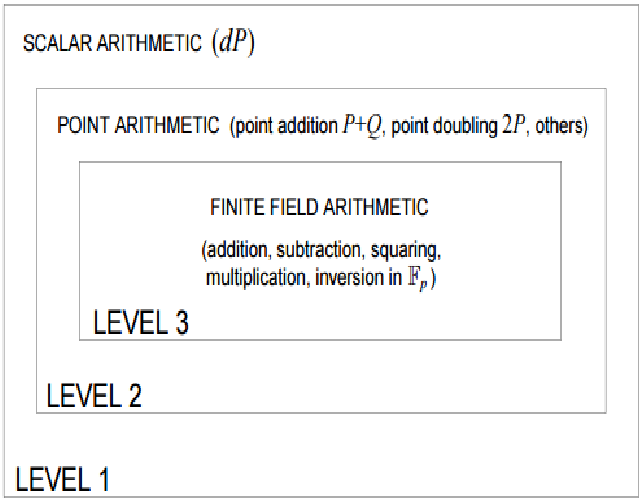

SCALAR ARITHMETIC (dP)
POINT ARITHMETIC (point addition $P+Q$, point doubling $2P$, others)
FINITE FIELD ARITHMETIC
(addition, subtraction, squaring, multiplication, inversion in $\mathbb{F}_p$)
LEVEL 3
LEVEL 2
LEVEL 1

Figure.1.ECC Mathematical Hiearchi[3]

ISSN:2319-7900

III.CURVE BASED CRYPTOGRAPHY

The main operation in any curve-based primitive is scalar multiplication.The general hierarchical structure for operations required for implementations of curve-based cryptography is given below. Point/divisor multiplication is at the top level. At the next (lower) level are the point/divisor group operations. The lowest level consists of finite field operations such as addition, multiplication and inversion required to perform the group operations.

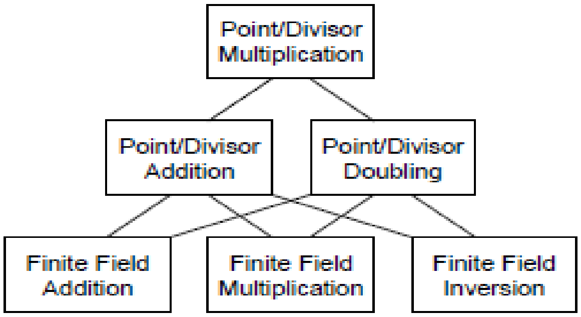


Figure. 2. Hierarchy for ECC[3]

IV FINITE FIELD MULTIPLICATION

Finite field multiplication of two elements in the field $GF(2^n)$ is defined as $C(x) = A(x)B(x) \bmod P(x)$, where $A(x)$, $B(x)$ and $C(x) \in GF(2^n)$ and $P(x)$ is the irreducible polynomial of degree n which generates the field$GF(2^n)$. Implementing the multiplication requires two steps. First, the polynomial product $C'(x) = A(x)B(x)$ is determined then, the modulo operation is done on$C'(x)$. The Karatsuba algorithm is used for the polynomial multiplication. The basic recursive Karatsuba multiplier cannot be applied directly to ECC because the binary extension fields used in standards such as have a degree which is prime.

There have been several published works such as the Binary Karatsuba Multiplier , the Recursively Applied Iterative Karatsuba , the Simple Karatsuba Multiplier and the General Karatsuba Multiplier . The Simple Karatsuba Multiplier is the basic recursive Karatsuba multiplier with a small modification. If an n bit multiplication is needed to be done, n being any integer, it is split into two polynomials. The Karatsuba multiplication can then be done with two $n/2$ bit multiplications and one $n/2$ bit multiplication. In the General Karatsuba Multiplier, the multiplicands are split into more than two terms. For example an n term multiplier is split into n different terms.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 General Karatsuba multiplier is more efficient for small sizes of multiplicands, while the Simple Karatsuba multiplier is efficient for large multiplicands. In our proposed Hybrid Karatsuba multiplier, all recursions are done using the Simple Karatsuba multiplier except the final recursion. The final recursion is done using a General Karatsuba multiplier when the multiplicands have a size less than 29 bits. The initial recursions using the Simple Karatsuba multiplier result in low gate count, while the final recursion using the General Karatsuba multiplier results in low LUT requirements. For a 233-bit Hybrid Karatsuba multiplier, the initial four recursions are done using the Simple Karatsuba multiplier, while the final recursion is done with 14-bit and 15-bit General Karatsuba multipliers.

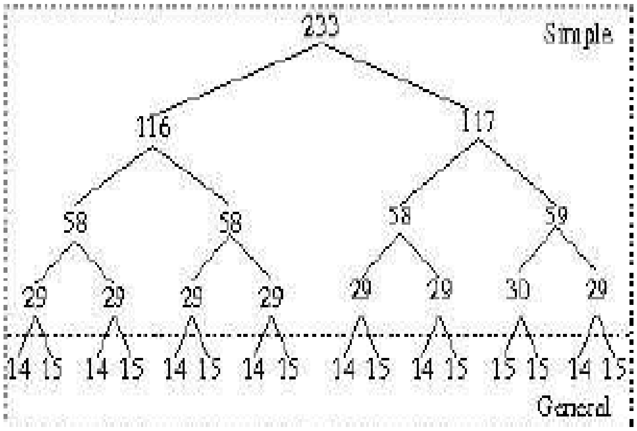


Figure.3. 233 bit Hybrid karatsuba multiplier[2]

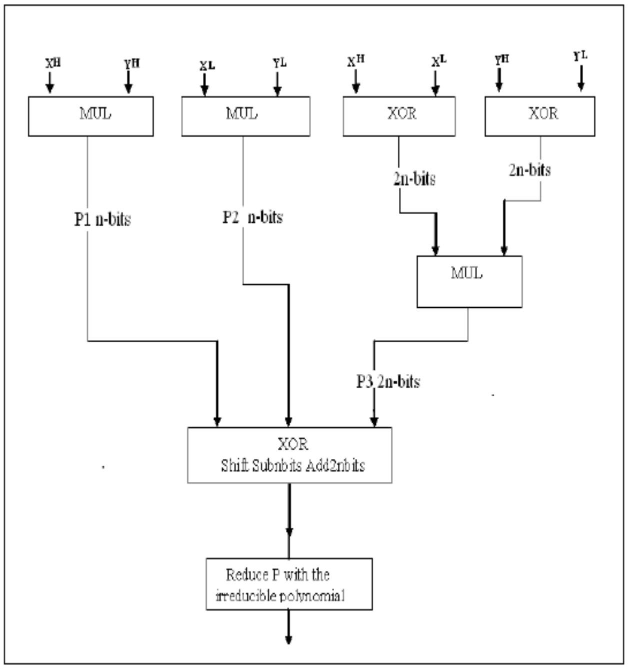


Figure.4.Hardware diagram for Karatsuba Multiplier[2]

V. POINT ADDITION AND POINT DOUBLING

To add two distinct points P and Q on an elliptic curve, draw a straight line between them. The line will intersect the elliptic cure at exactly one more point –R. The reflection of the point –R with respect to x-axis gives the point R, which is the results of addition of points R and Q.To the point P on elliptic curve, draw the tangent line to the elliptic curve at P. The line intersects the elliptic cure at the point –R. The reflection of the point –R with respect to x-axis gives the point R, which is the results of doubling of point P.

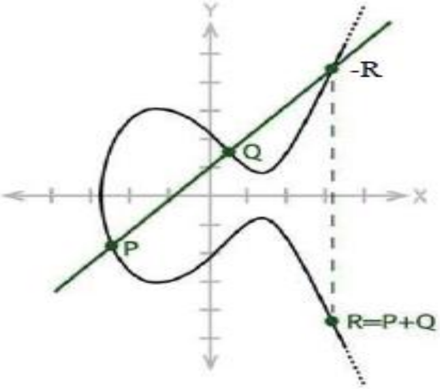


Figure 5.Point addition[3]

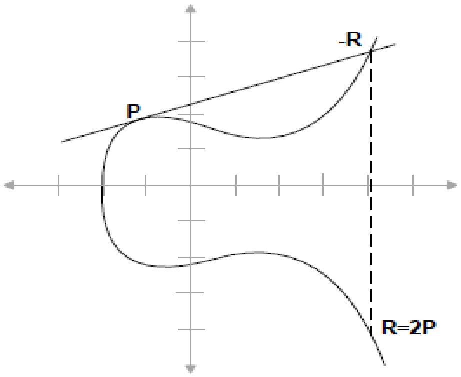


Figure 6.Point doubling[3]

VI. ELLIPTIC CURVE SCALAR MULTIPLICATION

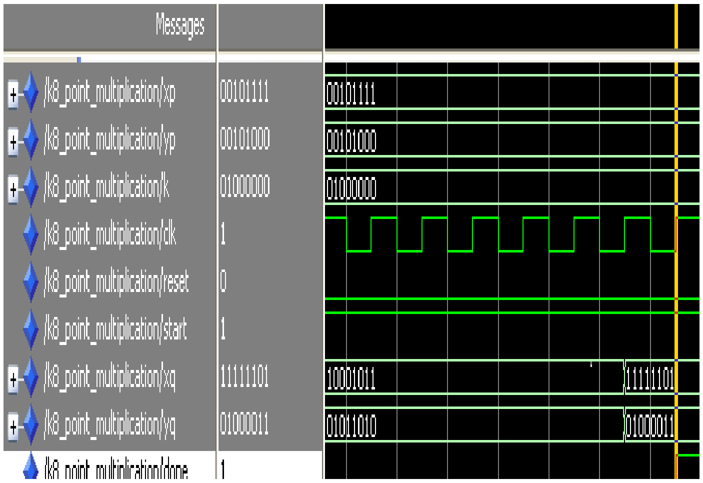
Elliptic curve scalar multiplication (kP), where k is a scalar (integer) and Q is a point on the curve.Scalar multiplication of point Q is computed using the below algorithm.

```
Algorithm 4 Scalar Multiplication by Double and Add Method
Input: Integer $k = (k_{l-1}, k_{l-2}, \ldots, k_1, k_0)_2$, Point $P$
Output: Point $Q = kP$
  $Q \leftarrow \mathcal{O}$;
  if $(k_{l-1} == 1)$ then
    $Q \leftarrow P$;
  for $i = l - 2$ downto $0$ do
    $Q \leftarrow$ DOUBLE$(Q)$;
    if $(k_i == 1)$ then
      $Q \leftarrow$ ADD$(Q, P)$;
```

Figure.7.Double and Add Algorithm.[3]

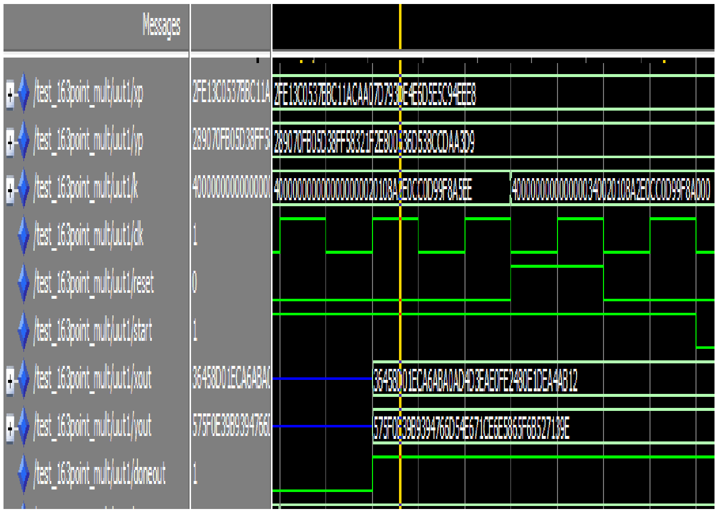
VII. RESULTS

A.SIMULATION RESULT



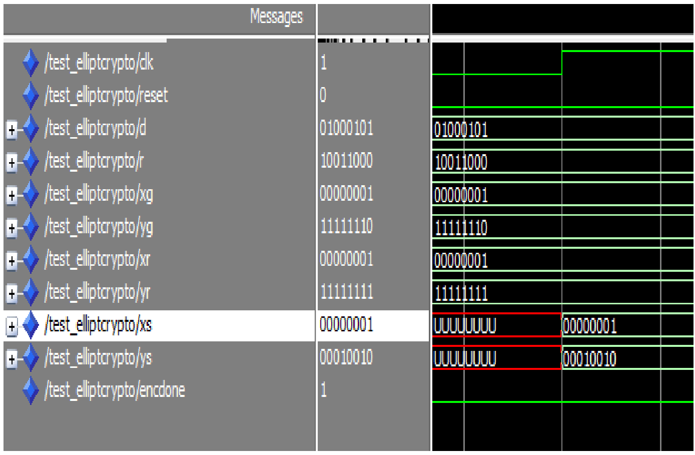
```
Messages
/k8_point_multiplication/xp      00101111   00101111
/k8_point_multiplication/yp      00101000   00101000
/k8_point_multiplication/k       01000000   01000000
/k8_point_multiplication/clk     1
/k8_point_multiplication/reset   0
/k8_point_multiplication/start   1
/k8_point_multiplication/xq      11111101   10001011   11111101
/k8_point_multiplication/yq      01000011   01011010   01000011
/k8_point_multiplication/done    1
```

Figure.8.8 bit Elliptic curve scalar multiplication



```
Messages
/test_163point_mult/uut1/xp      2FE13C0537BBC11A   2FE13C0537BBC11ACAA07D793E4E6D5E5C94EEE8
/test_163point_mult/uut1/yp      289070FB05D38FF5   289070FB05D38FF58321F2E80036D538CCDAA309
/test_163point_mult/uut1/k       4000000000000000   40000000000000000002010BA2E0CC0D99F8A5EE   400000000000000340020108A2E0CC0D99F8A000
/test_163point_mult/uut1/clk     1
/test_163point_mult/uut1/reset   0
/test_163point_mult/uut1/start   1
/test_163point_mult/uut1/xout    36458D01ECA6ABA0   36458D01ECA6ABA0AD4D3EAE0FE2480E1DEA4AB12
/test_163point_mult/uut1/yout    575F0E39B939476E   575F0E39B9394766D54E671CE6E5865F6B527108E
/test_163point_mult/uut1/doneout 1
```

Figure.9.163 bit Elliptic curve scalar multiplication



```
Messages
/test_eliptcrypto/clk       1
/test_eliptcrypto/reset     0
/test_eliptcrypto/d         01000101
/test_eliptcrypto/r         10011000
/test_eliptcrypto/xg        00000001
/test_eliptcrypto/yg        11111110
/test_eliptcrypto/xr        00000001
/test_eliptcrypto/yr        11111111
/test_eliptcrypto/xs        00000001
/test_eliptcrypto/ys        00010010
/test_eliptcrypto/encdone   1
```

Figure.10.8 bit Encryption

B.SYNTHESIS RESULTS

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 |         |           |
|
-----------------------------------------------------------------
```

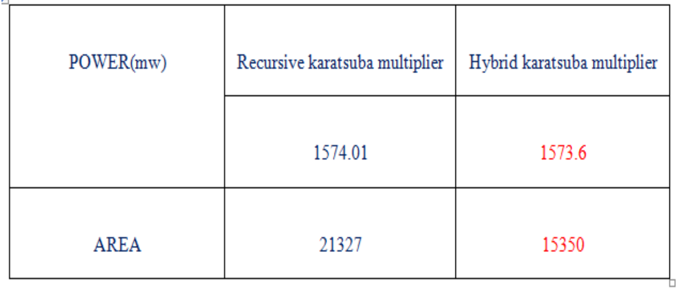
Figure.11.Power Report of Recursive Karatsuba multiplier

```
-----------------------------------------------------------------
-------------
|        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 |         |           |
|
-----------------------------------------------------------------
```

Figure.12.Power Report of Hybrid Karatsuba multiplier

C.COMPARISON

Table 1. Comparison of Two Karatsuba Multipliers



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

VIII.CONCLUSION

Cryptography is a mathematical based technology to ensure the information security over a public channel.Elliptic curve cryptography(ECC) is considered a more suitable choice because ECC obtains higher performance, lower power consumption,and smaller area on most platforms.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 Virtex6 FPGA.Synthesis report shows that scalar multiplication using hybrid karatsuba multipliers have low power and less area utilization .

IX.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]] K. Järvinen, “Optimized FPGA-based elliptic curve cryptography processor for high speed applications,” Integr., VLSI J., vol. 44, no. 4, pp. 270–279, Sep. 2011.

[4] N. A. Saqib, F. Rodríguez-Henríquez, and A. Diaz-Perez, “A parallel architecture for fast computation of elliptic curve scalar multiplication over GF(2m),” in Proc. 18th Int. Parallel Distrib. Process. Symp., Apr. 2004, pp. 144–151.

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 Saint Gits college of engineering,Kootayam,India.

Ms.Jyothisree K R, , Assistant professor at Mangalam College of Engineering,Kottayam,India.She completed her B-Tech in electronics and communication engineering from Mangalam college of engineering,Kottayam,India.She Received her M.Tech in Embedded system Technology.