International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163
Volume 1 Issue 6 (July 2014) http://ijirae.com

VHDL Implementation of ECC Processor over GF (2^163)

Shemina A Karim
Dept. of ECE, MG University, Kerala
Mangalam College of Engineering

Reneesh C.Zacharia
Dept. of ECE, MG University, Kerala
Mangalam College of Engineering

Rijo Sebastian
Dept. of ECE, MG University, Kerala
Mangalam College Engineering

Abstract*— ECC (Elliptic curve cryptography) is the most modern technology arising in the more secure data transmission in the field of Public key cryptography. As compared to the RSA it requires smaller keysize. ECC is defined over Galois Fields over (2^163).The basis of ECC is the point multiplication, which involves the point addition and doubling, finite field arithmetic's. Montgomery modular multiplication is used for the efficient implementation of the finite field in ECC Processor. Synthesized with Xilinx ISE 13.2 and simulated in Modelsim.

***Keywords*— Elliptic curve cryptographic Processor, Montgomery multiplier, Point Multiplication, FPGA, Finite Field Arithmetic**

I. INTRODUCTION

Cryptography is the processes of making the transfer of data secure, to avoid the eaves drops. The cryptography is divided into mainly two. Public key cryptography and symmetric key cryptography .RSA is the well established public key cryptography. Cryptography having a cryptographic algorithm in which it needs a plain text and cipher text, for the public key cryptography the senders and receivers key is different. For symmetric key both the keys are same [2].It consists of the encryption and decryption of data ,the encryption key and decryption key are different for the Public key cryptography.

Elliptic curve cryptography (ECC) is superior to RSA. The advantage of ECC over RSA is it having the lesser key size compared to the RSA.ECC is defined with finite field over Elliptic curves. Finite field is also termed as the Galois field, which involves the finite field arithmetic. ECC is based on the point multiplication. The point multiplication is composed with the point addition and doubling and the finite field arithmetic's.

The ECC was introduced by by Koblitz[4] and Miller[3].ECC is an attractive cryptographic method, which is used in mobile communication .FPGA implementation of ECC processor over GF(2^163) is more efficient and high performance. The point multiplication of ECC involves the point P which on the elliptic curve E and k is the integer and Q is defined as Q=kP, means the P is added k times .Montgomery multiplication is introduced in the point multiplication in ECC processor[5]. The scalar point multiplication over GF(2^163)is implemented with binary fields and synthesized with Xilinx ISE and Modelsim.

II. ARCHITECTURE OF ECC OVER GF(2^163) .

Point multiplication is the heart of ECC having high speed and which is defined in to three distinct layers.

a) Point multiplication
b) Point addition and Doubling
c) Finite field Arithmetic

The Architecture of ECC is shown below.

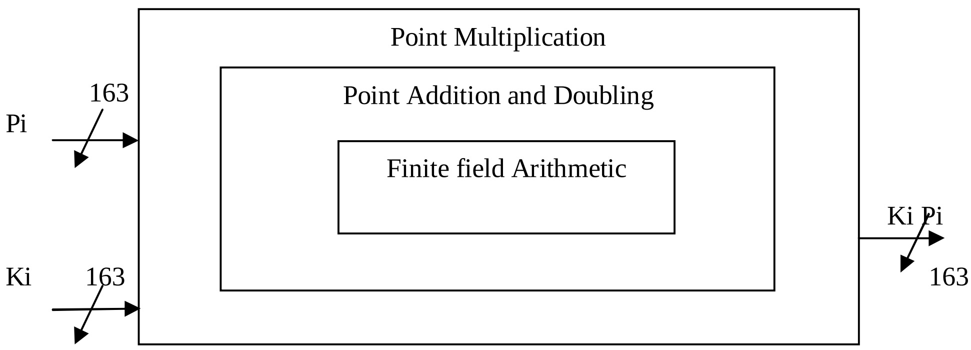


Fig.1 Architecture of ECC

The finite field arithmetic is the inner most part, after that the point addition and doubling, and the point multiplication is the combined with this all factors, which forms the top most layer. The scalar point multiplication is found out by P is added k times to itself [1].

A. Finite Field Arithmetic over GF(2^163)

The Finite field arithmetic is well in cryptographic design. Which involves the mainly four different layers, also we can say that it constitutes [2] :-

1) Addition
2) Multiplication
3) Squaring
4) Division /Inversion

1. Addition

The addition operation in Finite field arithmetic is simple XOR operation .it is defined as follows,
C(x)= A xor B Mod f(x),where f(x) is the defined polynomial over GF(2^163).

Algorithm 1

```
for i in 0 . . m-1 loop
c(i) :=(a(i) + b(i)) mod f;
end loop;
```

where as,
c(x)= a(x) xor b(x) = $\sum_{i=0}^{m-1}$ cmod f

2. Multiplication

Algorithm 2-*Montgomery Multiplier*

Input :a(x),b(x),f(x)
Output :c(x)= a(x)b(x)x^{-m} mod f(x)

```
1.c(x) := 0
2.for i = 0 to m-1 do
3.c(x) := c(x)+a1b(x)
4.c(x) :=c(x) +c
```

3. Squaring

Algorithm 3-*Montgomery Squarer*

```
for I in 0  . . 2*m-2 loop c(i)  := 0; end loop;
for i in 0 . . m-1 loop c(2*i)  :=a(i);d(i) :=0;
end loop;
for I in 0 . . m-1 loop
if c(0)=1 then
c := m2xvv2(c, f);
c(m) :=m2xor(c(m),1);
end if;
c :=lshift2(c);
end loop;
```

4. Division

Algorithm 4- *Binary algorithm polynomial*

```
A:=f; b:=h; c:=zero; d:=g; alpha:=m; beta :=m-1;
While beta >=0 loop
If b(0)=0 then
b:=shift _one (b);d:=divide _ by _x(d, f);beta :=beta-1
else
old b:b;  old d:=d;  old _beta:=beta;
 b:=shift _one add(add(a, b));
d :=divide _by _x(add(c ,d)f);
if alpha>beta then
a:= old; c:=old; beta:=alpha-1;alpha:=old beta;
else beta :=beta-1;
else beta:=beta-1;
end if;
end if;
end loop;
z :=c;
```


International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163
Volume 1 Issue 6 (July 2014) http://ijirae.com

B . Point addition and Doubling

Point doubling can be substituted by squaring ,over the finite field by a simple operation .It is constituted by the squaring that done in the field arithmetic. Point Addition is carried out by the field GF(2^163).

Let P=(x1, y1),Q=(x2,y2) over F2^m where P and Q are two points defined in the elliptic curve E defined with the polynomial f(x)=$x^{163}+x^{7}+x^{6}+x^{3}+1$.

Point Addition:

P+Q =(X3,Y3) where x3=λ2+λ1+x1+x2+a ,y3=λ(x1+x3)+x3+y1 and λ=(y1+y2)/(x1+x2).

Point Doubling:

2P=(x3,y3) where x3=λ2+λ+a=x12+b/x12,y3=x12+λx3+x3 and λ=x1+y1/x1 [4].

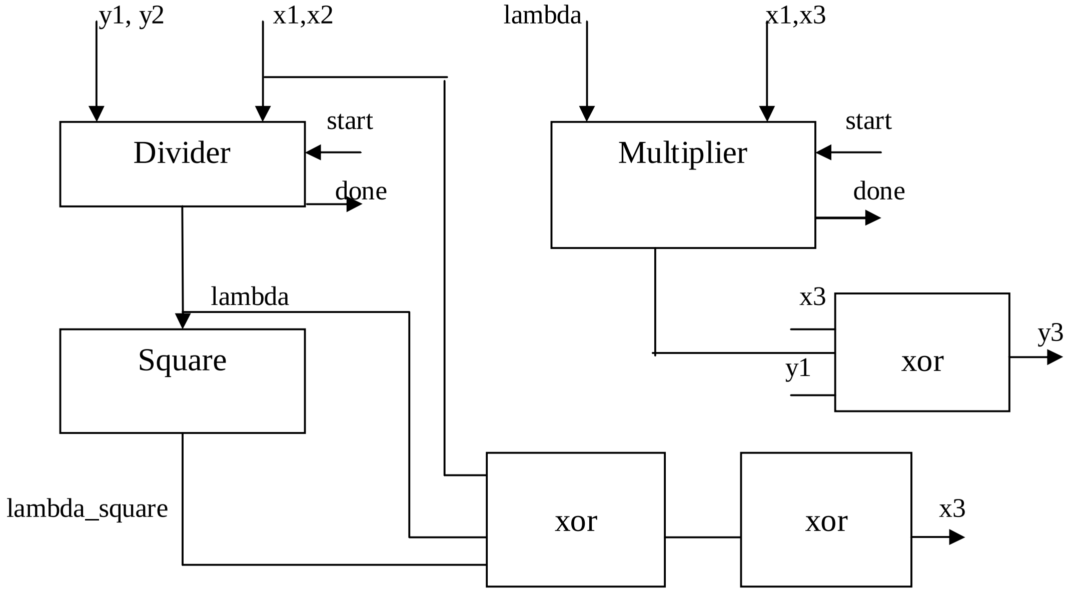


Fig 2.Block diagram for Point addition operation.

C . Point Multiplication

Point Multiplication is the basis of ECC Processor.All the finite field arithmetic, point addition and doubling constitutes the point multiplication .Montgomery point multiplication shows less delay, area and power [5].

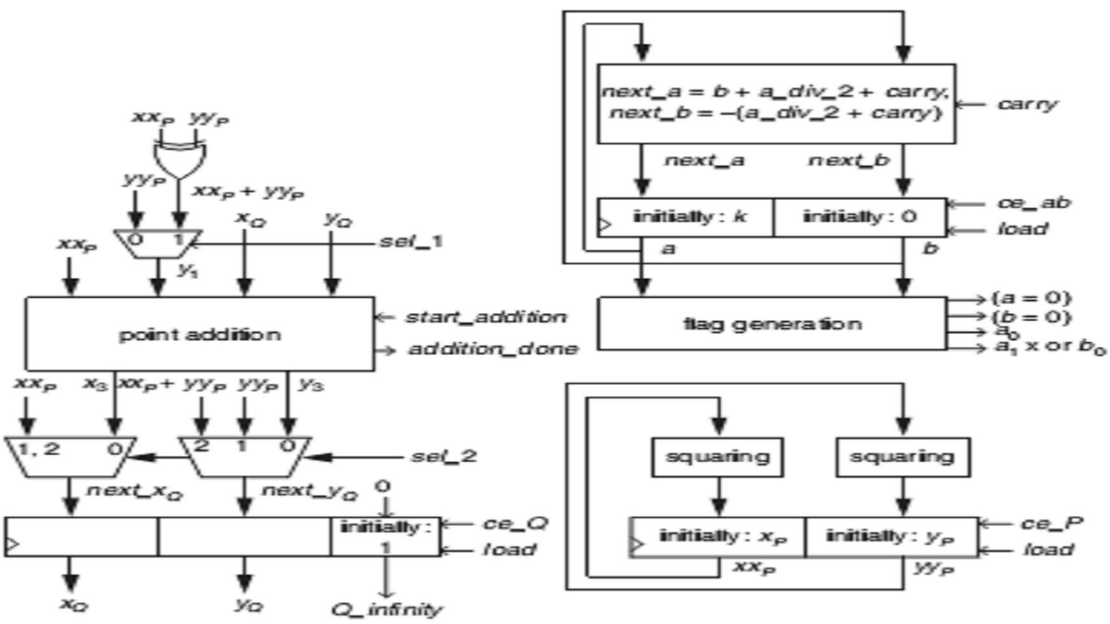


Fig 3.Architecture for Point Multiplication

III. SYNTHESIS AND SIMULATION RESULTS

A. Simulation Result.

The point addition and multiplication is synthesized and simulated in Modelsim for the field of GF(2^163)defined with the polynomial f(x)= x^{163} + x^7 + x^6 + x^3 +1

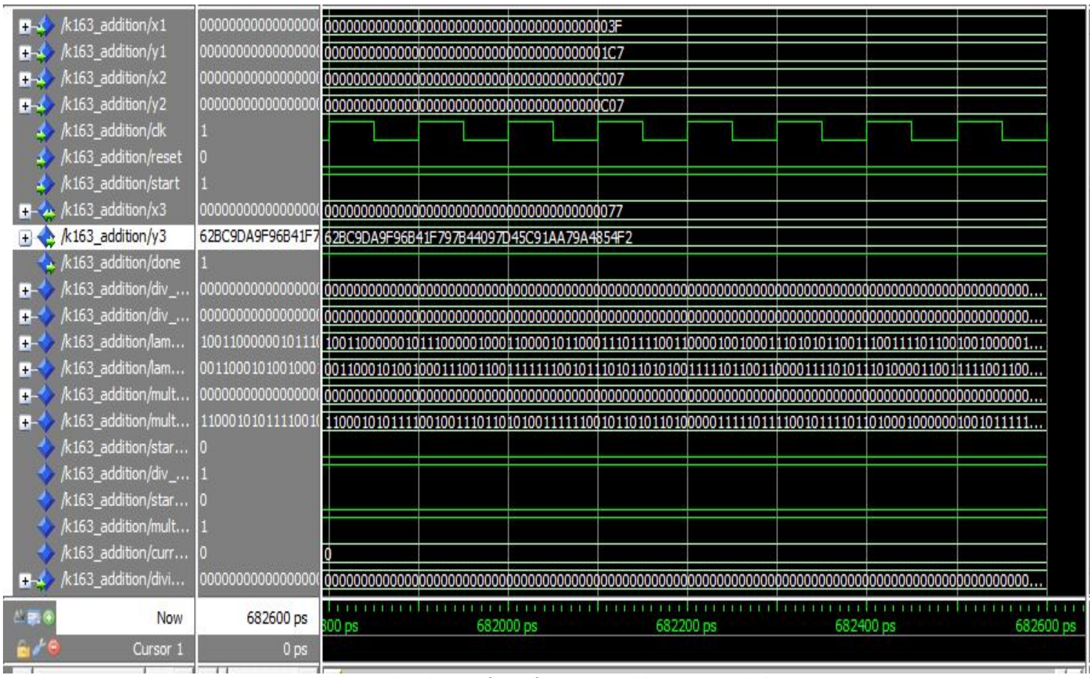


Fig. 4. Simulated waveform for Point Addition in Modelsim.

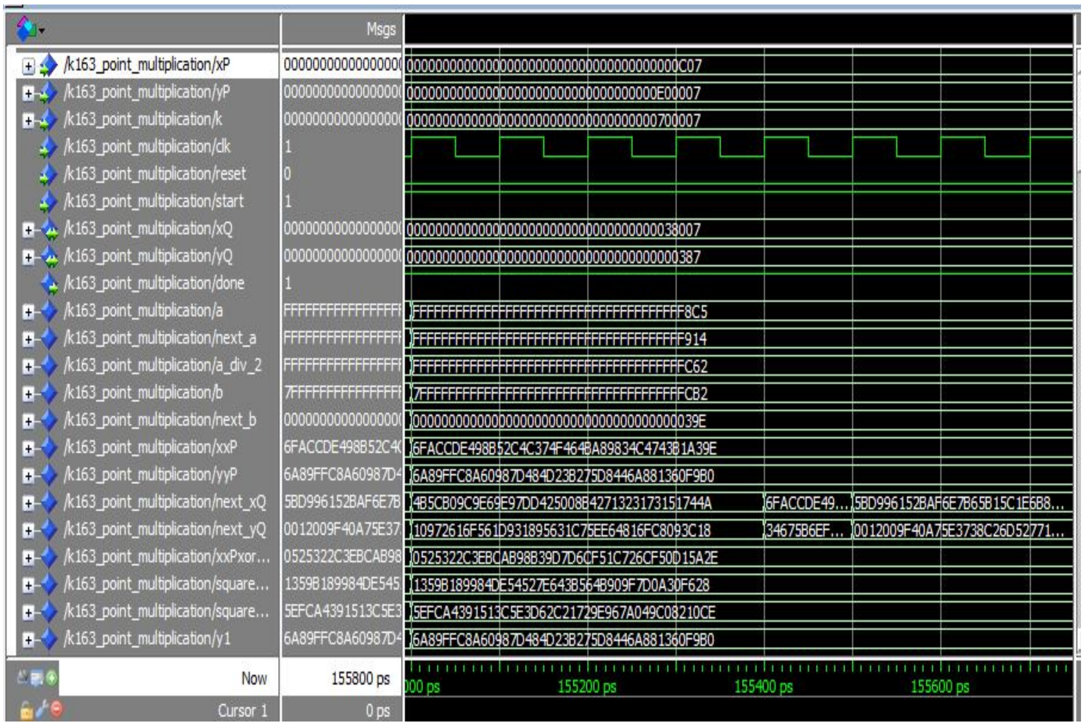


Fig. 5. Simulated waveform for Point multiplication in Modelsim

B. Synthesis Results

The point multiplication with interleaved multiplier and Montgomery multiplier is synthesized using Xilinx ISE 13.2 and the Device utilization summary for Point multiplication is displayed.

International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163
Volume 1 Issue 6 (July 2014) http://ijirae.com

Device Utilization Summary (est	
Logic Utilization	**Used**
Number of Slices	2080
Number of Slice Flip Flops	2163
Number of 4 input LUTs	3678
Number of bonded IOBs	819
Number of GCLKs	1

Fig.6. Device utilization summary for point multiplication using Interleaved multiplier

Device Utilization Summary (est	
Logic Utilization	**Used**
Number of Slices	2014
Number of Slice Flip Flops	2159
Number of 4 input LUTs	3680
Number of bonded IOBs	819
Number of GCLKs	1

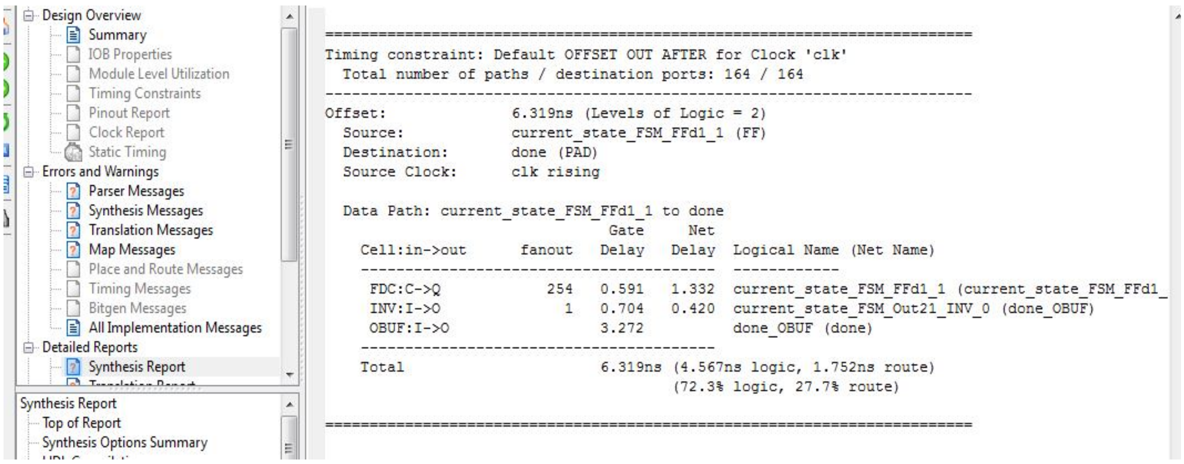
Fig.7 .Device utilization summary for point multiplication using Montgomery multiplier

Power Summary	
Optimization	None
Data	Production
Quiescent(W)	0.036
Dynamic (W)	0.403
Total (W)	0.439

Fig 8. Interleaved multiplier

Power Summary	
Optimization	None
Data	Production
Quiescent(W)	0.032
Dynamic (W)	0.052
Total (W)	0.085

Fig.9 Mongomery Multiplier




```
================================================================================
Timing constraint: Default OFFSET OUT AFTER for Clock 'clk'
  Total number of paths / destination ports: 164 / 164
--------------------------------------------------------------------------------
Offset:              6.319ns (Levels of Logic = 2)
  Source:            current_state_FSM_FFd1_1 (FF)
  Destination:       done (PAD)
  Source Clock:      clk rising

  Data Path: current_state_FSM_FFd1_1 to done
                                Gate     Net
    Cell:in->out      fanout   Delay   Delay  Logical Name (Net Name)
    ----------------------------------------  ------------
     FDC:C->Q            254   0.591   1.332  current_state_FSM_FFd1_1 (current_state_FSM_FFd1_
     INV:I->O              1   0.704   0.420  current_state_FSM_Out21_INV_0 (done_OBUF)
     OBUF:I->O                 3.272          done_OBUF (done)
    ----------------------------------------
    Total                      6.319ns (4.567ns logic, 1.752ns route)
                                       (72.3% logic, 27.7% route)

================================================================================
```

Fig 10. Point multiplication delay obtained using interleaved multiplier

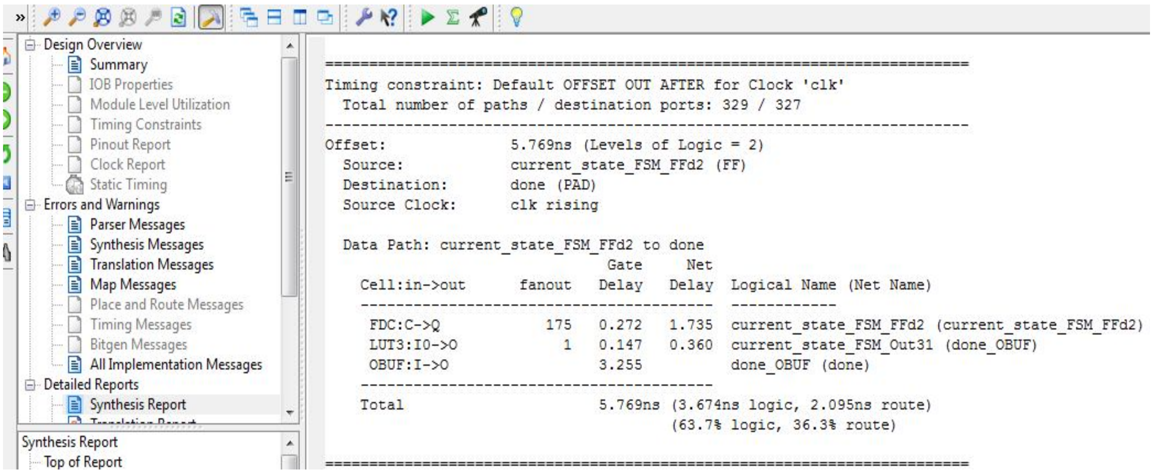


Fig 11. Point multiplication Delay obtained with Montgomery multiplier

C. *Comparison of Results*

TABLE I
COMPARISON OF PIONT MULTIPLICATION AREA, POWER, DELAY

Multiplier used	Number of slices	Power (W)	Delay (ns)
Interleaved	2080	0.439	6.319
Montgomery	2014	0.85	5.769

IV. CONCLUSIONS

Proposed ECC Processor over GF(2^163) was simulated using Modelsim and synthesized with Xilinx ISE 13.2.The area, power and delay was estimated .The comparison of point multiplication using interleaved and Montgomery multiplier is tabulated.

ACKNOWLEDGMENT

I owe my heartfelt gratitude to God almighty for all the blessings showered on me during this endeavour. I take this opportunity to show my sincere thanks towards all who helped me to finish this research work.

REFERENCES

[1]" Novel Architecture for Efficient FPGA Implementation of Elliptic Curve Cryptographic Processor Over GF(2^163)" by Hossein Mahdizaeh and Massoud Ma soumi. *IEEE Transactions on Very Large Scale Integration Systems*,vol.21 ,no.12,December 2013.
[2]W.Stallings, Cryptography and Network Security, 4th Ed..,Prentice-Hall,2006.
[3]K.Jarvenin,M.Tommiska, and J.Skytta,"A scalable architecture for elliptic curve point multiplication"ICFPT,Brisbane,Australia,2004.
[4]T.Wollinger, J.Guuajardo, and C.Paar,"Security on FPGAs:State-of-the –art and Lmplementations Attacks,"ACM Trans. On Embedded Computing Sys.,3(3):534-574,2004.
[5]R.C.C.Cheung,N.J Telle,W.Luk, and P.Y.K.Cheung,"Customizable elliptic curve Cryptosystems" IEEE Trans.Very Large Scale Integr.(VLSI) Syst."., vol.13,no.9,pp.1048-1059,Sep.2005.
[6]W.N.Chelton and M.Benaissa,"Fast elliptic curve cryptography on FPGA,"IEEE Trans.on Very Large Scale Integration (VLSI)Systems." Vol.16,no.2,Feb.2008,pp.198-205.
[7]B.Ansari and a.Hasan,"High-Performance Architecture of Elliptic Curve Scalar multiplication",IEEE Trans.on Comp.,Vol.57, No. 11, pp.1443-1453.,Nov.2008
[8]C.H.Kim,S.Kwon, C.P.Hong,"FPGA implementation of high performance elliptic curvecryptographic processor over GF(2^163),"J.of Sys.Architecture, 54 (10)(2008) 893-900.
[9] J.Fan, K. Sakiyama, and I .Verbanuwhede," Montgomery modular multiplication algorithm on multi-core systems," in Proc.IEEE Workshop Signal Process.Syst.,Shanghai,China,Oct.2007,pp. 261-266.
[10]Z.Chen and P.Schaumont ,"A parallel implementation of Montgomery multiplication on multicore Systems:Algorithm,analysis,and prototype,"IEEE Trans.Comput.,vol.60,no.12, pp.1692-1703,Dec.2011.