IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735. Volume 6, Issue 2 (May. - Jun. 2013), PP 11-14
www.iosrjournals.org

Low Power FPGA Based Elliptical Curve Cryptography

Ajay S[1], Kotresh H[2], Shruthi B S[3,] Swetha G S[4], Srividya B V[5]
[1,2,3,4]*Students of Telecommunication Engineering department, Dayananda Sagar College of engineering.*
[5] *Assistant Professor, Telecommunication Engineering department, Dayananda Sagar College of engineering. Bangalore-78*

Abstract: *Cryptography is the study of techniques for ensuring the secrecy and authentication of the information. The development of public-key cryptography is the greatest and perhaps the only true revolution in the entire history of cryptography. Elliptic Curve Cryptography is one of the public-key cryptosystem showing up in standardization efforts, including the IEEE P1363 Standard. The principal attraction of elliptic curve cryptography compared to RSA is that it offers equal security for a smaller key-size, thereby reducing the processing overhead. As a Public-Key Cryptosystem, ECC has many advantages such as fast speed, high security and short key. It is suitable for the hardware of implementation, so ECC has been more and more focused in recent years. The hardware implementation of ECC on FPGA uses the arithmetic unit that has small area, small storage unit and fast speed, and it is an extremely suitable system which has limited computation ability and storage space.[1][2] The modular arithmetic division operations are carried out using conditional successive subtractions, thereby reducing the area. The system is implemented on Vertex-Pro XCV1000 FPGA.*
Index Terms – VHDL, FSM, FPGA, Elliptic Curve Cryptography.

I. Introduction

Elliptic curve arithmetic can be used to develop a variety of elliptic curve cryptographic (ECC) schemes including key exchange, encryption and digital signature. The study of elliptic curves by algebraists, algebraic geometers and number theorists dates back to the middle of the nineteenth century. Elliptic Curve Cryptography (ECC) was discovered in1985 by Neil Koblitz and Victor Miller. Elliptic Curve Cryptographic (ECC) schemes are public-key mechanisms that provide the same functionality as RSA schemes. However, their security is based on the hardness of a different problem, namely the Elliptic Curve Discrete Logarithmic Problem (ECDLP). At the time of its discovery, the ECC algorithm was described and placed in the public domain. What others found was that while it offered greater potential security it was slow. Certicom focused its efforts on creating better implementations of the algorithm to improve its performance. After many years of research, Certicom introduced the first commercial toolkit to support ECC and make it practical for use in a variety of applications. Most of the products and standards that use public-key cryptography for encryption and digital signatures use RSA schemes. The competing system to RSA is elliptic curve cryptography. The principal attraction of elliptic curve cryptography compared to RSA is that it offers equal security for a smaller key-size
. An elliptic curve E over a field R of real numbers is defined by an equation

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

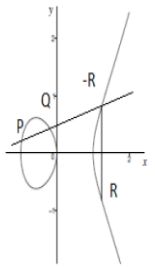
Here a_1, a_2, a_3, a_4, a_6 are real numbers belong to R, x and y take on values in the real numbers. If L is an extension field of real numbers, then the set of L-rational points on the elliptic curve E is,
In the present paper for the purpose of the encryption and decryption using elliptic curves it is sufficient to consider the equation of the form $y^2 = x^3 + a*x + b$. For the given values of a and b the plot consists of positive and negative values of y for each value of x. Thus this curve is symmetric about the x-axis.

1.1 Galois field: -A field with a finite number of elements.[5]

1.2 Geometric rules of Addition: -Let P(x1,y1) and Q(x2,y2) be two points on the elliptic curve E. The sum R is defined as: First draw a line through P and Q, this line intersects the elliptic curve at a third point. Then the reflection of this point of intersection about x-axis is R which is the sum of the points P and Q. The same geometric interpretation also applies to two points P and –P, with the same x-coordinate. The points are joined by a vertical line, which can be viewed as also intersecting the curve at the infinity point. We therefore have P + (-P) = ∞, the identity element which is the point at infinity.

1.3 Doubling the point on the elliptic curve:-

First draw the tangent line to the elliptic curve at P which intersects the curve at a point. Then the reflection of this point about x-axis is R. As an example the addition of two points and doubling of a point are shown in the following figures 1 and 2 for the elliptic curve
$y^2 = x^3 - x$.[3]



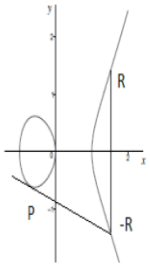


Fig 1. Geometric addition Fig 2.Geometric doubling

1.4 Identity:-P + ∞ = ∞+P = P for all E (K), where ∞ is the point at infinity.

1.5Negatives:- Let P(x, y) €E (K) then (x, y) + (x,-y) = ∞. Where (x,-y) is the negative of P denoted by –P.

1.6Point addition: - Let P(x1, y1), Q(x2, y2) € E (K) where P ≠ Q. Then P + Q = (xr, yr)
Where,
$\lambda = \{(y_q - y_p)/(x_q - y_p) \bmod p.$ If P≠Q
$X_r = (\lambda^2 - x_p - x_q) \bmod p.$
$Y_r = (\lambda (x_p - x_r) - y_p) \bmod p.$

1.7 Points Doubling:-
Let $P(x_1, y_1)$ €EK (a, b) where P ≠ −P then,
$\lambda = \{(3*X_p^2 + a) / (2*y_p)\} \bmod p$ if P =Q
$X_r = (\lambda^2 - x_p - x_q) \bmod p.$
$Y_r = (\lambda (x_p - x_r) - y_p) \bmod p.$

1.8 Point Multiplication: - Let P be any point on the elliptic curve (K). Then the operation multiplication of the point P is defined as repeated addition. kP = P + P +.....k times

1.9 Elliptic Curve Cryptography: - Elliptic Curve Cryptography (ECC) makes use of the elliptic curve in which the variables and coefficients are all restricted to elements of the finites fields. Two families of elliptic curves are used in cryptographic applications: Prime curves over *Zp* and binary curves *GF* (2^m). For a prime curve over Z_p, we use a cubic equation in which the variables and the coefficients all take on values in the set of integers from 0 through p-1 and the calculations are performed with respect to modulo p.

II. Related Work

Elliptic curve cryptography has been thoroughly researched for the last twenty years. The actual application of elliptic curve cryptography and the practical implementation of cryptosystem primitives in the real world constitute interdisciplinary research in computer science as well as in electrical engineering. Elliptic Curve Cryptography provides an excellent solution not only for the data encryption but also for the secure key transport between two communicating parties, and authentic session key establishment protocols.

III. Encryption

-If user A wants to communicate the message M to user B then all the characters of the message are coded to the points on the elliptic curve using the code table which is agreed upon by the communicating parties A and B. Then each message point is encrypted to a pair of cipher points Y1, Y2 as follows.

Pb=> Public key of B
Pm=> Plain Text
Cm=> Cipher Text
K=>Secret Key.
G => Reference point.
Pa => Public key of A.
Nb=>Private Key of B
Na => Private Key of A.

Considering the following example on the cubic curve [8]
Cm= {K, Pm + Na*Pb}

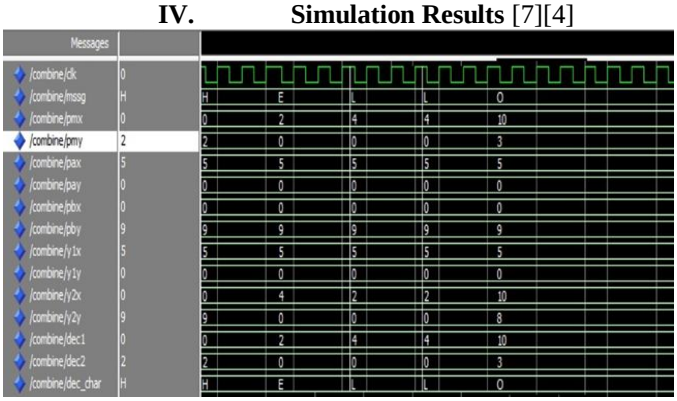
- Na = *2.*
- *Pa = Na * G = 2(10, 3) = (5, 0).*
- *Nb = 3.*
- *Pb = Nb * G= 3(10, 3) = (10, 8).*
- *K= Na * Pb =2(10, 8) = (5,0).*
- Pm = (2, 0).
- Cm={K ,Pm + Na*Pb}
  ={(5,0),(2,0)+(5,0)}
  ={(5,0),(2,0)+(5,0)}
  = {(5, 0), (4, 0)} = Y1, Y2

Decryption: - After receiving the cipher text, B converts the cipher text into the points on the elliptic curve and recognizes the points Y1 and Y2 of each character. Then the decrypted message is as follows.

- Pm = y2 – nB* y1
  = {(4, 0)-3(5, 0)}
  = {(4, 0)-{(5, 0) + (5, 0) + (5, 0)}}
  = {(4, 0)-{∞ + (5, 0)}
  = {(4, 0) - (5, 0)}
  = {(4, 0) + (5, 0)}
  = (2, 0) → Pm

Note: - (5, 0) = (5, 0 mod p**)**
= (5, 0 mod 11)
= + (5, 0)
- (5, -2) = + (5, -2 mod 11**)**
= + (5, 8)

IV. Simulation Results [7][4]



V. Synthesis Report

Number of Slices:	2089 out of 13696 15%
Number of Slice Flip Flops:	1100 out of 27392 4%
Number of 4 input LUTs:	3803 out of 27392 13%
Number of MULT18X18s:	44 out of 136 32%
Number of GCLKs:	10 out of 16 62%
# Multipliers:	15
# Adders/Subtractors:	20
# Registers:	163
# Latches:	34
# Comparators :	17

VI. Timing Summary: [6]

Minimum period: 6.329ns
(Maximum Frequency: 157.995MHz).
Minimum input arrival time before clock; 3.463ns.
Maximum output required time after clock; 5.742ns

VII. Conclusion:-

Elliptic Curve Cryptography provides greater security and more efficient performance than the first generation public key techniques (RSA and Diffie-Hellman) now in use. As vendors look to upgrade their systems they should seriously consider the elliptic curve alternative for the computational and bandwidth advantages they offer at comparable security.

In the encryption algorithm proposed here the communicating parties agree upon to use an elliptic curve and a point C on the elliptic curve. The security of the Elliptic Curve Cryptography depends on the difficulty of finding the value of k, given kP where k is a large number and P is a random point on the elliptic curve. This is the Elliptic Curve Discrete Logarithmic Problem. The elliptic curve parameters for cryptographic schemes should be carefully chosen in order to resist all known attacks of Elliptic Curve Discrete Logarithmic Problem (ECDLP).

The straightforward use of public key encryption provides confidentiality but not the authentication. Each communicating party publishes a specific public key for the communication with a specific communicator. With this the receiver is assured that the cipher was constructed by the sender only because the sender uses receiver's general public keys, receiver's specific public key published for the sender alone and sender's private key for constructing the cipher. This ensures that sender has "digitally signed" the message by using the specific public key published for him alone by the receiver. Hence, the cipher has achieved the qualities confidentiality, authentication and non-repudiation. Moreover, each message point is encrypted as a pair of points on the elliptic curve. Here a random number is used in the encryption of each message point and is different for encryption of different message points. That is why the same characters in the message space are encrypted to different characters in the cipher space. In this work on FPGA the implementation on VERTEXxcv1000 architecture consumes less area and operates at a higher frequency compared to [6] .The difference between characters of the plain text is not the same as difference between the characters of the cipher text. Due to this the linear cryptanalysis is highly difficult. In addition to this each character of the message is coded to the point on the elliptic curve using the code table which is agreed upon by the communicating parties and each message point is encrypted to a pair of points on the elliptic curve. Hence, the method of encryption proposed here provides sufficient security against cryptanalysis at relatively low computational overhead.

References

[1] HDL PROGRAMMING, VHDL and VERILOG by"Nazeih M. Botros".
[2] HDL PROGRAMMING by "J Bhasker".
[3] Cryptography and Network Security by "William Stallings".
[4] Prof.Rahila Bilal and Dr.M.Rajaram "International Journal of Computer Applications – Volume 8-No 3 October 2010.
[5] D.Saravana kumar and CH Suneetha,"international journal of distributed and parallel systems (IJDPS)"Vol 3,no 1,jan 2013.
[6] Nele Mentens and JoVliegen "A Compact FPGA Based Architecture for Elliptical Curve Cryptography over Prime Fields".
[7] Yingjie qu and Zhengming hu "Research and Design of Elliptic Curve Cryptography "(2010 IEEE).
[8] Padma Bh and Chandravathi "International Journal of Computer Science and Engineering' Vol 2 - 2010