ISSN: 2277-3754
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 1, Issue 1, January 2012

# Point Multiplication Methods for Elliptic curve Cryptography

Alka Sawlikar, Astt.Prof, Electronics Department RCERT, Chandrapur
alkaprasad.sawlikar@gmail.com

***Abstract*—: Elliptic curve based cryptosystem is an efficient public key cryptosystem, which is more suitable for limited environments. The performance of elliptic curve cryptosystem heavily depends on an operation called point multiplication. This paper gives an introduction to elliptic curve cryptography (ECC) and presents the comparative study of methods for point multiplication operation. and moreover in this paper I have examined that the NAF method is efficient than the binary method as this improves the speed of the scalar multiplication. This paper also discusses the implementation of ECC on two finite fields, prime field and binary field.***

*Index Terms*— **Elliptic curve cryptography, ECC Foundation, Scalar multiplication method NAF.**

## I. INTRODUCTION

Elliptic curve cryptography was introduced by Victor Miller and Neal Koblitz [1] in 1985.The popularity of elliptic curve cryptography is due to the determination that is based on a harder mathematical problem than other cryptosystems. It is gaining wide acceptance as an alternative to the conventional public key cryptosystem such as RSA[2],DSA [3].ECC offers the same level of security with smaller key size and it leads to the better performance in limited environments like cellular phones, PDA, sensor networking, etc. For example, ECC with a key size of 160 bits provides the same level of security as RSA with a key size of 1024 bits. Another advantage that makes ECC more attractive is the possibility of optimizing the arithmetic operations in the underlying field [4]. In elliptic curve cryptosystem, main operations such as key agreement, signature generation, signing and verification involve scalar multiplication. The speed of scalar multiplication plays an important role in the efficiency of whole system. Fast multiplication is very essential in some environments such as constrained devices, central servers, where large number of key agreements, signature generations and verification occurs. The mathematical operations of ECC is defined over the elliptic curve $y^2 = x^3 + ax + b$, where $4a^3+ 27b^2 \neq 0$ [5]. Each value of the 'a' and 'b' gives a different elliptic curve. The public key is a point in the curve and the private key is a random number. The public key is obtained by multiplying the private key with the generator point G in the curve. The generator point G, the curve parameters 'a' and 'b', together with few more constants constitutes the domain parameter of ECC.

## II. ELIPTIC CURVE CRYPTOGRAPHY FOUNDATION

ECC has a very unique mathematical structure that enables the process of taking any two points on a specific curve, of adding the two points and getting as a result another point on the same curve. This special feature is advantageous for cryptography due to the inherent difficulty of determining which original two points were used to get the new point. The choice of various parameters in the equation will set the level difficulty exponentially as compared to the key length. Breaking encryption with ECC must use very advanced mathematics. However, ECC itself only require small increase in the number of bits in its keys in order to achieve a higher security. ECC consists of a few basic operations and rules that define how addition, subtraction, multiplication, and doubling are performed. ECC point addition is described in figure1 and is defined as finding the line between two points, in this case P and Q. The result is a third point R. Point multiplication kP is accomplished by performing multiple additions. Thus, the elliptic curve discrete logarithm is the following given public key kP, find the private key k. The work of [6] gives a comprehensive explanation about elliptic curve mathematical foundation and its implementation.

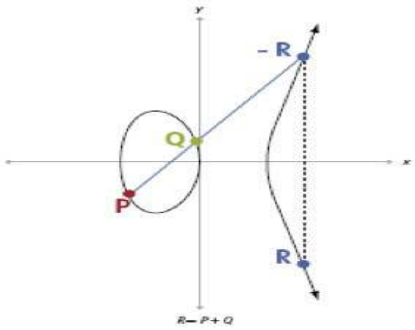


**Fig.1. ECC Point Addition**

## III. FINITE FIELDS

To make operations on elliptic curve accurate and more efficient, the curve cryptography is defined over two finite fields.

- Prime field Fp
- Binary field $F2^m$

The field is chosen with finitely large number of points suited for cryptographic operations [5].

ISSN: 2277-3754
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 1, Issue 1, January 2012

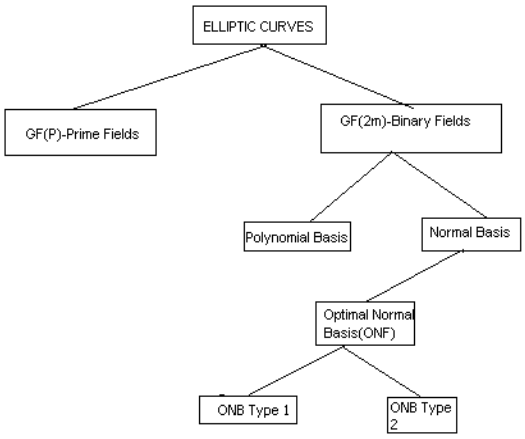


**Fig.2 Taxonomy o f Elliptic Curves**

## IV. EC ON PRIME FIELD

The equation of the elliptic curve on a prime field Fp is $y^2 \bmod p = x^3 + ax + b \bmod p$, where $4a^3 + 27b^2 \bmod p \neq 0$. Here the elements of the finite field are integers between 0 and p – 1. All the operations such as addition, substation, division, multiplication involves integers between 0 and p – 1. The prime number p is chosen such that there is finitely large number of points on the elliptic curve to make the cryptosystem secure.

**Point Addition**

Consider two distinct points J and K such that
$J = (x_J, y_J)$ and $K = (x_K, y_K)$
Let $L = J + K$ where $L = (x_L, y_L)$, then
$x_L = s^2 - xJ - x_K \bmod p$
$y_L = -y_J + s(x_J - x_L) \bmod p$
$s = (y_J - y_K) / (x_J - x_K) \bmod p$, s is the slope of the line through J and K.

**Point Subtraction**

Consider two distinct points J and K such that
$J = (x_J, y_J)$ and $K = (x_K, y_K)$
Then $J - K = J + (-K)$ where $-K = (x_k, -y_k \bmod p)$
Point subtraction is used in certain implementation of point multiplication such as NAF.

**Point Doubling**

Consider a point J such that $J = (x_J, y_J)$,
Where $y_J \neq 0$
Let $L = 2J$ where $L = (x,y)$Then
$x_L = s^2 - 2x_J \bmod p$
$y_L = -y_J + s(x_J - x_L) \bmod p$
$s = (3x_J^2 + a) / (2y_J) \bmod p$

## V. EC ON BINARY FIELD F2 $^M$

The equation of the elliptic curve on a binary field F2 m is $y^2 + xy = x^3 + ax^2 + b$, where $b \neq 0$. Here the elements of the finite field are integers of length at most m bits. These numbers can be considered as a binary polynomial of degree m–1. In binary polynomial the coefficients can only be 0 or 1. All the operation such as addition, substation, division, multiplication involves polynomials of degree m – 1 or lesser. The m is chosen such that there is finitely large number of points on the elliptic curve to make the cryptosystem secure.

## VI. POINT MULTIPLICATION

In point multiplication a point P on the elliptic curve is multiplied with a scalar k using elliptic curve equation to obtain another point Q on the same elliptic curve i.e. KP=Q. Point multiplication is achieved by two basic Elliptic curve operations [5]

•Point addition, adding two points J and K to obtain another point L i.e., L = J + K.

• Point doubling, adding a point J to itself to obtain another point L i.e. L = 2J.

Here is a simple example of point multiplication. Let P be a point on an elliptic curve. Let k be a scalar that is multiplied with the point P to obtain another point Q on the curve i.e. to find Q = kP.If k = 23 then kP = 23.P = 2(2(2(2P) + P) + P) + P.Thus point multiplication uses point addition and point doubling repeatedly to find the result. The above method is called 'double and add' method for point multiplication. There are other efficient methods for point multiplication such as NAF (Non – Adjacent Form). In the following sections we review some methods for computing scalar multiplication.

## VII. BINARY METHOD

For computing kp, the simplest method is binary method [7]. The integer k is represented as
$k = k_{n-1} 2^{n-1} + k_{n-2} 2^{n-2} + \ldots\ldots + k_1 + k_0$
Where ki € {0, 1}, n = 0, 1, 2… n -1.
That is
$k = \Sigma k_j 2^j$, where $k_j$ € {0, 1}.

This method is called binary method [8] which scans the bits of k either from left-to-right or right-to-left. The binary method for the computation of kP is given in the following:

Algorithm 1: Binary method
Input: Binary representation of k and point P
$k = (kn\text{-}1 \ldots . k_1 k_0)_2$
Output: kP
1. R ←P
2. For i = n-2 to 0 do
2.1 R←2R (Doubling)
2.2 If ki =1 then
R = R + P (Addition)
2.3 i ← i −1
3. Return R

The cost of multiplication depends on the length of the binary representation of k and the number of 1s in this representation. If the representation (kn-1….k1k0)2 has kn-1 # 0 then the number of doubling operation is (n - 1) and the number of addition operations is one less than the number of non-zero digits in (kn-1….k1k0)2. The number of non-zero digits is called the Hamming weight of scalar representation. In an average, binary method requires n -1 doublings and n -1/ 2 additions .For example, the integer k = 729 and the binary representation is$(1011011001)_2$, computation of 729P requires 9 doublings and 5 additions. Whenever the bit is 1,

ISSN: 2277-3754
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 1, Issue 1, January 2012

two elliptic curve arithmetic operations such as ECDBL and ECADD will be made and if it is 0, only one operation, ECDBL is required. So if we reduce the number of 1s in the scalar representation or hamming weight, we could speed up the above computation.

## VIII. ADDITION SUBTRACTION METHOD

Another method for scalar multiplication was proposed by Booth [9], called signed binary method. The property of this representation is that, of any two consecutive digits, at most one is non-zero. Before discussing this method we first discuss about non-adjacent form (NAF) that is the basis of this method. An improved method for computing kP can be obtained from the following facts: Every integer $k$ has a unique representation of the form

$k = \Sigma kj\ 2$ ,

Where each kj € {-1, 0, 1}.such that no two consecutive digit are nonzero. This representation is known as non-adjacent form (NAF).

The expected weight of a NAF of length $n$ is n/3 [10].A procedure for computing NAF (k) is described in the algorithm 2.

Algorithm 2: Computation of NAF of an integer
Input: Positive integer $k$
Output: NAF ($k$)
1. i ← 0
2. While $k \geq 1$ do
2.1 If $k$ is odd then: $k$i ← 2 - ($k$ mod 4),
$k$ ←$k$ - $k$i
2.2 Else: $k$i ← 0
2.3 $k$← $k$/2, i← i +1.
3. Return ($k$i-1, $k$i-2… $k$1, $k$0).

The average hamming weight of signed binary Representation is n/3 and it has the lower hamming weight than the binary representation. The binary method is revised accordingly and the new algorithm is called addition–subtraction method [11] given in Algorithm 3.

Algorithm 3: Computation of NAF of an integer
Input: NAF of a Positive integer $k$ and P
Output: kP
1. R ← P
2. For i= n −2 to 0 do
2.1 R←2R
2.2 if $k$i = 1 then R←R+P
2.3 if $k$i = −1 then R←R-P
2.4 i ← i −1
3. Return R

The addition-subtraction method is analogue of the binary method, performs an addition or subtraction depending on the sign of digit of non-adjacent form (NAF) of , scanned from left to right This algorithm performs n-1 doublings and n-1/3 additions in an average.

## IX. COMPARISON

We compare binary method with the NAF method of point multiplication. In an average, binary method requires n -1 doublings and n -1/ 2 additions where n is the bit length. The addition-subtraction algorithm performs n-1 doublings and n-1/3 additions in an average. For example, the binary representation of 63 is (111111)2, the hamming weight is 6 and NAF of 63 is NAF (63) = (100000 −1), the hamming weight is only 2. Here the hamming weight of k is reduced from 6 to 2, which improve the speed of the scalar multiplication. So, number of addition also reduces in the NAF method. However, the rate of change is much faster in addition than the doubling.

## X. CONCLUSION AND FUTURE WORK

Elliptic curve cryptosystem becomes to be the cryptosystem for the future. One way to improve the performance of such cryptosystem is to use an efficient method for point multiplication which is the most time consuming operation. In this Paper I have presented a study of the scalar multiplication methods to be used in elliptic curve cryptography. The addition-subtraction method decreases number of point additions that speed up the computation. Therefore in the future some efficient methods for point multiplication can be used to speed up the computation. So if we implement ECC with projective co-ordinate rather than affine co-ordinate system, this system may be fast.

## REFERENCES

[1] N. Koblitz, Elliptic curve cryptosystem, Mathematics of Computation 48 (1987) 203–209.

[2] R.L. Rivest, A. Shamir, L.M. Adleman, A Method for obtaining digital signatures and public key cryptosystem, Communications of the ACM 21 (1978) 120–126.

[3] T. ElGamal, Public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions on InformationTheory 31 (4) (1985) 469–472.

[4] E. Al-Daoud, R, mahmod, Md. Rushdan, A. Kilicman (2002), “A new addition formula for Elliptic curve over GF (2n)”, IEEE Transactions on Computers, vol. 51, no. 8, pp. 972-975, Aug.

[5] Darrel Hankerson, Alfred Menezes, and Scott Vanstone. Guide to Elliptic Curve Cryptography. Springer-Verlag New York, Inc., 2004.

[6] J. Lopez, R. Dahab (2000), “An overview of elliptic curve cryptography”, Technical report, IC-00-10, May 22. Available at http:// www.dcc.unicamp.br/ic-main/public-cation - e.html.

[7] Standard Specifications for Public Key Cryptography, IEEE Standard 1363, 2000.

[8] A.D. Booth, A signed binary multiplication technique, Journal of Applied Mathematics 4 (2) (1951) 236–240.

[9] J. Solinas (2000), “Efficient arithmetic on Koblitz curves”, Designs, Codes and Cryptography, vol. 19, pp. 195-249.

ISSN: 2277-3754
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 1, Issue 1, January 2012

[10] F. Morain, J. Olives, Speeding up the computations on an elliptic curve using addition–subtraction chains, RAIRO Theoretical Informatics and Applications 24 (1990) 531–543.

[11] Anoop MS, "Elliptic curve Cryptography", available at http://security.ittoolbox.com/research/ellipticcurvecryptography,5 Jan 2007.