Applied Mathematical Sciences, Vol. 9, 2015, no. 45, 2235 - 2243
HIKARI Ltd, www.m-hikari.com
http://dx.doi.org/10.12988/ams.2015.53204

Improved Elliptic Curve Arithmetic over GF(p) Using Different Projective Coordinate System

M. Lavanya

Dept. of Instrumentation Engineering
MIT campus, Anna University Chennai, India

V. Natarajan

Dept. of Instrumentation Engineering
MIT campus, Anna University Chennai, India

Abstract

Elliptic curve cryptography is a public key cryptography which contains two different keys for encryption and decryption. The points on elliptic curves are represented in affine coordinates, the arithmetic on elliptic curves contain the expensive inverse operation in modular arithmetic, which increases the computation time, memory etc. Hence to avoid the inverse operation the points are represented in projective coordinate system. In this paper the different projective coordinates for different elliptic curves are derived and the number of operations for point addition in EC arithmetic are compared.

Keywords: Elliptic curves, Projective coordinates, Affine coordinates, Point addition,Point doubling

1 Introduction

Elliptic curves finds application in wide areas of mathematics, they are applied in various fields from cryptography to mathematical physics. Elliptic curves

with points in finite field are called finite groups. Elliptic curve cryptography (ECC) is a public key cryptographic system. It is based on the algebraic structure of elliptic curves over finite fields. Elliptic curve cryptography was proposed by Miller and Koblitz in 1980's. Elliptic curve cryptosystem is based on Galois Field (GF). GF can be defined over a prime field (i.e. GF (p)) or over polynomial field (i.e. GF (2^m)). Compared to the traditional RSA algorithm the key sizes are very less in ECC. A 160 bit ECC provides same level of security as 1024 bit RSA algorithm. Hence ECC is suitable for energy constrained environments like Wireless sensor networks, RFID etc. ECC is based on difficulty of solving the elliptic curve discrete logarithm problem. [2] Elliptic curves are represented by Weierstrass equation given by

$$E: y^2 + a_1 x y + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \quad (1)$$

where $a_1, a_2, a_3, a_4, a_6 \in$ K(the finite field) , where is the discriminant of E and is defined as follows:

$$\Delta = -d_2 d_8 - 8d_4 - 27d_6 + 9d_2 d_4 d_6 \quad (2)$$
$$d_2 = a_1 + 4a_2$$
$$d_4 = 2a_4 + a_1 a_3$$
$$d_6 = a_3 + 4a_6$$
$$d_8 = a_1 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3 - a_4$$

The Weierstrass equation is simplified with different values of x and y. The simplified equations are used for cryptographic purpose. The two simplified forms of the equation are

$$y^2 = x^3 + ax + b \quad \cdots (3) \quad \text{and} \quad y^2 + xy = x^3 + ax^2 + b \quad \cdots (4)$$

The values of x and y are

$$(x,y) = \left\{ x - \frac{a_2}{3}, y - \frac{a_1 x + a_3}{2} \right\} \cdot for\, 3 \quad \text{and} \quad (x,y) = \left\{ a_1^2 x + \frac{a_3}{a_1}, a_1^3 y + \frac{a_1^2 a_4 + a_3^2}{a_1^3} \right\} \cdot for\, 4$$

Curve (3) is used for implementations over prime field (Fp) and curve (4) is used for implementations using binary fields ($F2^m$). The prime curves are suitable for software applications and binary curves are suitable for hardware applications.

2 Preliminaries

2.*1) Point representation of Elliptic curves*

Elliptic curves are represented by the points, x and y. These curves are generally non singular curves. An extra point is tossed on an elliptic curve; the point at infinity O. So the elliptic curve equation is set as

$$E=\{(x,y): y^2=x^3+ax+b\}\cup\{O\}\ldots(5)$$

Group law on elliptic curves [5]

The addition function on E has the following group properties

$$1.\ P+O=p=O+P \quad for\ all\ P\epsilon E$$
$$2.\ P+(-P)=O \quad for\ all\ P\epsilon E$$
$$3.\ P+(Q+R)=(P+Q)+R \quad forallP,Q,R\epsilon E$$
$$4.\ P+Q=Q+P \quad for\ all\ P,Q\ \epsilon E$$

Normally the x and y coordinate representation is called as the affine coordinate system. The algebraic equations for elliptic curve arithmetic like point addition and point doubling (discussed in next section) contain inverse operation. The inverse operation is very expensive in terms of computation time and memory. Hence affine coordinate representation is time consuming, alternate representation is using the projective coordinate system. A projective plane p^2 is defined to be the set of equivalence classes of triples (x, y, z) not all zeros. Here the points (x_1, y_1, z_1) and (x_2, y_2, z_2) are said to be equivalent if there exists $\lambda \in GF(2^n)$, $\lambda \neq 0$ such that $x_1=\lambda x_2$, $y_1=\lambda^2 y_2$ and $z_1=\lambda z_2$. Each equivalence class is called as projective point. Hence (x, y) pair is represented as(x, y, z) and the relationship between them is

$$(x,y,z)=\lambda^c x,\ \lambda^d y,\ \lambda z \quad \ldots(6)$$
$$(x,y)=(X/Z^c, Y/Z^d) \quad \ldots(7)$$
$$\lambda\neq 0$$

There are number of types of coordinates when c and d are set to different values [2]. The three projective coordinate system currently used for representing elliptic curves are the following, they are formed by substituting different values for c and d of equation 7

If c=d=1, called standard projective coordinates

$$(x,y)=(X/Z, Y/Z)$$

If c=2 and d=3, called Jacobian coordinates

$$(x,y)=(X/Z^2, Y/Z^3)$$

If c=1 and d=2 , called Lopez Dahab system

$$(x,y)=(X/Z, Y/Z^2)$$

2.2) Elliptic curve arithmetic [2]

There are three arithmetic operations on elliptic curves, point addition, point doubling and point multiplication.

Point addition(fig 1)

Let P and Q be any two points on the elliptic curve addition of two points follows the following steps

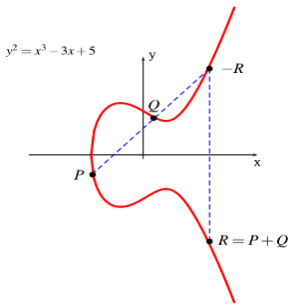

Fig.1 Point addition source :www.embedded.com

Step 1: Draw a line through the points P& Q
Step 2: The line intersects at another point R on the curve
Step 3: Draw a vertical line through R
Step 4: P+Q is where the line hits curve in another point

Point doubling (p+p)

Adding a point to itself is called point doubling i.e., Draw a tangent line to E at P
Step 1: Take the third intersection point R and reflect it across the x-axis and call it the point 2P (P+P)

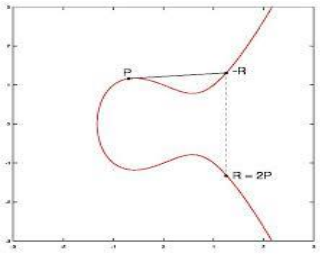

Fig 2. Point Doubling
source: www.cryptocode.com

Point Multiplication

Point multiplication is also called scalar multiplication, multiplying a point P with a scalar value. Point multiplication is performed using repeated addition and point doubling, called as double and add method.
Montgomery Modular Multiplication is an efficient method for performing modular multiplication as it avoids trial division by modulus [7]

3 Mathematical Derivations

There are different forms of elliptic curves like Jacobian curve , Hessian curves, Edward curves, Doubling- oriented Doche-Icart-kohel curves, Tripling oriented Doche-Icart-kohel curves and Montgomery curves[3]. There are different twisted curves also. In this paper the arithmetic operations of the above mentioned curves are studied and the equations are derived for different coordinate system. The mathematical results are compared to identify the best curve and coordinate system for optimized operation of the elliptic curve.

3.1 Hessian Curve

The equation for the hessian curve is given by [6]

$$H_d : x^3 + y^3 + 1 = dxy \quad where d^3 - 1 \neq 0 \ \wedge \ d^3 \neq 27 \ldots\ldots (8)$$

Point addition in affine coordinates

Let P(x_1, y_1) Q (x_2, y_2) be two points, the coordinates of P+Q is given by

$$x_3 = \frac{y_1^2 x_2 - y_2^2 x_1}{x_2 y_2 - x - 1 y_1} \ldots (9) \quad y_3 = \frac{x_1^2 y_2 - x_2^2 y_1}{x_2 y_2 - x_1 y_1} \ldots (10)$$

Projective coordinates for Hessian curve

(i) Standard coordinates $(x,y)=(X/Z,Y/Z)$
The curve equation is

$$X^3+Y^3+Z^3c=dXYZ$$

Substituting the standard projective coordinates in equation 9 and 10

$$x_3=\frac{Y_1^2X_2Z_2-Y_2^2X_1Z_1}{Z_1^2X_2Y_2-Z_2^2X_1Y_1} \qquad y_3=\frac{X_1^2Y_2Z_2-X_2^2Y_1Z_1}{X_2Y_2Z-1^2-X_1Y_1Z_1^2}$$

$$z_3=X_2Y_2Z_1^2-X_1Y_1Z_2^2$$

$$X_3=Y_1^2X_2Z_2-X_1Y_1Z_2^2,\ Y_3=X_1^2Y_2Z_2-X_2^2Y_1Z_1,\ Z_3=1$$

$$let\ \partial_1=Y_1^2,\ \partial_2=y_2^2,\ \partial_3=X_1^2,\ \partial_4=X_2^2,\ \partial_5=X_2Z_2,$$
$$\partial_6=X_1Z_1,\partial_7=Y_2Z_2,\ \partial_8=Y_1Z_1$$

then the values of X_3 and Y_3 becomes

$$X_3=\partial_1\partial_5-\partial_2\partial_6..(11),\ Y_3=\partial_3\partial_6-\partial_4\partial_8\ldots(12)$$

Hence the equations 11 and 12 eliminates inverse operation and contains 8 parallel multiplications and 4 serial multiplications and two serial subtractions. Similarly the Jacobian and Lopez coordinate systems are substituted in the equations 9 and 10. The obtained results are tabulated in table 1. PM-parallel multiplication, SM -serial multiplication, PA-parallel addition, SA- serial Addition, SS-serial subtraction

Table 1. Comparison of the coordinate systems for Hessian Curve

Curve	Coordinate	PM	SM	PA	SA	SS	TOTAL
Hessian	Jacobian	10	14			4	28
	Lopez	8	10			3	21

3.2 Edwards curves

The Edward curve equation is given by [1]

$$E_d:x^2+y^2=c^2(1+dx^2y^2)\ldots(13)$$

the values of x_3 and y_3 (point addition in affine coordinate system) are

$$x_3=\frac{x_1y_2+y_1x_2}{1+dx_1x_2y_1y_2}\ldots(14)\quad y_3=\frac{y_1y_2-x_1x_2}{1-dx_1x_2y_1y_2}\ldots(15)$$

Projective coordinates for Edward curves

(i) Standard projective coordinates $(x,y)=(X/Z,Y/Z)$
Substituting in the equation 18 and 19,

$$x_3=\frac{(X_1Y_2+Y_1X_2)Z_1Z_2}{Z_1^2Z_2^2+dX_1X_2Y_1Y_2} \qquad y_3=\frac{Z_1Z_2(Y_1Y_2-X_1X_2)}{Z_1^2Z_2^2-dX_1Y_1X_2Y_2}$$
$$z_3=Z_1^4Z_2^4-(dX_1X_2Y_1Y_2)^2$$

now the values of X_3 Y_3 and Z_3 are follows

$$X_3=(X_1Y_2+Y_1X_2)(Z_1^2Z_2^2-dX_1X_2Y_1Y_2),Y_3=(Y_1Y_2-X_1X_2)(Z_1^2Z_2^2+dX_1X_2Y_1Y_2)$$

$$\partial_1=Z_1^2Z_2^2,\partial_2=X_1Y_2,\partial_3=Y_1X_2,\partial_4=Y_1Y_2\partial_5=X_1X_2\partial_6=d\partial_5\partial_4$$
$$NowX_3=(\partial_2-\partial_3)(\partial_1-\partial_6)\ldots(16),Y_3=(\partial_4-\partial_5)(\partial_1+\partial_6)\ldots(17)$$

From the equations 16 and 17, it is inferred that there are 6 parallel multiplications, 4 serial multiplications, one serial addition and one serial subtraction. Similarly the jacobian and Lopez coordinates are substituted in the equations 14 and 15 and the results ate tabulates in table 2.

Table 2. Comparison of the Coordinates for Edward curves

Curve	Coordinate	PM	SM	PA	SA	SS	TOTAL
Edward	Jacobian	7	9		2	1	19
	Lopez	8	9		2	3	22

3.3 Jacobian Curve

The equation for the jacobian form of the elliptic curve is

$$y^2=x^3+ax+bmodP \quad \ldots(18)$$
$$\Delta=4a^3+27b^2modP\neq 0$$

Point addition in affine coordinates
Let $P(x_1,y_1),Q(x_2,y_2)$ be two points on the elliptic curve let $R(x_3,y_3)$ be the point P+Q

$$\lambda=\frac{y_2-y_1}{x_2-x_1} \qquad (x_3,y_3)=(\lambda^2-x_1-x_2,\lambda(x_1-x_3)-y_1)\ldots(19)$$

(i) Standard projective coordinates $(x,y)=(X/Z,Y/Z)$

On substituting the coordinates in the equation 19

$$\lambda=\frac{Y_2Z_1-Y_1Z_2}{X_2Z_1-X_1Z_2},\ Let\ A=Y_2Z_1-Y_1Z_2 \text{ and } B=X_2Z_1-X_1Z_2\ ,\ \lambda=\frac{A}{B}$$

$$y_3=\frac{A\left(B^2X_1Z_2-A^2Z_1Z_2+B^2X_1Z_1+B^2X_2Z_2\right)-B^3Z_2Y_1}{B^3Z_1Z_2}$$

$$z_3=B^3Z_1Z_2$$

now the projective coordinates are

$$X_3=x_3Z_3=A^2BZ_1Z_2-B^3X_1Z_2-B^3X_2Z_1$$

$$Y_3=A\left(B^2X_1Z_2-A^2Z_1Z_2+B^2X_1Z_1+B^2X_2Z_2\right)-B^3Z_2Y_1$$

$$Let\ \partial_1=B^2,\partial_8=A^2,\partial_2=Z_1Z_2,\partial_3=X_1Z_2\partial_4=X_2Z_1$$

$$\partial_5=X_1Z_1\partial_6=X_2Z_2,\partial_7=\partial_3\partial_1,\partial_9=\partial_8\partial_{2,}\partial_{10}=\partial_1\partial_5\partial_{11}=\partial_6\partial_1,$$

$$\partial_{12}=Y_1Z_2\partial_{13}=\partial_{12}\partial_{15,}\partial_{15}=\partial_1B$$

$$X_3=\partial_{14}-\partial_3\partial_{15}-\partial_4\partial_{15}\ldots(20)$$

$$Y_3=A\left(\partial_7\partial_8\partial_2+\partial_{10}+\partial_{11}\right)-\partial_{13}..(21)$$

from the above equationS 20 and 21 there are 10 parallel multiplications, 9 serial multiplications, 2 serial additions and 4 serial subtractions . Similarly the Jacobian and Lopez coordinates are substituted in the equation 19, and the obtained results are tabulated in the table 3

Table 3. Comparison of the Coordinates for Edward curves

Curve	Coordinate	PM	SM	PA	SA	SS	TOTAL
Standard Jacobian	Jacobian	9	8	2	2	2	23
	Lopez	10	8	2	1	4	25

4 Result Analysis / Comparison

The fig.3 takes reference of the tables 1,2,and 3 and the equations 11,12, 16,17, and 19 and gives comparison of the arithmetic's in the point addition operation of Hessian, standard Jacobi and Edward curves. The comparison is based on parallel addition (PA), parallel subtraction (PS), serial addition (SA), serial subtraction (SS), parallel multiplication (PM), serial multiplication (SM).

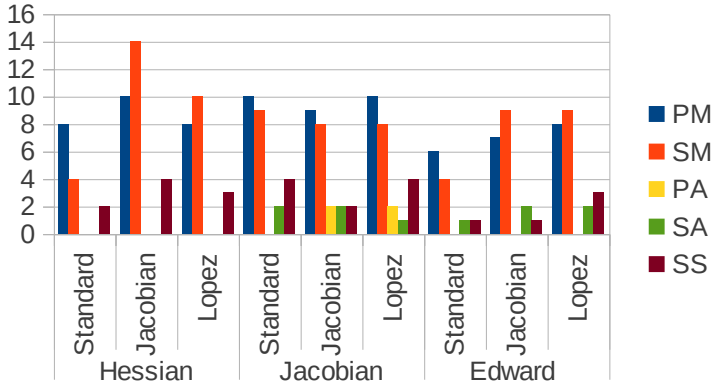

Fig 3. Comparing the arithmetic operations for various coordinate system

The total arithmetic operations are compared in the fig.4, which concludes that the number of operations are minimum in the standard coordinates of the edward curve.

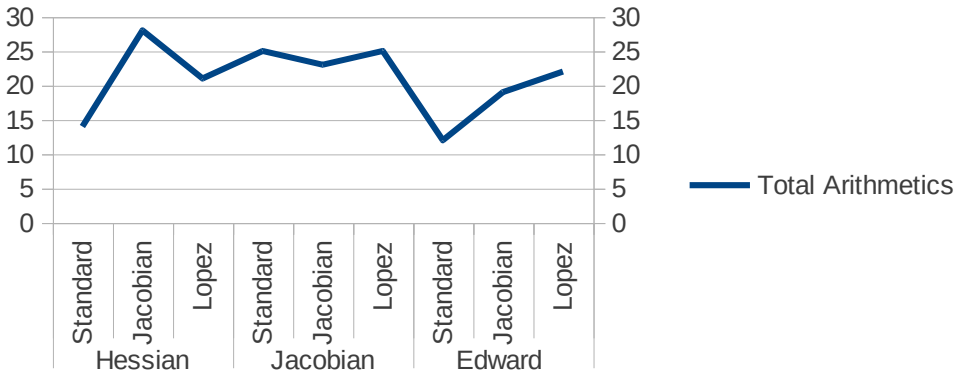

Fig.4 Comparison of total arithmetics in the curves

5 Conclusion

The above table shows the operations using the different coordinate system in elliptic curves. When the number of parallel multiplication increases then the speed of operation increases, if the number of operations gets reduced it implies that the architecture needs less number of hardware components. Depending on the application hardware or software, corresponding coordinate systems can be used in order to optimize the performance of an elliptic curve. For cryptographic purpose it would be better to use a group for which solving DLP takes time that is exponential in the order of G.

References

[1] Akira Higuchi, Naofumi Takagi "A fast addition algorithm for elliptic curve arithmetic in GF (2^n) using projective coordinates". Inf. Process. Lett. 76(3): 101-103 (2000). http://dx.doi.org/10.1016/s0020-0190(00)00134-4

[2] Darrel Hankerson, Alfred Menezes, Scott Vanstone, "Guide to Elliptic Curve Cryptography," Springer-Vl-Rlag New York, Inc., 175 I-'If th Avenue, New York, Ny 10010, USA, 2004.

[3] Kimmo U. Järvinen, Jorma Skyttä "Fast point multiplication on Koblitz curves: Parallelization method and implementations". Microprocessors and Microsystems - Embedded Hardware Design 33(2): 106-116 (2009). http://dx.doi.org/10.1016/j.micpro.2008.08.002

[4] Lo'ai Ali Tawalbeh,Qasem Abu Al-Haija "Efficient Algorithms & Architectures for Elliptic Curve Crypto-Processor Over GF(P) Using New Projective Coordinates Systems " Journal of Information Assurance and Security 6 (2011) 063-072.

[5] Menezes, A.J., P.C. Van Oorschot, and S.A. Vanstone, "Handbook of Applied Cryptography", CRC Press, Boca Raton, Florida, 1996. http://dx.doi.org/10.1201/9781439821916

[6] Reza Rezaeian Farashahi, Marc Joye "Efficient Arithmetic on Hessian Curves. Public Key Cryptography" 2010: 243-260. http://dx.doi.org/10.1007/978-3-642-13013-7_15

[7] C. D. Walter. Precise bounds for Montgomery modular multiplication and some potentially insecure RSA moduli. In B. Preneel, editor, Proceedings of Topics in Cryptology- CT-RSA 2002, number 2271 in Lecture Notes in Computer Science, pages 30-39, 2002. http://dx.doi.org/10.1007/3-540-45760-7_3

Received: December 15, 2015; Published: March 21, 2015