International Journal of Computer Networks and Communications Security

VOL. 2, NO. 12, DECEMBER 2014, 462–471
Available online at: www.ijcncs.org
ISSN 2308-9830

Improved Arithmetic on Elliptic Curves over Prime Field

NAJLAE FALAH HAMEED AL SAFFAR[1] AND MOHAMAD RUSHDAN MD SAID[2]

[1] Institute for Mathematical Research, Universiti Putra Malaysia,Malaysia

[2] Department of Mathematics, Faculty of Mathematics and Computer Science,Kufa University,Iraq

[2] Institute for Mathematical Research, Universiti Putra Malaysia,Malaysia

E-mail: [1]najlae_falah@yahoo.com, [2]mrushdan@upm.edu.my

ABSTRACT

A fast point doubling and point addition operations on an elliptic curve over prime field are proposed. This occur when we use a special coordinates system (to represent any point on elliptic curve over prime field. Using this system improved the elliptic curve point arithmetic by reducing the computation cost for point doubling and point addition operation.

Keywords: *Elliptic curve cryptosystem, point arithmetic of elliptic curve, affine coordinates, projective coordinates and Jacobian coordinates.*

1 INTRODUCTION

Elliptic curves are used for several kinds of cryptosystems, even it involved in key exchange protocols and digital signature algorithms [11], since it independently presented by Miller [20] and Koblitz [15] in the 1980s. Elliptic curve cryptography *ECC* has attracted attention in recent years due to it's dependence on the difficulty of the elliptic curve discrete logarithm problem (*ECDLP*). Since there are no known subexponential time algorithms to solve the *ECDLP*, *ECC* supplies the same level of security with a shorter key size comparing with the well known public key cryptosystems based on the discrete logarithm problem (*DLP*) and the integer factoring problem (*IFP*) over finite fields such as *RSA* [23], *DSA* [18] and ElGamal [9]. Because of this singularity (requires a shorter key sizes are translated to less power and storage requirements, and reduced computing time comparing with another public cryptosystems) using *ECC* is recommended in resource constrained environments, such as mobile phones, *PDAs* and smart cards [3] [12]. Towards this end, considerable research has been performed to accelerate and improve this system, by focusing on the most important part of *ECC* which is elliptic curve scalar multiplication, denoted by kP where P is a point on an elliptic curve E and k considered as a secret scalar. This basically means adding a point P on elliptic curve E, k times. Reducing the total computation time for this operation was the main focus for many researchers such as [8] [21].

The structure of the elliptic curve scalar multiplication operation involves three computational levels: field arithmetic, point arithmetic and scalar arithmetic [10] [19]. In this work, we will focus on developments at the elliptic curve point arithmetic level to accelerate the elliptic curve scalar multiplication.

The computation of the elliptic curve point arithmetic involves the effective implementation of point doubling and point addition operations. An elliptic curve can be represented using several coordinates systems. For each such system, the speed of point doubling and point addition operations is different. This means a good choice of coordinates system is an important factor for speeding up the elliptic curve scalar multiplication.

Due to the expensive cost of the field multiplication inversion involves in both point doubling and point addition operation with the arithmetic of the affine coordinates (x, y), the

projective coordinates systems were proposed. This means projective coordinates system offer an alternative method for efficient performance of the arithmetic of elliptic curve [24].

In 1986, Chudnovsky and Chudnovsky [6] used the Jacobian coordinates system to represent an affine point (x,y) as the triplet (X,Y,Z), where $x=\frac{X}{Z^2}$ and $y=\frac{Y}{Z^3}$. In 1993 Agnew et al. [1] the homogeneous projective coordinates systems was introduced, where a projective point (X,Y,Z) corresponds to the affine point $(x=\frac{X}{Z},y=\frac{Y}{Z})$, whereas at the end of nineties LD coordinates system [25] was proposed, which an affine point $(x=\frac{X}{Z},y=\frac{Y}{Z^2})$ is presented as (X,Y,Z) using elliptic curve over binary field. Significant effort to optimize the LD coordinates system performance has been carried out since it was introduced such as [16] [2] [17].

In 2007, Kim et al. [13] introduced the $4-$ dimensional coordinates system, where the point (X,Y,Z,T^2) corresponds to the affine point $(x=\frac{X}{Z},y=\frac{Y}{T})$, with $T=Z$, on an elliptic curve over finite fields of characteristic three. In the same year, the same technique introduced by Kim and Kim [14] but on an elliptic curves over binary fields.

In this work, we introduce a modification on Jacobian coordinates, which gives faster point doubling and point addition operation than affine, projective, and Jacobian coordinates. Each point is presented by the $4-$ dimensional coordinates $(X=xT,Y=yZ^3,Z,T=Z^2)$ corresponding to the affine point on a curve $y^2=x^3+ax+b$ over F_p. The basic technique of this work is to rewrite the point doubling and point addition operation on the elliptic curve with less costly field multiplication inversion, multiplication and squaring operation. Due to the discussion on the computation time for the point doubling and point addition operation on an elliptic curve, we will neglect the point addition, subtraction and multiplication by small constant in the prime field F_p since they are much faster than field multiplication inversion and field multiplication operation. Throughout this work, I, M and S in italics, denote field multiplication inversion, multiplication and squaring operation respectively.

2 PRELIMINARIES

In this section, we will give a brief review of the materials which is used in the current work. The interested reader may find additional information in [3] [24]. Also, for background on finite field we refer [5].

An elliptic curve E over an arbitrary field F denoted by $E(F)$ is given by the Weierstrass equation [24] [7] as follows:

$$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6 \quad (1)$$

where $a_1,a_2,a_3,a_4,a_6\in F,$ and $\Delta\neq 0,$ where Δ denoted to the discriminant of E.

The set of points on E that solved the equation (1), together with a special point named point at infinity (denoted by O_∞) which is the identity for the group law, form an abelian group. This abelian group is used for the implementation of ECC.

Elliptic curve can be defined over finite fields, such as binary field or prime field. Furthermore, we can define elliptic curve over field of real number but only for algebraic geometry manner.

Over the prime field F_p, the equation (1) simplifies as follows:

$$y^2=x^3+ax+b \quad (2)$$

where $a,b\in F_p$ and $\Delta=4a^3+27b^2\neq 0$.

Over the binary field F_{2^m}, equation (1) can be simplified to:

$$y^2+xy=x^3+ax^2+b \quad (3)$$

where $a,b\in F_{2^m}$ and $\Delta=b\neq 0$.

Over the field of real number R, the elliptic curve is defined on equation (2) but with $a,b\in R$ and $\Delta=4a^3+27b^2\neq 0$.

Theorem 2.1 *[24]*

Let $P,Q\in E$, L the line connecting P and Q (tangent line to E if $P=Q$), and M the third point of intersection L with E. Let L' be the line connecting M and O_∞. Then the point $P+Q$ is the third point on E, such that L' intersects E at M, O_∞ and $P+Q$.

The set $E(F)$ of rational points on an elliptic curve E defined over a field F forms an abelian additive group. The additive operation is defined by the tangent and secant law. **Figure** 1 illustrate this operation geometrically [7] on special elliptic curve over the real field, as an example if the target is to

compute $P+Q$ for P and Q are points on E, then we have to draw a line though P and Q which intersects with the E at the third point M on E, the intersection between the vertical line and the E is $P+Q$.

Theorem 2.2 *[24]*
If a line L intersects E at the points Q,P,M (not necessarily distinct), then $Q+P+M=O_\infty$.

This means, when we need to find $Q+P$ we have to find M and then apply the negation formula for M.

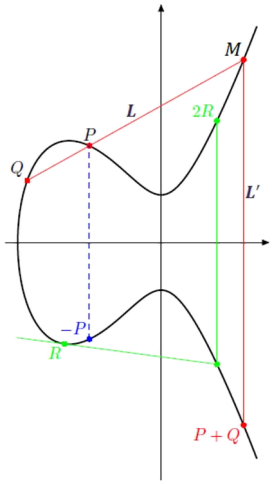

Fig. 1. Elliptic Curve Point Addition

The focus of this work will be with elliptic curve E defined over field of prime number F_p which is denoted by $E(F_p)$ given by equation (2).

In the rest of this section, the formulas for the inverse point, point doubling and point addition in the affine coordinates system are presented.

Theorem 2.3 *[24]*
Let $P_0=(x_0,y_0)$ be point in $E(F_p)$. Then $-P_0=(x_0,-y_0)$.

Theorem 2.4 *[24]*
Let $P_1=(x_1,y_1)$ and $P_2=(x_2,y_2)$ be points in $E(F_p)$.

1. If $x_1=x_2$. Then $P_1+P_2=O_\infty$.
2. If $x_1=x_2$ but $P_1\neq -P_2$. Then $P_1+P_2=(x',y')$ where $x'=m^2-x_1-x_2,\ y'=m(x_1-x')-y_1$ and $m=\frac{3x_1^2+a}{2y_1}$.
3. If $x_1\neq x_2$. Then $P_1+P_2=(x_3,y_3)$ where $x_3=m^2-x_1-x_2$, $y_3=m(x_1-x_3)-y_1)$ and $m=\frac{y_2-y_1}{x_2-x_1}$.

Theorem 2.4 2.4 is the formula for point doubling operation, while theorem 2.4 2.4 represented the formula for point addition operation. So, the computation time for the point doubling operation is $1I+2M+2S$ and $1I+2M+1S$ for the point addition operation in affine coordinates system.

To achieve efficiency, field multiplication inversion in group operations should be avoided, projective coordinates systems have ensured this requirement. There are different types of projective coordinates systems having the advantages in efficiency, such as ordinary projective coordinates system where $(x,y)=(\frac{X}{Z},\frac{Y}{Z})$, Jacobian coordinates system where $(x,y)=(\frac{X}{Z^2},\frac{Y}{Z^3})$, LD projective coordinates system where $(x,y)=(\frac{X}{Z},\frac{Y}{Z^2})$ and $4-$dimensional coordinates system (X,Y,Z,T) where $(x,y)=(\frac{X}{T},\frac{Y}{Z^3})$ and $T=Z^2$.

In the next section, we will give a brief review of the formulas for point doubling and point addition operation on elliptic curve over prime field but with various coordinates systems.

3 COORDINATES SYSTEMS

To avoid the field multiplication inversion in point doubling and point addition operation in affine coordinates system which is one $I=1$, points on elliptic curve are usually substituted with projective coordinates system.

In homogeneous coordinates system, a projective point (X,Y,Z) with $Z\neq 0$, corresponds to affine point $(\frac{X}{Z},\frac{Y}{Z})$. In this case the equation of elliptic curve will be:

$$Y^2Z=X^3+aXZ^2+bZ^3 \qquad (4)$$

In Jacobian coordinates system, a point (x,y) in affine coordinates system is recovered as $(\frac{X}{Z^2},\frac{Y}{Z^3})$ with $Z\neq 0$. In this case the equation of elliptic curve will be:

$$Y^2=X^3+aXZ^4+bZ^6 \qquad (5)$$

That means, the projective coordinates system can be identified with all points (x,y) of the affine coordinates system plus point (point at infinity O_∞) for which $Z=0$. Putting $Z=0$ in equation (4) or (5), the O_∞ is $(0,1,0)$ or $(1,1,0)$ respectively, there is only one projective points that satisfy the equation (4) and (5) for which $Z=0$.

We have earlier mentioned the formulas for point doubling and point addition in the affine coordinates system **section 2**. Point doubling and point addition formulas for projective coordinates and Jacobian coordinates will be mentioned in the following subsections.

1) *3.1 The Point Doubling and Point Addition Formulas in Projective Coordinates System*

The computation time for the point doubling operation is $7M+5S$ while it is $12M+2S$ operations for point addition, as in the following theorems:

Theorem 3.1 *[8]*

Let $P=(X,Y,Z)$ be a point in a non singular elliptic curve in projective coordinates on $E(F_p)$. Then the formula for the point doubling operation $2P=(X',Y',Z')$ is as follows

$$X'=2BD$$
$$Y'=A(4C-D)-8Y^2B^2$$
$$Z'=8B^3$$

with $A=3X^2+aZ^2$, $B=YZ$, $C=XYB$ and $D=A^2-8C$.

For efficiency purposes, the constant a in equation 5 has been recommended to a fix -3 [10] [11] [4]. Without loss of generality, if we consider this case $a=-3$ in equation 5, the computation cost for A in theorem 3.1 is reduced as follows:

$$A=3(X-Z)(X+Z)$$

The computation cost for point doubling operation is reduced to $8M+3S$.

Theorem 3.2 *[8]*

Let $P_1=(X_1,Y_1,Z_1)$ and $P_2=(X_2,Y_2,Z_2)$ be points in a non singular elliptic curve in projective coordinates on $E(F_p)$ with $P_1\neq P_2$. Then the formula for the point addition operation $P_1+P_2=(X_3,Y_3,Z_3)$ is as follows

$$X_3=FG$$
$$Y_3=E(X_1Z_2F^2-G)$$
$$Z_3=Z_1Z_2F$$

with $E=Y_2Z_1-Y_1Z_2,\ F=X_2Z_1-X_1Z_2$ and $G=E^2Z_1Z_2-F^3-2FX_1Z_2$.

From theorems 3.1 and 3.2 we have confirmation that a point doubling operation requires $7M+5S$, while a point addition operation requires $12M+2S.$ Now, if we consider $Z=Z_1=1$, the computation cost reduces to $5M+3S$ for point doubling and $9M+2S$ for point addition, while when $Z_2=1$ then the computation cost reduces to $8M+2S$ for point addition. The case where one point in affine coordinates and the other one in projective coordinates is referred to as a mixed point addition operation. Furthermore, If $Z_1=Z_2=1$, the computation cost for point addition drops to $4M+2S$.

2) *3.2 The Point Doubling and Point Addition Formulas in Jacobian Coordinates System*

The computation time for the point doubling operation is $5M+4S$ while it is $12M+4S$ operations for point addition, as in the following theorems:

Theorem 3.3 *[19]*

Let $P=(X,Y,Z)$ be a point in a non singular elliptic curve in Jacobian coordinates on $E(F_p)$. Then the formula for the point doubling operation $2P=(X',Y',Z')$ is as follows:

$$X'=B^2-2A$$
$$Y'=B(A-X_3)-8Y^4$$
$$Z'=2YZ$$

with $A=4XY^2$ and $B=3X^2+aZ^4$.

If we consider the efficient case ($a=-3$ in equation 5), then the computation cost for B in theorem 3.3 is reduced as follows:

$$B=3(X-Z^2)(X+Z^2)$$

That means, the computation cost for point doubling operation is reduced to $5M+3S$.

Theorem 3.4 *[19]*

Let $P_1=(X_1,Y_1,Z_1)$ and $P_2=(X_2,Y_2,Z_2)$ be points in a non singular elliptic curve in Jacobian coordinates on $E(F_p)$ with $P_1\neq P_2$. Then the formula for the point addition operation $P_1+P_2=(X_3,Y_3,Z_3)$ is as follows

$$X_3=D^2-E^3-2X_1Z_2^2E^2$$
$$Y_3=D(3X_1Z_2^2E^2-D^2+E^3)-Y_1Z_2^3E^3$$
$$Z_3=Z_1^3Z_2^3E^3$$

with $D=Y_2Z_1^3-Y_1Z_2^3$ and $E=X_2Z_1^2-X_1Z_2^2$.

From theorems 3.3 and 3.4 we have confirmation that a point doubling operation requires $5M+4S$, while a point addition operation requires $12M+4S$. Now, if we consider $Z=Z_1=1$, the computation cost reduces to $3M+3S$ for point doubling and $10M+3S$ for point addition. While when $Z_2=1$ the computation cost for point addition will be $8M+3S$. This case, where one point in affine coordinates and

the other one in Jacobian coordinates also as in the previous subsection 3.2 is referred to as a mixed point addition operation. Furthermore, If $Z_1 = Z_2 = 1$, the computation cost for point addition drops to $3M + 2S$.

Using Jacobian coordinates system offer a faster point doubling than projective coordinates system. On other hand, it offer a slower point addition than projective coordinates system, which is usually the most frequent operation in elliptic curve scalar multiplication [22]. In the following section we will introduce new formula using $4-$ dimensional coordinates system (X,Y,Z,T) with $Z \neq 0$ corresponds to the affine point $(\frac{X}{T},\frac{Y}{Z^3})$ with $T = Z^2$.

4 NEW DESIGN POINT DOUBLING AND POINT ADDITION IN DIMENSIONAL JACOBIAN COORDINATES SYSTEM

In this section, we investigate a new design for point doubling and point addition on elliptic curve over prime field, using $4-$ dimensional coordinates system, where an affine $(\frac{X}{T},\frac{Y}{Z^3})$ with $Z \neq 0$ and $T = Z^2$ is presented as (X,Y,Z,T). Due to the first two coordinates is as recovered point using Jacobian coordinates, we call this the $4-$ dimensional Jacobian coordinates system (denoted by $4-DJC$).

In other words, In $4-DJC$ system, a point (X,Y,Z,T) with $Z \neq 0$ and $T = Z^2$, is corresponds to affine point $(\frac{X}{T},\frac{Y}{Z^3})$. In that case the equation of elliptic curve will be:

$$Y^2 = X^3 + aXT^2 + bT^3 \qquad (6)$$

The first use of this formula was in 2007, by Kim and Kim [7] [14], but in both they used elliptic curves over fields of characteristic three and over binary fields.

3) *4.1 The Point Doubling and Point Addition Formulas in* $4-DJC$

The computation time for the point doubling operation is $4M+3S$ while it is $12M+2S$ operations for point addition, as in the following theorems:

Theorem 4.1

Let $P=(X,Y,Z,T)$ be a point in a non singular elliptic curve in $4-DJC$ on $E(F_p)$. Then the formula for the point doubling operation $2P=(X',Y',Z',T')$ is as follows

$$X' = A^2 - 2B$$
$$Y' = A(B-X') - 8Y^4$$
$$Z' = 2YZ$$

with $A = 3X^2 + aT^2$ and $B = 4XY^2$.

Proof

We will prove that these formulas will lead to the point on non singular in affine coordinates on $E(F_p)$. Suppose that $x=\frac{X}{T}, y=\frac{Y}{Z^3}$ and $T=Z^2$. We will prove that $x'=\frac{X'}{T'}$ and $y'=\frac{Y'}{Z^{3'}}$, where (x', y') is the result for point doubling in affine coordinates system.

$$\frac{X'}{T'} = \frac{(A)^2 - 2B}{2Z'^2}$$
$$= \frac{(3X^2 + aT^2)^2 - 2(4XY^2)}{4Y^2Z^2}$$
$$= \frac{(3X^2 + aT^2)^2}{2YZ^2} - 2\frac{X}{T}$$
$$= \left(\frac{(3X^2 + aT^2)}{2T^2}\frac{Z^3}{Y}\right)^2 - 2x$$
$$= \left(\frac{3\left(\frac{X}{T}\right)^2 + a)}{2\frac{Y}{Z^3}}\right)^2 - 2x$$
$$= \frac{3x^2 + a}{2y} - 2x$$
$$= m - 2x \quad m \text{ refers to the slope}$$
$$= x'$$
$$\frac{Y'}{Z^{3'}} = \frac{A(B-X') - 8Y^4}{8Y^3Z^3}$$
$$= \frac{(3X^2 + aT^2)(4XY^2 - X') - 8Y^4}{8Y^3Z^3}$$
$$= \frac{(3X^2 + aT^2)(4XY^2 - X')}{8Y^3Z^3} - \frac{Y}{Z^3}$$
$$= \frac{3X^2 + aT^2}{2YZ}\frac{4XY^2 - X'}{4Y^2Z^2} - y$$
$$= m\left(\frac{4XY^2}{4Y^2Z^2} - \frac{X'}{4Y^2Z^2}\right) - y,$$
$$= m\left(\frac{X}{T} - \frac{X'}{T'}\right) - y \quad m \text{ refers to the slope}$$
$$= m(x - x') - y$$
$$= y'.$$

If we consider the efficient case where $a=-3$ in equation 6, without loss of generality the computation cost for A in theorem 4.1 is reduced as follows:

$$B = 3(X-T)(X+T)$$

That means, the computation cost for point doubling operation is reduced to $5M + 2S$.

Theorem 4.2

Let $P_1 = (X_1, Y_1, Z_1, T_1)$ and $P_2 = (X_2, Y_2, Z_2, T_2)$ be points in a non singular elliptic curve in $4-DJC$ on $E(F_p)$. Then the formula for the point addition operation $P_1 + P_2 = (X_3, Y_3, Z_3, T_3)$ is as follows

$X_3 = D^2 - C^3 - 2X_1T_2C^2$

$Y_3 = D(X_1T_2C^2 - X_3) - Y_1Z_2T_2C^3$

$Z_3 = Z_1Z_2C$

with $C = X_2T_1 - X_1T_2$ and $B = Y_2Z_1T_1 - Y_1Z_2T_2$.

Proof

We will prove that these formulas will lead to the point on non singular in affine coordinates on $E(F_p)$. Suppose that $x_1 = \frac{X_1}{T_1}, y_1 = \frac{Y_1}{Z_1^3}$, $T_1 = Z_1^2$, $x_2 = \frac{X_2}{T_2}, y_2 = \frac{Y_2}{Z_2^3}$ and $T_2 = Z_2^2$. We will prove that $x_3 = \frac{X_3}{T_3}$ and $y_3 = \frac{Y_3}{Z_3^3}$, where (x_3, y_3) is the result for point doubling in affine coordinates system.

$$\frac{X_3}{T_3} = \frac{D^2 - C^3 - 2X_1T_2C^2}{T_1T_2C^2}$$

$$= \frac{(Y_2Z_1T_1 - Y_1Z_2T_2)^2 - (X_2T_1 - X_1T_2)^3 - 2X_1T_2(X_2T_1 - X_1T_2)^2}{T_1T_2(X_2T_1 - X_1T_2)^2}$$

$$= \frac{(Y_2Z_1^3 - Y_1Z_2^3)^2 - (X_2T_1 - X_1T_2)^3 - 2X_1T_2(X_2T_1 - X_1T_2)^2}{T_1T_2(X_2T_1 - X_1T_2)^2}$$

$$= \frac{(Y_2Z_1^3 - Y_1Z_2^3)^2 - X_1T_2(X_2T_1 - X_1T_2)^2 - X_2T_1(X_2T_1 - X_1T_2)^2}{T_1T_2(X_2T_1 - X_1T_2)^2}$$

$$= \left(\frac{Y_2Z_1^3 - Y_1Z_2^3}{Z_1Z_2(X_2T_1 - X_1T_2)}\right)^2 - \frac{X_1}{T_1} - \frac{X_2}{T_2}$$

$$= \left(\frac{\frac{Y_2}{Z_2^3} - \frac{Y_1}{Z_1^3}}{\frac{X_2}{T_2} - \frac{X_1}{T_1}}\right)^2 - x_1 - x_2$$

$= m^2 - x_1 - x_2$, m refers to the slope

$= x_3$

$$\frac{Y_3}{Z_3^3} = \frac{D(X_1T_2C^2 - X_3) - Y_1Z_2T_2C^3}{Z_1^3Z_2^3C^3}$$

$$= \frac{(Y_2Z_1T_1 - Y_1Z_2T_2)(X_1T_2(X_2T_1 - X_1T_2)^2 - X_3) - Y_1Z_2T_2(X_2T_1 - X_1T_2)^3}{Z_1^3Z_2^3(X_2T_1 - X_1T_2)^3}$$

$$= \frac{(Y_2Z_1^3 - Y_1Z_2^3)(X_1T_2(X_2T_1 - X_1T_2)^2 - X_3) - Y_1Z_2T_2(X_2T_1 - X_1T_2)^3}{Z_1^3Z_2^3(X_2T_1 - X_1T_2)^3}$$

$$= \frac{Y_2Z_1^3 - Y_1Z_2^3}{Z_1Z_2(X_2T_1 - X_1T_2)}\left(\frac{X_1T_2(X_2T_1 - X_1T_2)^2 - X_3}{T_1T_2(X_2T_1 - X_1T_2)^2}\right) - \frac{Y_1}{Z_1}$$

$= m\left(\frac{X_1}{T_1} - \frac{X_3}{T_3}\right) - y_1$ m refers to the slope

$= m(x_1 - x_3) - y_1$

$= y_3$.

From theorems 4.1 and 4.2 we have confirmation that a point doubling operation requires $4M + 3S$, while a point addition operation requires $12M + 2S$. Now, if we consider $Z = Z_1 = 1$, that means $T = T_1 = 1$ then the computation cost reduces to $2M + 3S$ for point doubling and $8M + 2S$ for point addition, with the same cost of computation when $Z_2 = 1$. This case, where one point in affine coordinates and the other one in $4-DJC$ is also referred to as a mixed point addition operation. Furthermore, If $Z_1 = Z_2 = 1$, the computation cost for point addition drops to $3M + 2S$.

5 MIXED COORDINATES SYSTEM

It is possible to mix two different coordinates as was mentioned in 3.1, 3.2 and 4.1. In other words, it is a scheme to add two points: one of them is in some coordinates system, and the second point is in some other coordinates system. This technique has been suggested in [8].

In this section, we will discuss four different kinds of coordinates systems (affine, projective, Jacobian and $4-DJC$). We will show theoretically that the mixed coordinates system with the forth kind of coordinates ($4-DJC$) is more faster than the mixed addition in Jacobian- affine coordinates, and has the same cost of computation with mixed addition in projective- affine coordinates.

In order to use this technique to add two points on elliptic curve, we have to convert a point from one coordinates system to another to apply the formula

for point addition operation on elliptic curve. For example, a point (x, y) in affine coordinates system can be converted to projective coordinates system $(X, Y, 1)$. Table 1 and 2 contained formulas for converting points from one coordinates system to another and the computations cost for each of these conversions among coordinates systems.

Table 1: Conversion Points Among Coordinates Systems

From/ To		Coordinates Systems: Affine (x, y)	Projective (xZ, yZ, Z)	Jacobian (xZ^2, yZ^3, Z)	$4-DJC$ (xT, yZ^3, Z, T)
Coordinates Systems	Affine (x, y)	-	$(x, y, 1)$	$(x, y, 1)$	$(x, y, 1, 1)$
	Projective (xZ, yZ, Z)	$\left(\frac{X}{Z}, \frac{Y}{Z}\right)$	-	(XZ, YZ^2, Z)	(XZ, YZ, Z, T)
	Jacobian (xT, yZ^3, Z, T)	$\left(\frac{X}{Z^2}, \frac{Y}{Z^3}\right)$	$\left(\frac{X}{Z}, \frac{Y}{Z^2}, Z\right)$	-	(X, Y, Z, T)
	$4-DJC$ (xT, yZ^3, Z, T)	$\left(\frac{X}{T}, \frac{Y}{Z^3}\right)$	$\left(\frac{X}{Z}, \frac{Y}{T}, Z\right)$	(XT^2, YT^3, Z)	-

Table 2: Computations Cost for Conversions Points among Coordinates Systems

From/ To		Coordinates Systems: Affine	Projective	Jacobian	$4-DJC$
Coordinates Systems	Affine	-	-	-	-
	Projective	$2M+1I$	-	$2M+1S$	$2M$
	Jacobian	$3M+1S+1I$	$2M+1S+1I$	-	-
	$4-DJC$	$3M+1S+2I$	$2M+2I$	$2M+1S+1I$	-

From tables 1 and 2, we can find out that non of the conversion from affine to projective, Jacobian or $4-DJC$ coordinates and conversion from Jacobian to the $4-DJC$ require field multiplication inversion, multiplication or squaring, this is because the Z, Z^2 and Z^3 setting to 1, which make them fast. On the other hand, the conversion from projective, Jacobian and $4-DJC$ coordinates to affine coordinates involved field multiplication inversion , making these conversion expensive. Conversion from Jacobian to the projective coordinates is less efficient than converting from projective to Jacobian coordinates. The most expensive conversion is from $4-DJC$ to the other coordinates.

4) *5.1 Mixed Addition in Projective-Affine Coordinates*

The formula for the mixed addition for two points with projective coordinates and affine coordinates requires $8M+2S$ [8], as in the following theorem :

Theorem 5.1

Let $P_1=(X_1, Y_1, Z_1)$ and $P_2=(x_2, y_2)$ be points in a non singular elliptic curve in projective and affine coordinates respectively both on $E(F_p)$. Then the formula for the mixed point addition operation $P_1+P_2=(X_3, Y_3, Z_3)$ is as follows

$X_3 = FG$

$Y_3 = E(X_1F^2 - G)$

$Z_3 = Z_1F$

with $E = Y_2Z_1 - Y_1$, $F = X_2Z_1 - X_1$ and $G = E^2Z_1 - F^3 - 2X_1F^2$.

5) *5.2 Mixed Addition in Jacobian-Affine Coordinates*

The formula for the mixed addition for two points with Jacobian coordinates and affine coordinates requires $8M+3S$, as in the following theorem:

***Theorem 5.2** [19]*

Let $P_1 = (X_1, Y_1, Z_1)$ and $P_2 = (x_2, y_2)$ be points in a non singular elliptic curve in Jacobian and affine coordinates respectively both on $E(F_p)$. Then the formula for the mixed point addition operation $P_1 + P_2 = (X_3, Y_3, Z_3)$ is as follows

$X_3 = D^2 - E^3 - 2X_1E^2$

$Y_3 = D(X_1E^2 - X_3) - Y_1E^3$

$Z_3 = Z_1^3E^3$

with $D = Y_2Z_1^3 - Y_1$ and $E = X_2Z_1^2 - X_1$.

6) *5.3 Mixed Addition in $4-DJC$ -Affine Coordinates*

The formula for the mixed addition for two points with Jacobian coordinates and affine coordinates requires $8M + 2S$, as in the following theorem:

Theorem 5.3

Let $P_1 = (X_1, Y_1, Z_1, T_1)$ and $P_2 = (x_2, x_2)$ be points in a non singular elliptic curve in $4-DJC$ and affine coordinates respectively both on $E(F_p)$. Then the formula for the mixed point addition operation $P_1 + P_2 = (X_3, Y_3, Z_3, T_3)$ is as follows

$X_3 = D^2 - C^3 - 2X_1C^2$

$Y_3 = D(X_1C^2 - X_3) - Y_1C^3$

$Z_3 = Z_1C$

with $C = x_2T_1 - X_1$ and $D = y_2Z_1T_1 - Y_1$.

Proof

We will prove that these formulas will lead to the point on non singular elliptic curve in affine coordinates on $E(F_p)$. Suppose that $x_1 = \frac{X_1}{T_1}, y_1 = \frac{Y_1}{Z_1^3}$ and $T_1 = Z_1^2$. We will prove that $x_3 = \frac{X_3}{T_3}$ and $y_3 = \frac{Y_3}{Z_3^3}$, where (x_3, y_3) is the result for point doubling in affine coordinates system.

$$\frac{X_3}{T_3} = \frac{D^2 - C^3 - 2X_1C^2}{T_1C^2}$$

$$= \frac{(y_2Z_1T_1 - Y_1)^2 - (x_2T_1 - X_1)^3 - 2X_1(x_2T_1 - X_1)^2}{T_1(x_2T_1 - X_1)^2}$$

$$= \frac{(y_2Z_1^3 - Y_1)^2 - (x_2T_1 - X_1)^3 - 2X_1(x_2T_1 - X_1)^2}{T_1(x_2T_1 - X_1)^2}$$

$$= \left(\frac{y_2Z_1^3 - Y_1}{Z_1(x_2T_1 - X_1)}\right)^2 - \frac{X_1}{T_1} - x_2$$

$$= \left(\frac{y_2 - \frac{Y_1}{Z_1^3}}{x_2 - \frac{X_1}{T_1}}\right)^2 - x_1 - x_2$$

$$= \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$$

$= m^2 - x_1 - x_2$, m refers to the slope

$= x_3$

$$\frac{Y_3}{Z_3^3} = \frac{D(X_1C^2 - X_3) - Y_1C^3}{Z_1^3C^3}$$

$$= \frac{(y_2Z_1T_1 - Y_1)(X_1(x_2T_1 - X_1)^2 - X_3) - Y_1(x_2T_1 - X_1)^3}{Z_1^3(x_2T_1 - X_1)^3}$$

$$= \frac{(y_2Z_1^3 - Y_1)(X_1(x_2T_1 - X_1)^2 - X_3) - Y_1(x_2T_1 - X_1)^3}{Z_1^3(x_2T_1 - X_1)^3}$$

$$= \frac{y_2Z_1^3 - Y_1}{Z_1(x_2T_1 - X_1)}\left(\frac{X_1(x_2T_1 - X_1)^2 - X_3}{T_1(x_2T_1 - X_1)^2}\right) - \frac{Y_1}{Z_1}$$

$= m\left(\frac{X_1}{T_1} - \frac{X_3}{T_3}\right) - y_1$, m refers to the slope

$= m(x_1 - x_3) - y_1$

$= y_3$.

6 COMPLEXITY AND COMPARISON

Using the proposed coordinates system will reduce the number of field operations for elliptic curve over prime field. Table 3 indicates that there is 41% reduction for point doubling operation comparing with point doubling operation using projective coordinates system, and 22% comparing with point doubling using Jacobian coordinates system. On the other hand, computing point addition operation using the $4-DJC$ system will reduce the number of field operations by 25% comparing with computing point addition using Jacobian. Using Jacobian Coordinates system to compute point addition operation will cost more than using projective coordinates system, while using $4-DJC$ system has the same computation cost with using projective coordinates.

If we consider the mixed coordinates system, then we find that using the proposed coordinates in this system will reduce the point addition by 29% comparing with using Jacobian coordinates in mixed coordinates system. It will has the same computation cost with using projective coordinates in mixed coordinates system.

Table 3: Number of Field Operations for Elliptic Curve Using Different Coordinates Systems

Coordinates System	Point Doubling			Point Addition			Total	
	I	M	S	I	M	S	Point Doubling	Point Addition
Affine	1	2	2	1	2	1	5	4
Projective	–	7	5	–	12	2	12	14
Jacobian	–	5	4	–	12	4	9	16
$4-DJC$	–	4	3	–	12	2	7	14
Mixed *	–	–	–	–	8	2	–	10
Mixed **	–	–	–	–	8	3	–	11
Mixed ***	–	–	–	–	8	2	–	10

* refers to 5.1, ** refers to 5.2 and *** refers to 5.3

Some special cases have been recommended, for example, assuming $a=-3$ in equation 5. Using the proposed coordinates system with these special cases will reduce the number of field operations for elliptic curve over prime field. As shown in table 4, if we consider $a=-3$ then we will get 36% and 12.5% reduction the cost of computation for point doubling using projective and Jacobian coordinates respectively.

In Case $Z=1$ for computing the point doubling the reduction rate will be 37% and 16% comparing with using projective and Jacobian coordinates respectively. Reduced rate will occur when we consider $Z_1=1$, $Z_2=1$ and $Z_1=Z_2=1$ for computing the point addition operation, except in the cases Z_2 and $Z_1=Z_2=1$ the cost of computation for addition operation will be the same comparing with projective and Jacobian coordinates respectively.

Table 4: Number of Field Operations for Elliptic Curve Using Different Coordinates Systems with Special Cases

Coordinates System	Point Doubling		Point Addition		
	$a=-3$	$Z=1$	$Z_1=1$	$Z_2=1$	$Z_1=Z_2=1$
Projective	$8M+3S$	$5M+3S$	$9M+2S$	$8M+2S$	$4M+2S$
	11	8	11	10	6
Jacobian	$5M+3S$	$3M+3S$	$10M+3S$	$8M+3S$	$3M+2S$
	8	6	13	11	5
$4-DJC$	$5M+2S$	$2M+3S$	$8M+2S$	$8M+2S$	$3M+2S$
	7	5	10	10	5

Total

Total

Total

7 CONCLUSION

The aim of this work is to obtain a faster possible point doubling and point addition operation for elliptic curve over prime field. For this, we introduced the $4-DJC$ system, where a point (X,Y,Z,T) with $Z\neq 0$ and $T=Z^2$, corresponds to affine point $(\frac{X}{T},\frac{Y}{Z^3})$ and satisfying the equation 6 over prime field. The computation cost for point doubling using this system is 7 as a total. For point addition operation it is 14 and 10 for point addition when we use this coordinates in addition mixed coordinates. Using $4-DJC$ system offers a faster point doubling than using projective and Jacobian coordinates system. Also, it offers a faster point addition than using Jacobian coordinates. In mixed coordinates system, using $4-DJC$ system offers a faster mixed addition operation than using Jacobian coordinates to compute this operation. Furthermore, if we consider the efficient cases, the $4-DJC$ offers a faster point doubling operation than the projective and the Jacobian coordinates.

8 REFERENCES

[1] Gordon B. Agnew, Ronald C. Mullin, and Scott A. Vanstone. An implementation of elliptic curve cryptosystems over . IEEE Journal on Selected Areas in Communications, 11(5):804–813, 1993.

[2] Essame Al-Daoud, Ramlan Mahmod, Mohammad Rushdan, and Adem Kilicman. A new addition formula for elliptic curves over . IEEE Transactions on Computers, 51(8):972–975, 2002.

[3] Ian F. Blake, Gadiel Seroussi, and Nigel Smart. Elliptic Curves in Cryptography. London Mathematical Society Lecture Note Series 265. Cambridge University Press, Cambridge, 1999.

[4] Eric Brier and Marc Joye. Fast point multiplication on elliptic curves through isogenies. Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, 2643:43–50, 2003.

[5] David M. Burton. Elementary Number Theory. Allyn & Bacon, Boston, revised printing edition, 1980.

[6] David V. Chudnovsky and Gregory V. Chudnovsky. Sequences of numbers generated by addition in formal groups and new primality and factorization tests. Advances in Applied Mathematics, 7(4):385–434, 1986.

[7] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen,

and Frederik Vercauteren. Handbook of Elliptic and Hyperelliptic Curve Cryptography. Series on Discrete Mathematics and Its Applications. Chapman & Hall/CRC, Boca Raton, 2010.

[8] Henri Cohen, Atsuko Miyaji, and Takatoshi Ono. Efficient elliptic curve exponentiation using mixed coordinates. In Advances in Cryptology-ASIACRYPTO'98, LNCS 1514, pages 51–65. Springer-Verlag, 1998.

[9] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, IT-31(4):469–472, 1985.

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

[11] IEEE. Ieee standard specifications for public-key cryptography. 1363 . The Institute of Electrical and Electronics Engineers, 2000.

[12] Don Johnson, Alfred Menezes, and Scott Vanstone. The elliptic curve digital signature algorithm (ecdsa). International Journal of Information Security, 1(1):36–63, 2001.

[13] Kwang Ho Kim, So In Kim, and Ju Song Choe. New fast algorithms for arithmetic on elliptic curves over finite fields of characteristic three. IACR Cryptology ePrint Archive, Report 2007/179, Available at: http://eprint.iacr.org/2007/179.pdf, September 2014., 2007.

[14] Kwang Ho Kim and So In Kim. A new method for speeding up arithmetic on elliptic curves over binary fields. IACR Cryptology ePrint Archive, Report 2007/181, Available at: http://eprint.iacr.org/2007/181.pdf, September 2014., 2007.

[15] Neal Koblitz. Elliptic curve cryptosystems. Mathematics of Computation, 48(177):203–209, 1987.

[16] Tanja Lange. A note on lópez-dahab coordinates. Tatra Mt. Math. Publ, 33:75–81, 2006.

[17] Chae Hoon Lim and Hyo Sun Hwang. Speeding up elliptic scalar multiplication with precomputation. In Information Security and Cryptology-ICISC'99, LNCS 1787, pages 102–119. Springer-Verlag, 2000.

[18] G. Locke and P. Gallagher. Fips pub 186-3: Digital signature standard (dss). federal information processing standards publication. National Institute of Standards and Technology, 2009.

[19] Patrick Longa. Accelerating the Scalar Multiplication on Elliptic Curve Cryptosystems over Prime Fields. PhD's Thesis. University of Ottawa, Canada, 2007.

[20] Victor S. Miller. Use of elliptic curves in cryptography. In Advances in Cryptology-CRYPTO'85 Proceedings (Santa Barbara, Calif., 1985), volume 218, pages 417–426. Springer-Verlag, 1986.

[21] Atsuko Miyaji, Takatoshi Ono, and Henri Cohen. Efficient elliptic curve exponentiation. 1334:282–290, 1997.

[22] Matthieu Rivain. Fast and regular algorithms for scalar multiplication over elliptic curves. IACR Cryptology ePrint Archive, 2011/338, 2011.

[23] Ronald L. Rivest, Adi Shamir, and Len Adleman. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2):120–126, 1978.

[24] Joseph H. Silverman. The Arithmetic of Elliptic Curves. Graduate Texts in Mathematics 106. Springer, New York, 2nd edition, 2009.

[25] Improved algorithms for elliptic curve arithmetic in . pages 201–212, 1999.