An Improved to Compute 2P+Q on Elliptic Curve Over Finite Field of Characteristic ≠ 2,3

Iqbal H. Jebril
Department of Mathematics, Faculty of Science, King Faisal University,
P.O. Box 400, Hufuf, Al Hasa 31982
Saudi Arabia
iqbal501@yahoo.com

***Abstract*- In this paper, we speed up computing (2P + Q) from given point P and Q on elliptic curve over GF(p) by using projective coordinates.**

***Keywords*- Elliptic curves, projective coordinates.**

1. INTRODUCTION

In 1995, Neal Koblits and Victor Miller proposed public key cryptosystems using the group of points on an elliptic curve. Since then, numerous researchers and developers have researching the strength of elliptic curve cryptosystems (ECC) and improving techniques for its implementation. [7]

Elliptic curve E over $GF(p)$, where $p>3$ and prime, is defined by the parameters a and b as the set of solutions (x, y) where $x, y \in GF(p)$ to the (affine) equation

$$y^2 = x^3 + ax + b, \tag{1}$$

where $a,b \in GF(p)$, and $4a^3 + 27b^2 \neq 0$, together with an extra point O "point at infinity". [1]

- Addition of two points, let $P = (x_1, y_1)$ and $Q = (x_2 y_2) \in E$, with $x_1 \neq x_2$,
  $P + Q = (x_1, y_1) + (x_2, y_2) = (x_3, y_3)$,
  $x_3 = \lambda^2 - x_1 - x_2 , y_3 = \lambda\ (x_1 - x_3) - y_1$,

where, $\lambda\ = (y_2 - y_1)(x_2 - x_1)^{-1}$, (2)

- Doubling of a point with $x_1 \neq 0$
  $R = 2P = 2(x_1, y_1) = (x_2, y_2)$,
  $x_2 = \lambda_1^2 - 2x_1 , y_2 = \lambda_2(x_1 - x_2) - y_1$,where,
  $\lambda_1 = (3x_1^2 + a)(2y_1)^{-1}$. (3)

Two points are added, forming $P + Q$, or point is doubled, forming $2P$, these formulae are evaluated at the cost of some number of inversion (I), squaring (S), and multiplications (M) in the field. For example, we note that addition for elliptic curve $GF(p)$, Formula 2 requires one inversion, two multiplications, one squaring ($1I + 2M + 1S$). To double a point for elliptic curve $GF(p)$, Formula 3 requires one inversion, two multiplications, two squaring ($1I + 2M + 2S$). To double a point, so that to perform a doubling and an addition $2P + Q$ costs two inversions, three squaring and four multiplications ($2I + 4M + 3S$) if the points are added as $(P + P) + Q$, i.e., first double P and then add Q. [7]

- If $2P = 2(x_1, y_1) = (\lambda_1^2 - 2x_1 , \lambda_1(x_1 - A) - y_1) = (A, B)$, then $(A, B) + (x_2, y_2) = (x_3, y_3) = (\lambda_1^2 - A - x_2 , \lambda_1^2(A - x_3) - B)$,
  where, $\lambda_2 = (y_2 - B)(x_2 - A)^{-1}$, so that
- $$\frac{y_2 - B}{x_2 - A} = \frac{y_2 - \lambda_1(x_1 - A) + y_1}{x_2 - \lambda_1^2 + 2x_1} = \frac{y_2 - \lambda_1(-\lambda_1^2 + 3x_1) + y_1}{x_2 - \lambda_1^2 + 2x_1} = \frac{y_2 + \lambda_1^3 - 3x_1\lambda_1 + y_1}{x_2 - \lambda_1^2 + 2x_1}.$$
- $$x_3 = \lambda_2^2 - A - x_2 = \left(\frac{y_2 - B}{x_2 - A}\right)^2 - \lambda_1^2 + 2x_1 - x_2 = \left(\frac{y_2 + \lambda_1^3 - 3x_1\lambda_1 + y_1}{x_2 - \lambda_1^2 + 2x_1}\right)^2 - \lambda_1^2 + 2x_1 - x_2 . \tag{4}$$
- $$y_3 = \lambda_2^2(A - x_3) - B = \left(\frac{y_2 - B}{x_2 - A}\right)^2 (\lambda_1^2 - 2x_1 - x_3) - \lambda_1(x_1 - \lambda_1^2 + 2x_1) + y_1 = \left(\frac{y_2 + \lambda_1^3 - 3x_1\lambda_1 + y_1}{x_2 - \lambda_1^2 + 2x_1}\right)^2 = (\lambda_1^2 - 2x_1 - x_3) - \lambda_1(3x_1 - \lambda_1^2) + y_1 . \tag{5}$$

ELM method [5] performs a doubling and an addition $2P + Q$ on an elliptic curve E using only three multiplication, two squaring, and two inversions. This is achieved as follows: to form $2P + Q$, where $P = (x_1, y_1)$ and $Q = (x_2, y_2)$, first find $(P + Q)$, except omit its y-coordinate, because we will not need that for the next stage. This saves a field multiplication. Next we form $(P + Q) + P$. So we have done two point additions and saved one multiplication.

Suppose $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ are distinct points on E, and $x_1 \neq y_1$. The point $P + Q$ will have coordinates (x_3, y_3) , where

$$\lambda_1 = (y_2 - y_1)(x_2 - x_1)^{-1},$$
$$x_3 = \lambda_1^2 - x_1 - x_2, \text{and } y_3 = (x_1 - x_3)\lambda_1 - y_1.$$

Now suppose we want to add $(P + Q)$ to P. We must add (x_1, y_1) to (x_3, y_3) using the above rule. Assume $x_3 \neq x_1$. The result has coordinates (x_4, y_4) , where

$$\lambda_2 = (y_3 - y_1)(x_3 - x_1)^{-1} = -\lambda_1 - 2y_1 / (x_3 - x_1),$$
$$x_4 = \lambda_2^2 - x_1 - x_3, \text{and } y_4 = (x_1 - x_4)\lambda_2 - y_1.$$

Omitting the y_3 computation saves a field multiplication. Each λ_2 formula requires a field inversion, so the overall saving is this field multiplication. Hence, ELM method requires $2I$+$3M$+$2S$.

CJLM method [6] performs a doubling and an addition, $2P + Q$, on an elliptic curve E using only $1I$+$9M$+2S. This is achieved as follows: to form $2P$+Q, where $P = (x_1, y_1)$ and $Q = (x_2, y_2)$, In first remark that x_4 can be obtained as $x_4 = (\lambda_2 - \lambda_1)(\lambda_1 + \lambda_2) + x_2$.

Furthermore, letting $d = (x_2 - x_1)^2 (2x_1 + x_2) - (y_2 - y_1)^2$, we see that $d = (x_2 - x_1)^2 (x_1 - x_3)$. Defining $D = d\ (x_2 - x_1)$ and $I = D^{-1}$, we have

$$\frac{1}{(x_2 - x_1)^2} = dI \text{ and } \frac{1}{x_1 - x_3} = (x_2 - x_1)^3 I .$$

Consequently, the value of x_3 is not needed. We note that the cost of computing $2P + Q$ is at most 1 inversion, 2 squaring, and 9 (field) multiplications.

2. ARITHMETIC USING PROJECTIVE COORDINATES

By improvement Jacobian coordinate formula, a projective point (X, Y, Z), $Z \neq 0$ corresponds to the affine point $(X / Z^2 , Y / Z^3)$ and the projective equation of the curve is $Y^2 = X^3 + aXZ^4 + bZ^6$. Let $P = (X_1, Y_1, Z_1)$, $Q = (X_2, Y_2, Z_2)$ and $2P + Q = (X_3, Y_3, Z_3)$. Curve addition formulas in a new addition formula $(P \neq ^{+}_{-} Q)$. These formulas have no inversion any more.

TABLE 1
PROJECTIVE COORDINATES
($2P$ +Q , PRIME CASE)

$A = 4X_1Y_1^2$,	$B = 3X_1^2 + aZ_1^4$,
$C = -2A + B^2$,	$D = 2Y_1Z_1$,
$E = -8Y_1^4 + B(A - C)$,	$F = CZ_2^2$,
$G = X_2D^2$,	$H = EZ_2^3$,
$I = Y_2D^3$,	$J = G - F$,
$K = I - H$,	$Z_3 = Z_2DJ$,
$X_3 = -J^3 - 2FJ^2 + K^2$,	
$Y_3 = -HJ^3 + K(FJ^2 - X_3)$	

Now, we are going to prove that the new formula, let $P = (X_1, Y_1, Z_1)$ and $Q = (X_2, Y_2, Z_2)$ be two points on the elliptic curve E. Assume that $X_1 / Z_1^2 = x_1, Y_1 / Z_1^3 = y_1$, $X_2 Z_2^2 = x_2$ and $Y_2 / Z_2^3 = y_2$, now we are going to show $X_3 / Z_3^2 = x_2$ and $Y_3 / Z_3^3 = y_3$, where (x_3, y_3) is generated by (x_1, y_1) and (x_2, y_2) by using the standard addition formula of affine coordinates, then the addition formula is $2P + Q = (X_3 / Z_3^2, Y_3 / Z_3^3)$. First, in order to prove $\frac{X_3}{Z_3^2} = x_2$,

$$\frac{C}{D^2} = \frac{-2A + B^2}{(2Y_1Z_1)^2} = \frac{-2(4X_1Y_1^2) + (3X_1^2 + aZ_1^4)^2}{(2Y_1Z_1)^2}$$
$$= \frac{-2X_1}{Y_1^2} + \left(\frac{3X_1^2 + aZ_1^4}{2Y_1Z_1}\right)^2$$
$$= -2x_1 + L^2, \text{ where}, L = \frac{3X_1^2 + aZ_1^4}{2Y_1Z_1}.$$

$$\mathrm{A - C} = 4X_1Y_1^2 - (-2A + B^2) = 3(4X_1Y_1^2) - (3X_1^2 + aZ_1^4)^2 = 12X_1Y_1^2 - (3X_1^2 + aZ_1^4)^2$$

$$\mathrm{B(A - C)} = (3X_1^2 + aZ_1^4)(12X_1Y_1^2 - (3X_1^2 + aZ_1^4)^2)$$

$$\frac{\mathrm{E}}{\mathrm{D}^3} = \frac{-8Y_1^4 + B(A - C)}{(2Y_1Z_1)^3} = -\frac{Y_1}{Z_1^3} + \frac{B(A - C)}{(2Y_1Z_1)^3}$$

$$= -y_1 + \frac{(3X_1^2 + aZ_1^4)(12X_1Y_1^2 - (3X_1^2 + aZ_1^4)^2)}{(2Y_1Z_1)^3}$$

$$= -y_1 + \frac{(12X_1Y_1^2)(3X_1^2 + aZ_1^4)}{(2Y_1Z_1)^3} - \left(\frac{3X_1^2 + aZ_1^4}{2Y_1Z_1}\right)^3$$

$$= -y_1 + 3\frac{X_1}{Z_1^2}\left(\frac{3X_1^2 + aZ_1^4}{2Y_1Z_1}\right) - L^3 = -y_1 + 3x_1L - L^3$$

$$\frac{X_3}{Z_3^2} = \frac{-J^3 - 2FJ^3 + K^2}{(DZ_2J)^2} = \frac{-J - 2F}{(Z_2D)^2} + \left(\frac{K}{Z_2DJ}\right)^2$$

$$= \frac{F - G - 2F}{(Z_2D)^2} + \left(\frac{I - M}{Z_2DJ}\right)^2$$

$$= \frac{-(X_2D^2 + CZ_2^2)}{(Z_2D)^2} + \left(\frac{Y_2D^3 - EZ_2^3}{Z_2D(X_2D^2 - CZ_2^2)}\right)^2$$

$$= \frac{-X_2}{Z_2^2} - \frac{C}{D^2} + \left(\frac{(Y_2/Z_2^3) - (E/D^3)}{(X_2/Z_2^2) - (C/D^2)}\right)^2$$

$$= -x_2 - \frac{C}{D^2} + \left(\frac{y_2 - (E/D^3)}{x_2 - (C/D^2)}\right)^2$$

$$= -x_2 - (-2x_1 + L^2) + \left(\frac{y_2 + y_1 - 3x_1L + L^3}{x_2 + 2x_1 - L^2}\right)^2$$

$$= -x_2 + 2x_1 - L^2 + \left(\frac{y_2 + y_1 - 3x_1L + L^3}{x_2 + 2x_1 - L^2}\right)$$

$$= x_3, \text{(see Formula(4))}$$

Second, in order to prove $\frac{Y_3}{Z_3^3} = y_3$,

$$\frac{I - H}{(Z_2D)(G - F)} = \frac{Y_2D^3 - EZ_2^3}{(Z_2D)(X_2D^2 - CZ_2^2)^3}$$

$$= \frac{(Y_2D^3 - EZ_2^3)/(Z_2D)^3}{(X_2D^2 - CZ_2^2)^3/(Z_2D)^2}$$

$$= \frac{y_2 - E/D^3}{x_2 - C/D^2} = \frac{y_2 - (-y_1 + 3x_1L - L^3)}{x_2 - (-2x_1 + L^2)}$$

$$= \frac{y_2 + y_1 - 3x_1L + L^3}{x_2 + 2x_1 - L^2}.$$

$$\frac{Y_3}{Z_3^3} = \frac{-HJ^3 + K(FJ^2 - x_3)}{(Z_2DJ)^3}$$

$$= \frac{-E}{D^3} + \frac{KCZ_2^2J^2}{(Z_2DJ)^3} - \frac{Kx_3Z_3^2}{(Z_2DJ)^3}$$

$$= -(-y_1 + 3x_1L - L^3) + \frac{KC}{Z_2JD^3} - \frac{Kx_3(Z_2DJ)^2}{(Z_2DJ)^3}$$

$$= y_1 - 3x_1L + L^3 + \frac{K(C - x_3D^2)}{Z_2JD^3}$$

$$= y_1 - 3x_1L + L^3 + \left(\frac{K}{Z_2JD}\right)\left(\frac{C - x_3D^2}{D^2}\right)$$

$$= y_1 - 3x_1L + L^3 + \left(\frac{I - H}{(Z_2D)(G - F)}\right)(-2x_1 + L^2 - x_3)$$

$$= y_1 - 3x_1L + L^3 + \left(\frac{y_2 + y_1 - 3x_1L + L^3}{x_2 + 2x_1 - L^2}\right)(-2x_1 + L^2 - x_3)$$

$$= y_3. \quad \text{(see Formula(5))}$$

In this formula $2P + Q = (X_3 / Z_3^2, Y_3 / Z_3^3)$ and the number of field multiplication is 16, and the number of squaring is 10. (See Table 3)

Table 2, summarizes the costs of some operations on *E* for some kind system of coordinates.

TABLE 2
COSTS OF SIMPLE OPERATIONS ON *E*

System of coordinates	*I*	*M*	*S*
Affine	2	2	3
ELM method	2	1	2
CJLM method	1	9	2
Our formulae	0	16	10

3. TIMING

The ratio of inversion to multiplication (with fast reduction) is roughly 80 to 1.[3]

Cost of non-adjacent form. The non-adjacent form (NAF) of an exponent *n* is

$$n = 2^{e_k} \pm 2^{e_{k-1}} \pm \cdots \pm 2^{e_2} \pm 2^{e_1},$$

in which $0 \le e_1 < e_2 < \ldots < e_k$, and no two e_i are consecutive. The value of k will be about $\log_2(n) / 3$ and e_k will be about $\log_2(n)$.

Point doubling is done with 6 squaring and 4 field multiplications (6*S*+4*M*) (assuming equation (1)). We will need e_k doublings, of which $k-1$ are followed immediately by an add (or subtract). The overall cost is

$$(k-1)(10S+16M)+(e_k-k+1)(6S+4M)$$
$$=(k-1)(4S+12M)+e_k(6S+4M),$$

which should be about

$$(\log_2(n)/3)(4S+12M)+\log_2(n)(6S+4M)$$
$$=\log_2(n)({}^{22}\!/\!_3\,2S+8M).$$

Divide by $\log_2(n)$ to get the average cost per bit:

$${}^{22}\!/\!_3\,2S+8M\ .$$

The comparisons in Table 3 neglect pre- and post-computations.

Table 3, presents rough estimates of costs in terms of both elliptic operation and field operation for point multiplication methods P-192 elliptic curve. [6]

TABLE 3
ROUGH ESTIMATES OF POINT MULTIPLICATION COST FOR P-192

System of coordinates		Cost per bit	$S=0.8M$	$I=80M$
Affine	2I+3S +2M	${}^4\!/\!_3 I+{}^7\!/\!_3 S+{}^8\!/\!_3 M$	1.33I+ 4.54M	111.18 M
ELM method	2I+2S +1M	${}^4\!/\!_3 I+2S+{}^7\!/\!_3 M$	1.33I+ 3.93M	110.57 M
CJLM method	1I+2S +9M	$1I+2S+{}^{13}\!/\!_3 M$	1.00I+ 5.93M	86.01 M
Our formulae	10S+ 16M	${}^{22}\!/\!_3 S+8M$	13.86M	13.86 M

REFERENCES

[1] http://www.certicom.com, Jan. **2001**.

[2] Blake, I., Serouss, G., and Smart, N., *Advances in Elliptic Curve Cryptography,* Cambridge University Press, 2005.

[3] Brown, M., Hankerson, D., L´opez, J. and Menezes, A., **2001**. Software implementation of the NIST elliptic curves over prime fields. In D. Naccache, editor, Topics in Cryptology – CT-RSA 2001, vol. 2020 of Lecture Notes in Computer Science, pp. 250–265. Springer-Verlag.

[4] Chudnovsky, D. and Chudnovsky, G., **1987**. Sequences of numbers generated by addition in formal groups and new primality and factoring tests", *Advances in Applied Mathematics*, 7 , 385-434.

[5] Eisentrager, K., Lauter, K. and Montgomery, P. **2003** . Fast elliptic curve arithmetic and improved Weil pairing evaluation. In M. Joye, editor, Topics in Cryptology – CT-RSA 2003, vol. 2612 of *Lecture Notes in ComputerScience*, pp. 343–354. *Springer-Verlag*.

[6] Ciet, M., Joye, M., Lauter, K. and Montgomery P. **2003**. Trading Inversions for Multiplications in Elliptic Curve Cryptography, *Kluwer AcademicPublishers. Printed in the Netherlands*.pp. 1-20.

[7] IEEE P1363, **2000**. Standard Specifications for Public Key Cryptography, *IEEE computer Society*.

[8] Konstantinov, E., Stamatiou, Y. and Zaroliagis, G, **2002**. A Software Library for Elliptic Curve Cryptography, Springer-Verlang, pp. 625- 637.