Comparison of Point Operations over Edwards Curve and its Variants

Dr. S. Joseph Robin

Associate Professor, Department of Mathematics, Scott Christian College (Autonomous)
Nagercoil – 629 003, Kanyakumari District, Tamil Nadu, India.
sjosephrobin@yahoo.com

***Abstract* – In this paper the point operation of Edwards Curves, Twisted Edwards Curve and Binary Edwards Curves are discussed. The computational efficiency are also calculated in terms of point addition, doubling and scalar multiplication.**

***Keywords* – Curve Arithmetic, Field, Edwards curve, Twisted Edwards curve, Binary Curves**

I. Edwards Curves

Edwards introduced a new model of elliptic curves over F with $char(F) \neq 2$ which is defined by (Edwards 2007)

$$E_c : x^2 + y^2 = c^2(1 + x^2y^2) \quad (1)$$

where $c \in F$. Here obtained an efficient explicit formula for point addition of these curves as follows: Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two points on E_c. Then $P + Q = R = (x_3, y_3)$, where

$$x_3 = \frac{x_1y_2+x_2y_1}{c(1+x_1x_2y_1y_2)}$$

$$y_3 = \frac{y_1y_2-x_1x_2}{c(1-x_1x_2y_1y_2)}$$

Edwards showed that all elliptic curves over non-binary finite field F can be transformed to Edwards's curves if F is algebraically closed. However, over the finite field F, only a small number of elliptic curves can be expressed in this form. Bernstein and Lange improved the notion of Edwards form defined by (Bernstein 2007)

$$E_d : x^2 + y^2 = 1 + dx^2y^2 \quad (2)$$

where $d \in F - \{0, 1\}$. They showed that more than ¼ of all isomorphism classes of elliptic curves over the finite field F could be transformed to Edwards curve over the same field. The curve E_d has an additive group structure together with the identity (neutral) element $O = (0, 1)$. The point $O^{|} = (0, -1)$ has order 2. The points $(1, 0)$ and $(-1, 0)$ have order 4.

The geometric interpretation of the addition law for Edwards curves is given by the following way (Arenea 2011): (Fig. 1, 2 and 3) We first observe that $\Omega_1 = (1 : 0 : 0)$ and $\Omega_2 = (0 : 1 : 0)$ are the points at infinity that have multiplicity 2. There is a conic C determined by passing through the 5 points P, Q, $O^{|}$, Ω_1 and Ω_2 has only one more intersection point $-R$ with the curve E. Let h_1 be the function corresponding to C with $div(h_1) = (P) + (Q) + (O^{|}) + (-R) - 2(\Omega_1) - 2(\Omega_2)$. In order to replace $O^{|}$ by O and $-R$ by R, one can use another function h_2 that is the product $h_2 = l_1l_2$ of two lines. A horizontal line l_1 passing through the point R is with $div(l_1) = (R) + (-R) - 2(\Omega_2)$, and a vertical line l_2 passing through the point O is with $div(l_2) = (O) + (O^{|}) - 2(\Omega_1)$. Therefore, the equation $R = P + Q$ corresponds to $div(h_1/l_1l_2) = (P) + (Q) - (R) - (O)$. Using this observation, Bernstein and Lange write down the explicit formula for point addition and point doubling of the curve E_d as follows (Bernstein 2007): Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two points on E_d. Then $P + Q = R = (x_3, y_3)$, where

$$x_3 = \frac{x_1y_2+x_2y_1}{(1+dx_1x_2y_1y_2)}$$

$$y_3 = \frac{y_1y_2-x_1x_2}{(1-dx_1x_2y_1y_2)}$$

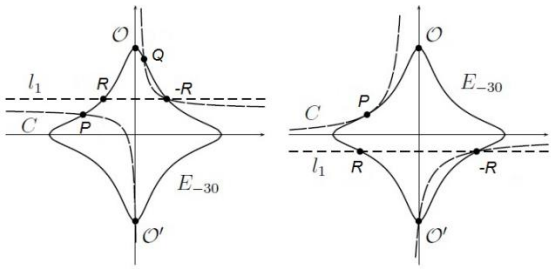

Fig.1 Addition and Doubling over R in Edwards Curves for $d < 0$

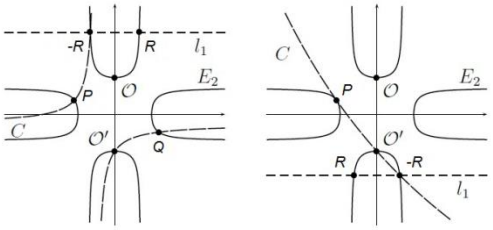

Fig. 2 Addition and Doubling over R in Edwards Curves for $d > 0$

These formulae are strongly unified. If d is a non-square in F, the addition law is complete, i.e., it works for all pairs of inputs. The inverse of the point (x_1, y_1) on E_d is $(-x_1, y_1)$. In order to avoid the

inversion in addition formulae, the notion of Edwards curves in projective coordinates (Bernstein 2007) is defined by

$$(X^2 + Y^2)Z^2 = (Z^4 + dX^2Y^2) \quad (3)$$

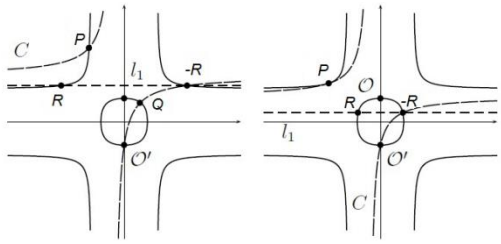

Fig. 3 Addition and Doubling over R in Edwards Curves for $0<d<1$

The point addition for equation (3) is obtained by the following formulae: Let $P = (X_1 : Y_1 : Z_1)$ and $Q = (X_2 : Y_2 : Z_2)$ be two points on equation 5.5, then $P + Q = R = (X_3 : Y_3 : Z_3)$, where

$X_3 = Z_1Z_2(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2)[(X_1 + Y_1)(X_2 + Y_2) - X_1X_2 - Y_1Y_2]$

$Y_3 = Z_1Z_2(Z_1^2Z_2^2 + dX_1X_2Y_1Y_2)(Y_1Y_2 - X_1X_2)$

$Z3 = (Z_1^2Z_2^2 - dX_1X_2Y_1Y_2)(Z_12Z_22 + dX_1X_2Y_1Y_2)$

These formulae are also unified. The point $(0 : 1 : 1)$ is the identity element of addition law. The inverse of $(X_1 : Y_1 : Z_1)$ is $(-X_1 : Y_1 : Z_1)$.

The computational cost for addition, doubling, and unified addition is $10M + 1S + 1D + 7a$, $3M + 4S + 6a$, and $10M + 1S + 1D + 7a$, respectively (where M represents point addition, D represents point doubling, S represents scalar multiplication and a represents multiplication with other constants). The mixed addition formulae can also be obtained by replacing $Z_2 = 1$ in the above formulae that reduces the total costs to $9M + 1S + 1D + 7a$. The presence of point of order 4 in the group of elliptic curves in equation 3, reduces the number of elliptic curves in Edwards model over F.

II. Twisted Edwards Curves

Let F be a field with char(F) ≠ 2. Then twisted Edwards curve is defined by

$$E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2 \quad (4)$$

where $a, d \in F - \{0\}$. The twisted Edwards curve $E_{a,d}$ is a quadratic twist of the Edwards curve $E_{1,d/a}$. If a is square in F, then $E_{a,d}$ is isomorphic to $E_{1,d/a}$ over F. The set of these curves is invariant under quadratic twists, in other words, every quadratic twist of a twisted Edwards curve is isomorphic to a twisted Edwards curve. The point addition for equation 5.6 is obtained by the following formulae: Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two points on $E_{a,d}$. Then $P + Q = R = (x_3, y_3)$, where

$$x_3 = \frac{x_1y_2 + x_2y_1}{(1 + dx_1x_2y_1y_2)}$$

$$y_3 = \frac{y_1y_2 - ax_1x_2}{(1 - dx_1x_2y_1y_2)}$$

These formulae are unified. The point $(0, 1)$ is the identity element of addition law and the inverse of the point (x_1, y_1) on $E_{a,d}(F)$ is $(-x_1, y_1)$. If a is square in F and d is non-square in F, then the addition law for Twisted Edwards curve is complete. In order to avoid inversion in addition formulae given above, twisted Edwards curves in projective coordinates is defined by

$$(aX^2 + Y^2)Z^2 = Z^4 + dX^2Y^2 \quad (5)$$

For $Z_1 \neq 0$, the homogeneous point $(X_1 : Y_1 : Z_1)$ represents the affine point $(X_1/Z_1, Y_1/Z_1)$ on $E_{a,d}$. We obtained the following explicit formulae for addition and doubling on twisted Edwards curves in projective coordinates as follows (Bernstein 2008): Let $P = (X_1 : Y_1 : Z_1)$ and $Q = (X_2 : Y_2 : Z_2)$ be two points on equation (5), then $P + Q = R = (X_3 : Y_3 : Z_3)$, where

$X_3 = (X_1Y_2 - Y_1X_2)(X_1Y_1Z_2^2 + X_2Y_2Z_1^2)$

$Y_3 = (Y_1Y_2 + aX_1X_2)(X_1Y_1Z_2^2 - X_2Y_2Z_1^2)$

$Z_3 = Z_1Z_2(X_1Y_2 - Y_1X_2)(Y_1Y_2 + aX_1X_2)$

and $2P = R = (X_3 : Y_3 : Z_3)$, where

$X_3 = (aX_1^2 + Y_1^2 - 2Z_1^2)[(X_1 + Y_1)^2 - X_1^2 - Y_1^2]$

$Y_3 = (aX_1^2 + Y_1^2)(aX_1^2 - Y_1^2)$

$Z_3 = (aX_1^2 + Y_1^2)(aX_1^2 + Y_1^2 - 2Z_1^2)$

The computational cost of point addition and point doubling are $11M + 2D + 9a$ and $3M + 4S + 1D + 7a$, respectively. It turns out that a mixed addition requires $9M + 2D + 9a$ by setting $Z_2 = 1$.

The unified addition formulae for twisted Edwards curves in projective coordinates are also obtained as follows: Let $P = (X_1 : Y_1 : Z_1)$ and $Q = (X_2 : Y_2 : Z_2)$ be two points on equation 5.7, then $P + Q = R = (X_3 : Y_3 : Z_3)$, where

$X_3 = Z_1Z_2(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2)[(X_1 + Y_1)(X_2 + Y_2) - X_1X_2 - Y_1Y_2]$

$Y_3 = Z_1Z_2(Z_1^2Z_2^2 + dX_1X_2Y_1Y_2)(Y_1Y_2 - aX_1X_2)$

$Z_3 = (Z_1^2Z_2^2 + dX_1X_2Y_1Y_2)(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2)$

The computational cost of unified addition is $10M + 1S + 2D + 7a$.

Another way to avoid inversions is to define inverted coordinates as follows:

$$(X^2 + aY^2)Z^2 = X^2Y^2 + dZ^4 \quad (6)$$

where $XYZ \neq 0$. The homogeneous point $(X_1 : Y_1 : Z_1)$ with $X_1Y_1Z_1 \neq 0$ represents the affine point $(Z_1/X_1, Z_1/Y_1)$ on $E_{a,d}$. In (Bernstein 2007), Bernstein and Lange introduced these inverted coordinates for the case $a = 1$, and observed that the coordinates save time in addition. Bernstein et al. generalized to arbitrary a in (Bernstein 2008). They also obtained the following explicit formulae for unified addition and doubling on twisted Edwards curves in inverted coordinates as follows: Let $P = (X_1 : Y_1 : Z_1)$ and $Q = (X_2 : Y_2 : Z_2)$ be two points on equation 5.8, then $P + Q = R = (X_3 : Y_3 : Z_3)$, where

$X_3 = Z_1Z_2(X_1X_2 + aY_1Y_2)(X_1Y_1Z_2^2 - Z_12X_2Y_2)$
$Y_3 = Z_1Z_2(X_1Y_2 - Y_1X_2)(X_1Y_1Z_2^2 + Z_1^2X_2Y_2)$
$Z_3 = (X_1Y_1Z_2^2 - Z_1^2X_2Y_2)(X_1Y_1Z_2^2 - Z_1^2X_2Y_2)$

and $2P = R = (X_3 : Y_3 : Z_3)$, where

$X_3 = (X_1^2 + aY_1^2)(X_1^2 - aY_1^2)$
$Y_3 = [(X_1 + Y_1)^2 - X_1^2 - Y_1^2](X_1^2 + aY_1^2 - 2dZ_1^2)$
$Z_3 = (X_1^2 - aY_1^2)[(X_1 + Y_1)^2 - X_1^2 - Y_1^2]$

The unified addition formulae for twisted Edwards curves in inverted coordinates are also obtained as follows: Let $P = (X_1 : Y_1 : Z_1)$ and $Q = (X_2 : Y_2 : Z_2)$ be two points on equation 5.7, then $P + Q = R = (X_3 : Y_3 : Z_3)$, where

$X_3 = (X_1X_2Y_1Y_2 + dZ_1^2Z_2^2)(X_1X_2 - aY_1Y_2)$
$Y_3 = (X_1X_2Y_1Y_2 - dZ_1^2Z_22)[(X_1 + Y_1)(X_2 + Y_2) - X_1X_2 - Y_1Y_2]$
$Z_3 = Z_1Z_2(X_1X_2 - aY_1Y_2)[(X_1 + Y_1)(X_2 + Y_2) - X_1X_2 - Y_1Y_2]$

The computational cost of point addition, point doubling and unified addition are *11M + 2D + 9a*, *3M + 4S + 2D + 6a*, and *9M + 1S + 2D + 7a*, respectively. The mixed addition formulae can also be obtained by replacing $Z_2 = 1$, which gives an obvious saving of 2M since $Z_1 \cdot Z_2 = Z_1$, leading to a total cost of *9M+ 2D + 9a*.

The extended Twisted Edwards coordinates is introduced in (Hisil 2008) by defining an auxiliary coordinate $t = xy$ to represent a point (x, y) on $E_{a,d}$ in extended affine coordinates (x, y, t). One can pass to the projective representation $(X : Y : T : Z)$ which satisfies equation 5.7 and corresponds to the extended affine point $(X/Z, Y/Z, T/Z)$ with $Z \neq 0$. The auxiliary coordinate T has the property T = XY/Z. Let $P = (X_1 : Y_1 : T_1 : Z_1)$ and $Q = (X_2 : Y_2 : T_2 : Z_2)$ be two points on equation 5.7 with $Z_1 \neq 0$ and $Z_2 \neq 0$, then $P + Q = R = (X_3 : Y_3 : T_3 : Z_3)$, where

$X_3 = (X_1Y_2 + Y_1X_2)(Z_1Z_2 - dT_1T_2)$
$Y_3 = (Y_1Y_2 - aX1X_2)(Z_1Z_2 + dT_1T_2)$
$T_3 = (Y_1Y_2 - aX_1X_2)(X_1Y_2 + Y_1X_2)$
$Z_3 = (Z_1Z_2 - dT_1T_2)(Z_1Z_2 + dT_1T_2)$

These formulae are unified that derived from thevaddition formulae on $E_{a,d}$. It is deduced from (Bernstein 2007) and (Bernstein 2008) that these formulae are also complete when d is not a square in F and a is a square in F. The identity element is represented by $(0 : 1 : 0 : 1)$. The negative of $(X_1 : Y_1 : T_1 : Z_1)$ on equation (5) is $(-X_1 : Y_1 : -T_1 : Z_1)$. The computational cost of point addition, point doubling and unified addition are *9M + 1D + 7a*, *4M + 4S + 1D + 7a*, and *9M + 2D + 7a*, respectively. The mixed addition formulae can also be obtained by setting $Z_2 = 1$ in the above formulae, reduces the total costs to *8M + 1D + 7a*. This means that one can add $(X_1 : Y_1 : T_1 : Z_1)$ and an extended affine point (x_2, y_2, x_2y_2), which is equally written as $(x_2 : y_2 : x_2y_2 : 1)$.

III. Binary Edwards Curves

Let F be a field with $char(F) = 2$. Then Binary Edwards curve is defined by $E_{B,d_1,d_2} : d_1(x + y) + d_2(x^2 + y^2) = xy + xy(x + y) + x^2y^2$, where $d_1 \neq 0$ and $d_2 \neq d_1^2 + d_1$. The point addition is obtained by the following formulae: Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two points on E_{B,d_1,d_2}. Then $P + Q = R = (x_3, y_3)$, where

$$x_3 = \frac{d_1(x_1+x_2)+d_2(x_1+y_1)(x_2+y_2)}{d_1+(x_1+x_1^2)(x_2+y_2)} + \frac{(x_1+x_1^2)(x_2(y_1+y_2+1)+y_1y_2)}{d_1+(x_1+x_1^2)(x_2+y_2)}$$

$$y_3 = \frac{d_1(y_1+y_2)+d_2(x_1+y_1)(x_2+y_2)}{d_1+(y_1+y_1^2)(x_2+y_2)} + \frac{(y_1+y_1^2)(y_2(x_1+x_2+1)+x_1x_2)}{d_1+(y_1+y_1^2)(x_2+y_2)}$$

The addition law on E_{B,d_1,d_2} is strongly unified. The point $(0, 0)$ is the identity element of addition law and the inverse of the point (x_1, y_1) on E_{B,d_1,d_2} is (y_1, x_1). The computational cost of addition and doubling in projective coordinates are *21M + 1S + 4D* and *2M + 6S + 3D*, respectively. When $t^2 + t + d_2 \neq 0$ for all $t \in F$, the addition law on the binary Edwards curve $E_{B,d_1,d_2}(F)$ is complete. The mixed addition formulae lead to a total cost of 13M + 3S + 3D that can be obtained by $(X_3 : Y_3 : Z_3) = (X_1 : Y_1 : Z_1) + (x_2, y_2)$, where $(X_1 : Y_1 : Z_1)$ and (x_2, y_2) on $E_{B,d_1,d_2}(F)$.

IV. Conclusion

The computational cost for addition, doubling, and unified addition is *10M + 1S + 1D + 7a*, *3M + 4S + 6a*, and *10M + 1S + 1D + 7a*, respectively for Edwards curves. The computational cost of point addition, point doubling and unified addition are *9M + 1D + 7a*, *4M + 4S + 1D + 7a*, and *9M + 2D + 7a*, respectively. The mixed addition formulae can also be obtained by setting $Z_2 = 1$ in the above formulae, reduces the total costs to *8M + 1D + 7a* for twisted Edwards curves and finally the cost of binary Edwards curve is: The computational cost of addition and doubling in projective coordinates are *21M + 1S + 4D* and *2M + 6S + 3D*, respectively. And the mixed addition formulae lead to a total cost of 13M + 3S + 3D that can be obtained by $(X_3 : Y_3 : Z_3) = (X_1 : Y_1 : Z_1) + (x_2, y_2)$, where $(X_1 : Y_1 : Z_1)$ and (x_2, y_2) on $E_{B,d_1,d_2}(F)$.

References

[1] Bernstein D. and Lange T. (2007), "Faster addition and doubling on elliptic curves", Progress in Cryptology – Africacrypt-2007, Lecture Notes in Computer Science Vol. 4833, Springer, pp.29-50.

[2] Bernstein D. and Lange T. (2007), "Inverted Edwards coordinates, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes", 17th International Symposium - AAECC-17, Lecture Notes in Computer Science Vol. 4851, Springer, pp. 20-27.

[3] Arenea C., Lange T., Naehrig M., Ritzenthaler C. (2011), "Faster Computation of the Tate Pairing", Journal of Number Theory, 131(5), pp. 842-857.
[4] Bernstein D., Birkner P., Joye M., Lange T. and Peters C. (2008), "Twisted Edwards curves", Progress in Cryptology : Africacrypt-2008, Lecture Notes in Computer Science Vol. 5023, Springer, pp. 389-405.
[5] Christopher Doche and Laurent Imber (2006), "Extended dounle-base number system with applications to elliptic curve cryptography", INDOCRYPT 2006, Springer-Verlag Berlin Heidelberg, LNCS 4329,pp.335-348.
[6] De Miguel, De Santos M., Sanchez-Avila C. and Sachez-Reillo R. (2004), "Elliptic curve cryptography on constraint environments", Proceedings of the international Garnahan conference on Security Technology, 11-14-Oct. 2004, pp.212-220.
[7] Feng R., Nie M. and Wu H. (2009), "Twisted Jacobi Intersections Curves", available at http:// eprint.iacr. org/ 2009/597.pdf.
[8] Gustavsen T. S. and Ranestad K. (2006), "A Simple Point Counting Algorithm for Hessian Elliptic Curves in Characteristic Three", Appl. Algebra Eng. Commun. Comput. 17(2), pp. 141-150.
[9] Jarvinen K, Tommiska M. and Skytta J. (2004), "A scalable architecture for elliptic curve point multiplication", Proceedings of IEEE international conference on Field-Programmable Technology, pp.303-306.
[10] Jia Xiangyu and Xang Chao (2005), "The application of elliptic curve cryptosystem in wireless communication", Proceedings of the international symposium on Microwave, Antenna, Propagation and EMC technologies for wireless communications : MAPE 2005, 8-12 Aug 2005, col 2, pp.1602-1605.
[11] John M. Pollard (1978), "Monte Carlo methods for index computation (mod p)", Mathematics of Computations, Vol. 32, No. 143, pp. 918-924.
[12] Joong Chul Yoon, Seok Won Jung and Sungwoo Lee (2004), "Architecture for an Elliptic curve scalar multiplication resistant to some side-channel attacks", Lecture Notes on Computer Science, Springer Berlin/Heidelberg, vol.2971/2004,pp.139-151.
[13] Smart N. and Westwood E. J. (2003), "Point Multiplication on Ordinary Elliptic Curves over Fields of Characteristic Three", Appl. Algebra Eng. Commun. Comput. 13(6), pp. 485-497.

