Twisted Jacobi Intersections Curves

Rongquan Feng[1], Menglong Nie[1], Hongfeng Wu[2]

[1]LMAM, School of Mathematical Sciences, Peking University,
Beijing 100871, P.R. China

[2]Academy of Mathematics and Systems Science, Chinese Academy of Sciences,
Beijing 100190, P.R. China

fengrq@math.pku.edu.cn, hustnml@163.com, whfmath@gmail.com

Abstract

In this paper, the twisted Jacobi intersections which contains Jacobi intersections as a special case is introduced. We show that every elliptic curve over the prime field with three points of order 2 is isomorphic to a twisted Jacobi intersections curve. Some fast explicit formulae for twisted Jacobi intersections curves in projective coordinates are presented. These explicit formulae for addition and doubling are almost as fast as the Jacobi intersections. In addition, the scalar multiplication can be more effective in twisted Jacobi intersections than in Jacobi intersections. Moreover, we propose new addition formulae which are independent of parameters of curves and more effective in reality than the previous formulae in the literature.

Keywords: elliptic curves, Jacobi intersections, twisted Jacobi intersections, scalar multiplication, isomorphic

1 Introduction

Elliptic curve cryptosystems were proposed by Miller (1986) and by Koblitz (1987) which relies on the difficulty of elliptic curve discrete logarithmic problem. One of the main operations and challenges in elliptic curve cryptosystem is the scalar multiplication. The speed of scalar multiplication plays an important role in the efficiency of the whole system. Elliptic curves can be represented in different forms. To obtain faster scalar multiplications, several elliptic curve representations have been considered in the last two decades. The detail of previous works can be find in [1, 3, 7].

Jacobi intersections curve is the intersection of two quadratic surfaces in three dimensional space with a point on it. The scalar multiplication on Jacobi intersections show competitive efficiency in scalar multiplication, such as faster doubling and tripling operations. Chudnovsky and Chudnovsky [5] proposed first fast doubling and addition formulae for Jacobi intersections in projective coordinates. Liardet and Smart [8], and [1] presented slightly faster formulae. Hisil etc. [6] presented faster tripling formulae. Some slightly faster formulae with a trick can also be found in [7].

In this paper, the Jacobi intersections is generalized to "twisted Jacobi intersections" which contains Jacobi intersections as a special case. It is show that every elliptic curve over the prime field with three points of order 2 is isomorphic to a twisted Jacobi intersections curve. Some fast explicit formulae for twisted Jacobi intersections curves in projective coordinates are presented. These explicit formulae for addition and doubling are almost as fast in the general case as they are for the Jacobi intersections. In addition, the scalar multiplication can be more effective in twisted Jacobi intersections than in Jacobi intersections. Moreover, we propose new addition formulae which are independent of parameters of curves and more effective in reality than the previous formulae in the literature.

This paper is organized as follows. In Section 2, the Jacobi intersections is reviewed, the twisted Jacobi intersections is introduced, and each twisted Jacobi intersections is a twist of a Jacobi intersections is proved. It is shown that every elliptic curve over the prime field with three points of order 2 is isomorphic to a twisted Jacobi intersections curve. In Section 3, the Jacobi intersections addition law is generalized to that for the twisted Jacobi intersections curves, and the explicit addition formulae and formulae independent of parameters of curves are proposed. The Jacobi versus twisted Jacobi is given in Section 4, and the conclusion is in Section 5.

2 Jacobi intersections and Twisted Jacobi Intersections

In this section we briefly review Jacobi intersections curves and the Jacobi intersections addition law. We then introduce twisted Jacobi intersections curves and discuss their relations to Jacobi intersections curves.

Jacobi intersections.

Throughout the paper we consider elliptic curves over a non-binary field K, i.e., a field K whose characteristic is not 2.

A Jacobi intersection form elliptic curve over K is defined by

$$\begin{cases} u^2 + v^2 = 1 \\ bu^2 + w^2 = 1, \end{cases}$$

where $b \in K$ with $b(1-b) \neq 0$. A point (u, v, w) on a Jacobi intersections curve is represented as $(U : V : W : Z)$ satisfying

$$U^2 + V^2 = Z^2, \;\; bU^2 + W^2 = Z^2$$

and $(u, v, w) = (U/Z, V/Z, W/Z)$. Here $(U : V : W : Z) = (\lambda U : \lambda V : \lambda W : \lambda Z)$ for any nonzero $\lambda \in K$. The negative of $(U : V : W : Z)$ is $(-U : V : W : Z)$. The neutral element $(0, 1, 1)$ is represented as $(0 : 1 : 1 : 1)$. The reader is refereed to [5] for more details on Jacobi intersections curves.

The affine version of the unified addition formulae, i.e., that can handle generic doubling, simplifying protection against side-channel attacks, are given by

$$(u_3, v_3, w_3) = (u_1, v_1, w_1) + (u_2, v_2, w_2),$$

where

$$u_3 = \frac{u_1v_2w_2 + u_2v_1w_1}{v_2^2 + u_2^2w_1^2}, \;\; v_3 = \frac{v_1v_2 - u_1w_1u_2w_2}{v_2^2 + u_2^2w_1^2}, \;\; w_3 = \frac{w_1w_2 - bu_1v_1u_2v_2}{v_2^2 + u_2^2w_1^2}.$$

The point addition formulae in projective homogenous coordinates are given by

$$(U_3 : V_3 : W_3 : Z_3) = (U_1 : V_1 : W_1 : Z_1) + (U_2 : V_2 : W_2 : Z_2),$$

where

$$\begin{aligned} U_3 &= U_1Z_1V_2W_2 + V_1W_1U_2Z_2, \;\; V_3 = V_1Z_1V_2Z_2 - U_1W_1U_2W_2 \\ W_3 &= W_1Z_1W_2Z_2 - bU_1V_1U_2V_2, \; Z_3 = Z_1^2V_2^2 + U_2^2W_1^2. \end{aligned}$$

Twisted Jacobi Intersections.

Definition 1. *A twisted Jacobi intersection form elliptic curve over K is defined by*

$$\begin{cases} au^2 + v^2 = 1 \\ bu^2 + w^2 = 1, \end{cases}$$

where $a, b \in K$ with $ab(a-b) \neq 0$. A Jacobi intersection elliptic curve is a twisted Jacobi intersection curve with $a = 1$.

The twisted Jacobi intersection curve $E_{a,b}: \ au^2+v^2 = 1, \ bu^2+w^2 = 1$ is a quadratic twist of the Jacobi intersection curve $E_{1,b/a}: \ \bar{u}^2+\bar{v}^2 = 1, \ (b/a)\bar{u}^2+\bar{w}^2 = 1$. The map $(u,v,w) \mapsto (\bar{u}/\sqrt{a}, \bar{v}, \bar{w})$ is an isomorphism from $E_{a,b}$ to $E_{1,b/a}$ over $K(\sqrt{a})$. Thus if a is a square in K then $E_{a,b}$ is isomorphic to $E_{1,b/a}$ over K. More generally, $E_{a,b}$ is a quadratic twist of $E_{\bar{a},\bar{b}}$ for any $\bar{a}, \bar{b}$ satisfying $\bar{b}/\bar{a} = b/a$. Conversely, every quadratic twist of a twisted Jacobi intersection curve is isomorphic to a twisted Jacobi intersection curve, i.e., the set of isomorphism classes of twisted Jacobi intersection curves is invariant under quadratic twists.

Every twisted Jacobi intersection curve $E_{a,b}: \ au^2+v^2 = 1, \ bu^2+w^2 = 1$ is birationally equivalent to a Jacobi quartic elliptic curve $E_{4,\epsilon,\delta}: \ y^2 = \epsilon x^4 + 2\delta x^2 + 1$ with $\epsilon = 1/a^2, \delta = (a-2b)/a^2$ under the transformations

$$\begin{cases} x = (v-1)/u, \\ y = w(a+x^2)/a, \end{cases} \quad \text{and} \quad \begin{cases} w = \dfrac{ay}{a+x^2}, \\[2ex] u = \dfrac{(w^2-1)(a+x^2)}{2bx}, \\[2ex] v = 1 + xu. \end{cases}$$

Theorem 1. *Let K be a field with char$(K) \neq 2$ and $E_{a,b}: \ au^2 + v^2 = 1, \ bu^2 + w^2 = 1$ be a twisted Jacobi intersection form curve define over K with $ab(a-b) \neq 0$. Then $E_{a,b}$ is a smooth curve and isomorphic to an elliptic curve of the form $E: y^2 = x(x-a)(x-b)$ over K.*

Proof. The proof is given in Appendix. $\square$

Theorem 2. *Let K be a field with char$(K) \neq 2$. Then every elliptic curve over K having three K-rational points of order 2 is isomorphic to a twisted Jacobi intersections curve.*

Proof. Let E be an elliptic curve over K having three $K-$rational points of order 2. Let $(\theta_1, 0), (\theta_2, 0)$ and $(\theta_3, 0)$ be these three distinct points of order 2 on the Weierstrass curve E, i.e., $y^2 = x^3 + a_2x^2 + a_4x + a_6 = (x - \theta_1)(x - \theta_2)(x - \theta_3)$. Replacing (x, y) by $(x + \theta_1, y)$ yields the equation of the form $y^2 = x(x - a)(x - b)$, where $a = \theta_2 - \theta_1, b = \theta_3 - \theta_1$. Therefore every elliptic curve over K having three $K-$rational points of order 2 is isomorphic to a twisted Jacobi intersections curve by Theorem 1. □

3 Arithmetic on Twisted Jacobi Intersections

Let K be a non-binary field. In this section we present fast explicit formulae for addition and doubling on twisted Jacobi intersections curves over K.

Theorem 3. *Let $P = (u_1, v_1, w_1),\ Q = (u_2, v_2, w_2)$ be two points on a twisted Jacobi intersections elliptic curve $E_{a,b}:\ au^2 + v^2 = 1,\ bu^2 + w^2 = 1$, and let $R = P + Q := (u_3, v_3, w_3)$. Then the affine version of the unified addition formulae are given by*

$$u_3 = \frac{u_1v_2w_2 + u_2v_1w_1}{v_2^2 + au_2^2w_1^2},\ v_3 = \frac{v_1v_2 - au_1w_1u_2w_2}{v_2^2 + au_2^2w_1^2},\ w_3 = \frac{w_1w_2 - bu_1v_1u_2v_2}{v_2^2 + au_2^2w_1^2}.$$

Especially, if $P = Q$ and $R = 2P := (u_3, v_3, w_3)$, then

$$u_3 = \frac{2u_1v_1w_1}{v_1^2 + au_1^2w_1^2},\ v_3 = \frac{v_1^2 - au_1^2w_1^2}{v_1^2 + au_1^2w_1^2},\ w_3 = \frac{w_1^2 - bu_1^2v_1^2}{v_1^2 + au_1^2w_1^2}.$$

The identity element is $(0, 1, 1)$. The negative of the point (u, v, w) is $(-u, v, w)$.

Proof. For the correctness of the addition law, observe that it coincides with the Jacobi intersections addition law on

$$\bar{u}^2 + v^2 = 1,\ \frac{b}{a}\bar{u}^2 + w^2 = 1,$$

with $\bar{u} = \sqrt{a}u$. These formulae also work for doubling. □

Theorem 4. *Let K be a field of odd characteristic. Let $E_{a,b}:\ au^2 + v^2 = 1, bu^2 + w^2 = 1$ be a twisted Jacobi intersections curve over K. Let $P = (u_1, v_1, w_1)$ and $Q = (u_2, v_2, w_2)$ be points on $E_{a,b}$. If ab is not a square in K, or if -1 is a square in K and neither a nor b is a square in K, then $v_2^2 + au_2^2w_1^2 \neq 0$.*

Proof. If $v = w = 0$, then $au^2 = bu^2$ and $a = b$, therefore ab is a square in K, contradict to ab is not a square in K. Therefore at most one in $\{u, v, w\}$ is equal to 0 for a point (u, v, w) on $E_{a,b}$. Thus if $u_2 = 0$, then $v_2^2 + au_2^2w_1^2 = v_2^2 \neq 0$. If $u_1 = 0$, then $w_1^2 = 1$, and $v_2^2 + au_2^2w_1^2 = v_2^2 + au_2^2 = 1$. Let $u_1u_2 \neq 0$, assume that ab is not a square in K. If $v_2^2 + au_2^2w_1^2 = 0$, then $au_2^2 + v_2^2 - (v_2^2 + au_2^2w_1^2) = au_2^2(1 - w_1^2) = 1$. Thus $1 - w_1^2 = 1/au_2^2 = bu_1^2$. therefore $ab = (1/u_1u_2)^2$ is a square in K, contradict to the assumption. Now assume that neither a nor b is a square in K, then $w_1v_2 \neq 0$. If $v_2^2 + au_2^2w_1^2 = 0$, then $a = -(v_2/u_2w_1)^2$ is square in K since -1 is a square in K, which is a contradiction. □

Note that the Theorem 4 shows that if ab is not a square in K, then the twisted addition formulae is complete. But generally, both a and b are non-squares in K. Therefore ab is not a square in K is not a reasonable assumption when $a \neq 1$. But in this case, if -1 is a square in K, then the above twisted addition formulae is also complete.

When using projective homogenous coordinates to eliminate field inversions, each point is represented by the quadruplet $(U : V : W : Z)$ which satisfies the equations

$$aU^2 + V^2 = Z^2,\ bU^2 + W^2 = Z^2,$$

and corresponds to the affine point $(U/Z,\ V/Z,\ W/Z)$ with $Z \neq 0$.

Theorem 5. *Let $P = (U_1 : V_1 : W_1 : Z_1),\ Q = (U_2 : V_2 : W_2 : Z_2)$ be two points on the twisted Jacobi intersections elliptic curve $E_{a,b}:\ aU^2 + V^2 = Z^2,\ bU^2 + W^2 = Z^2$, and let $R = P + Q := (U_3 : V_3 : W_3 : Z_3)$. Then the projective version of the unified addition formulae are given by*

$$\begin{aligned} U_3 &= U_1Z_1V_2W_2 + V_1W_1U_2Z_2,\quad V_3 = V_1Z_1V_2Z_2 - aU_1W_1U_2W_2, \\ W_3 &= W_1Z_1W_2Z_2 - bU_1V_1U_2V_2,\ Z_3 = Z_1^2V_2^2 + aU_2^2W_1^2. \end{aligned}$$

The identity element is $(0 : 1 : 1 : 1)$. The negative of the point $(U : V : W : Z)$ is $(-U : V : W : Z)$. □

Note that $Z_1^2(Z_2^2 - V_2^2) = aZ_1^2U_2^2$ and $aU_2^2(bU_1^2 + W_1^2) = aU_2^2Z_1^2$. We have $Z_1^2V_2^2 + aU_2^2W_1^2 = Z_1^2Z_2^2 - abU_1^2U_2^2$ which can be used to simplify the formulae.

Especially, the above theorem gives the following doubling formulae.

$$\begin{aligned} U_3 &= 2U_1V_1W_1Z_1, \qquad V_3 = V_1^2Z_1^2 - aU_1^2W_1^2, \\ W_3 &= W_1^2Z_1^2 - bU_1^2V_1^2, \quad Z_3 = V_1^2Z_1^2 + aU_1^2W_1^2. \end{aligned}$$

Note that $bU_1^2 = Z_1^2 - W_1^2$, and $V_1^2W_1^2 = W_1^2(Z_1^2 - aU_1^2) = W_1^2Z_1^2 - aU_1^2W_1^2$. We have the second doubling formulae

$$\begin{aligned} U_3 &= 2U_1V_1W_1Z_1, \; V_3 = V_1^2Z_1^2 - aU_1^2W_1^2, \\ W_3 &= 2W_1^2Z_1^2 - V_1^2Z_1^2 - aU_1^2W_1^2, \qquad (1) \\ Z_3 &= V_1^2Z_1^2 + aU_1^2W_1^2. \end{aligned}$$

Moreover, from

$$\begin{aligned} W_1^2Z_1^2 - bU_1^2V_1^2 &= W_1^2(aU_1^2 + V_1^2) - (Z_1^2 - W_1^2)V_1^2 = aU_1^2W_1^2 + 2V_1^2W_1^2 - V_1^2Z_1^2 \\ &= aU_1^2W_1^2 - V_1^2Z_1^2 + 2W_1^2(bU_1^2 + W_1^2 - aU_1^2) \\ &= aU_1^2W_1^2 - V_1^2Z_1^2 + 2bW_1^2U_1^2 + 2W_1^4 - 2aU_1^2W_1^2 \\ &= -aU_1^2W_1^2 - V_1^2Z_1^2 + 2(bU_1^2W_1^2 + W_1^4), \end{aligned}$$

we have the third doubling formulae

$$\begin{aligned} U_3 &= 2U_1V_1W_1Z_1, \; V_3 = V_1^2Z_1^2 - aU_1^2W_1^2, \\ W_3 &= -aU_1^2W_1^2 - V_1^2Z_1^2 + 2(bU_1^2W_1^2 + W_1^4), \qquad (2) \\ Z_3 &= V_1^2Z_1^2 + aU_1^2W_1^2. \end{aligned}$$

Addition in Projective Coordinates. By Theorem 5, the following formulae compute $(U_3 : V_3 : W_3 : Z_3) = (U_1 : V_1 : W_1 : Z_1) + (U_2 : V_2 : W_2 : Z_2)$ in $13M + 2S + 5D$ costs, i.e., 13 field multiplications, 2 squarings and 5 multiplications by the curve constant a and b, or in $14M + S + 4D$ costs. We denote the two algorithms by "AProjective.1" and "AProjective.2".

$$\begin{aligned}
A &= U_1V_1;\ B = W_1Z_1;\ C = U_2V_2;\ D = W_2Z_2;\ E = U_1W_2; \\
F &= V_1Z_2;\ G = W_1U_2;\ H = Z_1V_2;\ J = AD;\ K = BC; \\
U_3 &= (H+F)(E+G) - J - K; \\
V_3 &= (H+E)(F-aG) - J + aK; \\
W_3 &= (B-bA)(C+D) + bJ - K; \\
Z_3 &= H^2 + a\cdot G^2 = H^2 + aG\cdot G.
\end{aligned}$$

If the points represented by the sextuplet (U, V, W, Z, UV, WZ), then the addition formula can by modified by: $(U_3 : V_3 : W_3 : Z_3 : A_3 : B_3) = (U_1 : V_1 : W_1 : Z_1 : A_1 : B_1) + (U_2 : V_2 : W_2 : Z_2 : A_2 : B_2)$, where $A_1 = U_1V_1, B_1 = W_1Z_1, A_2 = U_2V_2, B_2 = W_2Z_2$. The cost are $11M+2S+5D$ or $12M + S + 4D$. We denote the two algorithms bye "MProjective.1" and "MProjective.2".

$$\begin{aligned}
C &= U_1W_2; D = V_1Z_2; E = W_1U_2; F = Z_1V_2; G = A_1B_2; H = B_1A_2; \\
U_3 &= (D+F)(C+E) - G - H; \\
V_3 &= (C+F)(D-aE) - G + aH; \\
W_3 &= (B_1 - bA_1)(A_2+B_2) + bG - H; \\
Z_3 &= F^2 + a\cdot E^2 = F^2 + aE\cdot E; \\
A_3 &= U_3V_3; B_3 = W_3Z_3.
\end{aligned}$$

Note that, if $a = \varepsilon^2$ is a square element in the field, then $Z_3 = (F + \varepsilon E)^2 - 2\varepsilon H$, the cost is $11M + 1S + 6D$.

Doubling 1 in Projective Coordinates. The following formulae compute $(U_3 : V_3 : W_3 : Z_3) = 2(U_1 : V_1 : W_1 : Z_1)$ in $3M + 4S + 1D$ by using formulae (1), where the $1D$ is a multiplication by a:

$$\begin{aligned}
A &= V_1Z_1;\ B = A^2;\ C = U_1W_1;\ D = C^2;\ E = 2(W_1Z_1)^2; \\
U_3 &= (A+C)^2 - B - D;\ V_3 = B - aD; \\
W_3 &= E - B - aD;\ Z_3 = B + aD.
\end{aligned}$$

Doubling 2 in Projective Coordinates. The following formulae compute $(U_3 : V_3 : W_3 : Z_3) = 2(U_1 : V_1 : W_1 : Z_1)$ in $2M + 5S + 2D$ by using formulae (2), where the $2D$ are multiplications by a and by b:

$$\begin{aligned}
A &= V_1Z_1;\ B = A^2;\ C = U_1W_1;\ D = C^2;\ E = W_1^4; \\
U_3 &= (A+C)^2 - B - D;\ V_3 = B - aD; \\
W_3 &= 2(bD+E) - B - aD;\ Z_3 = B + aD.
\end{aligned}$$

Doubling 1 in Projective Coordinates with $Z_1 = 1$. The following formulae compute $(U_3 : V_3 : W_3 : Z_3) = 2(U_1 : V_1 : W_1 : 1)$ in $1M + 4S + 1D$ by using formulae (1), where the $1D$ is a multiplication by a:

$$\begin{aligned}
A &= V_1;\ B = A^2;\ C = U_1W_1;\ D = C^2;\ E = 2W_1^2;\\
U_3 &= (A + C)^2 - B - D;\ V_3 = B - aD;\\
W_3 &= E - B - aD;\ Z_3 = B + aD.
\end{aligned}$$

Doubling 2 in Projective Coordinates with $Z_1 = 1$. The following formulae compute $(U_3 : V_3 : W_3 : Z_3) = 2(U_1 : V_1 : W_1 : 1)$ in $1M + 5S + 2D$ by using formulae (2), where the $2D$ are multiplications by a and by b:

$$\begin{aligned}
A &= V_1;\ B = A^2;\ C = U_1W_1;\ D = C^2;\ E = W_1^4;\\
U_3 &= (A + C)^2 - B - D;\ V_3 = B - aD;\\
W_3 &= 2(bD + E) - B - aD;\ Z_3 = B + aD.
\end{aligned}$$

Note that $V_1^2Z_1^2 = Z_1^2(Z_1^2 - aU_1^2) = Z_1^4 - aU_1^2Z_1^2$, $U_1^2W_1^2 = U_1^2(Z_1^2 - bU_1^2) = U_1^2Z_1^2 - bU_1^4$ and $W_1^4 = (Z_1^2 - bU_1^2)^2 = Z_1^4 + b^2U_1^4 - 2bU_1^2Z_1^2$. We have the following doubling formulae:

$$\begin{aligned}
U_3 &= 2U_1Z_1V_1W_1,\ V_3 = abU_1^4 - 2aU_1^2Z_1^2 + Z_1^4,\\
W_3 &= abU_1^4 - 2bU_1^2Z_1^2 + Z_1^4,\ Z_3 = Z_1^4 - abU_1^4.
\end{aligned} \tag{3}$$

Doubling 3 in Projective Coordinates with $Z_1 = 1$. The following formulae compute $(U_3 : V_3 : W_3 : Z_3) = 2(U_1 : V_1 : W_1 : 1)$ in $2M + 2S + 3D$ by using formulae (3), where the $3D$ are multiplications by a, b, ab:

$$\begin{aligned}
A &= U_1^2;\ B = A^2;\ C = Z_1^2;\ D = C^2;\ E = (U_1 + Z_1)^2 - A - C;\\
F &= (A + C)^2 - B - D;\ G = abB;\\
U_3 &= V_1W_1E;\ V_3 = G - aF + D;\\
W_3 &= G - bF + D;\ Z_3 = D - G.
\end{aligned}$$

The comparison of the costs of above doubling formulae in this paper to those in previous works is listed in Table 1.

Doubling formulae independent of a and b. From $aU_1^2 = Z_1^2 - V_1^2$ and $bU_1^2 = Z_1^2 - W_1^2$, we have the following doubling formulae which are

Table 1: Algorithm comparison with other algorithms in Doubling

Coordinates	Source of algorithms	Doubling	Doubling($Z_1 = 1$)
Jacobi Intersections	[8]	4M+3S	-
Jacobi Intersections	[2]	3M+4S	2M+4S
Jacobi Intersections	[6]	2M+5S+1D	-
Twisted Jacobi Intersections	Doubling 1	3M+4S+1D	1M+4S+1D
Twisted Jacobi Intersections	Doubling 2	2M+5S+2D	1M+5S+2D
Twisted Jacobi Intersections	Doubling 3	2M+6S+3D	2M+2S+3D

independent of the parameters a and b:

$$\begin{aligned} U_3 &= 2U_1V_1W_1Z_1,\ V_3 = V_1^2Z_1^2 - Z_1^2W_1^2 + V_1^2W_1^2, \\ W_3 &= W_1^2Z_1^2 - V_1^2Z_1^2 + V_1^2W_1^2,\ Z_3 = V_1^2Z_1^2 + Z_1^2W_1^2 - V_1^2W_1^2. \end{aligned}$$

Addition formulae independent of a and b

Theorem 6. *Let $P = (u_1, v_1, w_1),\ Q = (u_2, v_2, w_2)$ be two different points on the twisted Jacobi intersections elliptic curve $E_{a,b}:\ au^2 + v^2 = 1,\ bu^2 + w^2 = 1$, and let $R = P + Q = (u_3, v_3, w_3)$. Then the addition formulae can be given by*

$$u_3 = \frac{u_1^2 - u_2^2}{u_1v_2w_2 - v_1w_1u_2},\ v_3 = \frac{u_1v_1w_2 - w_1u_2v_2}{u_1v_2w_2 - v_1w_1u_2},\ w_3 = \frac{u_1w_1v_2 - v_1u_2w_2}{u_1v_2w_2 - v_1w_1u_2}.$$

Proof. From

$$\begin{aligned} &(u_1^2 - u_2^2)(v_2^2 + au_2^2w_1^2) = u_1^2v_2^2 + au_1^2w_1^2u_2^2 - u_2^2v_2^2 - au_2^2u_2^2w_1^2 \\ &= u_1^2v_2^2 + (1 - v_1^2)w_1^2u_2^2 - u_2^2v_2^2 - (1 - v_2^2)u_2^2w_1^2 \\ &= u_1^2v_2^2 - u_2^2v_2^2 + u_2^2v_2^2w_1^2 - v_1^2w_1^2u_2^2 \\ &= u_1^2v_2^2 - u_2^2v_2^2(1 - w_1^2) - v_1^2w_1^2u_2^2 \\ &= u_1^2v_2^2 - bu_1^2u_2^2v_2^2 - v_1^2w_1^2u_2^2 \\ &= u_1^2v_2^2(1 - bu_2^2) - v_1^2w_1^2u_2^2 \\ &= u_1^2v_2^2w_2^2 - v_1^2w_1^2u_2^2 \\ &= (u_1v_2w_2 + v_1w_1u_2)(u_1v_2w_2 - v_1w_1u_2), \end{aligned}$$

we have

$$\frac{u_1^2-u_2^2}{u_1v_2w_2-v_1w_1u_2}=\frac{u_1v_2w_2+v_1w_1u_2}{v_2^2+au_2^2w_1^2}.$$

From

$$\begin{aligned}
&(u_1v_1w_2-w_1u_2v_2)(u_1v_2w_2+v_1w_1u_2)\\
&=u_1^2v_1v_2w_2^2+u_1u_2v_1^2w_1w_2-u_1u_2v_2^2w_1w_2-u_2^2v_1v_2w_1^2\\
&=u_1^2v_1v_2(1-bu_2^2)+u_1u_2w_1w_2(1-au_1^2)-u_1u_2(1-au_2^2)w_1w_2-u_2^2v_1v_2(1-bu_1^2)\\
&=u_1^2v_1v_2-au_1^2u_1u_2w_1w_2-u_2^2v_1v_2+au_2^2u_1u_2w_1w_2\\
&=(u_1^2-u_2^2)(v_1v_2-au_1w_1u_2w_2),
\end{aligned}$$

we have

$$\frac{v_1v_2-au_1w_1u_2w_2}{v_2^2+au_2^2w_1^2}=\frac{(u_1v_1w_2-w_1u_2v_2)(u_1v_2w_2+v_1w_1u_2)}{(u_1^2-u_2^2)(v_2^2+au_2^2w_1^2)}$$

$$=\frac{u_1v_1w_2-w_1u_2v_2}{\dfrac{(u_1^2-u_2^2)(v_2^2+au_2^2w_1^2)}{u_1v_2w_2+v_1w_1u_2}}=\frac{u_1v_1w_2-w_1u_2v_2}{u_1v_2w_2-v_1w_1u_2}.$$

Again, from

$$\begin{aligned}
&(u_1w_1v_2-v_1u_2w_2)(u_1v_2w_2+v_1w_1u_2)\\
&=u_1^2w_1w_2v_2^2+u_1u_2v_1v_2w_1^2-u_1u_2v_1v_2w_2^2-u_2^2v_1^2w_1w_2\\
&=u_1^2w_1w_2(1-au_2^2)+u_1u_2v_1v_2(1-bu_1^2)-u_1u_2v_1v_2(1-bu_2^2)-u_2^2w_1w_2(1-au_1^2)\\
&=u_1^2w_1w_2-bu_1^2u_1v_1u_2v_2-u_2^2w_1w_2+bu_2^2u_1v_1u_2v_2\\
&=(u_1^2-u_2^2)(w_1w_2-bu_1v_1u_2v_2),
\end{aligned}$$

we have

$$\frac{w_1w_2-bu_1v_1u_2v_2}{v_2^2+au_2^2w_1^2}=\frac{(u_1w_1v_2-v_1u_2w_2)(u_1v_2w_2+v_1w_1u_2)}{(u_1^2-u_2^2)(v_2^2+au_2^2w_1^2)}$$

$$=\frac{u_1w_1v_2-v_1u_2w_2}{\dfrac{(u_1^2-u_2^2)(v_2^2+au_2^2w_1^2)}{u_1v_2w_2+v_1w_1u_2}}=\frac{u_1w_1v_2-v_1u_2w_2}{u_1v_2w_2-v_1w_1u_2}.$$

The theorem follows from Theorem 3. $\square$

The formulae fail for point doubling. In addition, there are exceptional cases. For example, when $2P = 2Q$, then the formulae cannot work. The above formulae in projective homogenous coordinates are given by the following theorem.

Theorem 7. *Let $P = (U_1 : V_1 : W_1 : Z_1)$, $Q = (U_2 : V_2 : W_2 : Z_2)$ be two different points on the twisted Jacobi intersections elliptic curve $E_{a,b}: aU^2 + V^2 = Z^2$, $bU^2 + W^2 = Z^2$, and let $R = P + Q = (U_3 : V_3 : W_3 : Z_3)$. Then the addition formulae can be given by*

$$\begin{aligned} U_3 &= U_1^2 Z_2^2 - Z_1^2 U_2^2,\ V_3 = U_1 V_1 W_2 Z_2 - W_1 Z_1 U_2 V_2, \\ W_3 &= U_1 W_1 V_2 Z_2 - V_1 Z_1 U_2 W_2,\ Z_3 = U_1 Z_1 V_2 W_2 - V_1 W_1 U_2 Z_2. \end{aligned}$$

The projective addition formulae in Theorems 5 and 7 have exceptional points in each case. But the following theorem tells us that the formulae together in Theorems 5 and 7 cover all points.

Theorem 8. *Let $P = (U_1 : V_1 : W_1 : Z_1)$, $Q = (U_2 : V_2 : W_2 : Z_2)$ be two points on the twisted Jacobi intersections elliptic curve $E_{a,b}: aU^2 + V^2 = Z^2$, $bU^2 + W^2 = Z^2$ defined over K with $ab(a-b) \neq 0$, let $R = (U_3 : V_3 : W_3 : Z_3)$ and $S = (U_3' : V_3' : W_3' : Z_3')$, where*

$$\begin{aligned} U_3 &= U_1 Z_1 V_2 W_2 + V_1 W_1 U_2 Z_2, \quad V_3 = V_1 Z_1 V_2 Z_2 - aU_1 W_1 U_2 W_2, \\ W_3 &= W_1 Z_1 W_2 Z_2 - bU_1 V_1 U_2 V_2,\ Z_3 = Z_1^2 V_2^2 + aU_2^2 W_1^2, \end{aligned}$$

and

$$\begin{aligned} U_3' &= U_1^2 Z_2^2 - Z_1^2 U_2^2, & V_3' &= U_1 V_1 W_2 Z_2 - W_1 Z_1 U_2 V_2, \\ W_3' &= U_1 W_1 V_2 Z_2 - V_1 Z_1 U_2 W_2, & Z_3' &= U_1 Z_1 V_2 W_2 - V_1 W_1 U_2 Z_2. \end{aligned}$$

Then $P + Q = R = S$ if $R = S$, and $P + Q = R$ (or S) if $S = 0$ (or $R = 0$).

Proof. If $R \neq (0, 0, 0, 0)$, then $R \in E_{a,b}$ and $P + Q = R$. Similarly, if $S \neq (0, 0, 0, 0)$, then $S \in E_{a,b}$ and $P + Q = S$. Now assume $R = S = (0, 0, 0, 0)$. Then $U_1 Z_1 V_2 W_2 + V_1 W_1 U_2 Z_2 = 0$ and $U_1 Z_1 V_2 W_2 - V_1 W_1 U_2 Z_2 = 0$. Thus $U_1 Z_1 V_2 W_2 = V_1 W_1 U_2 Z_2 = 0$.

If $U_1 = 0$, then $Z_1^2 U_2^2 = 0$ since $U_1^2 Z_2^2 - Z_1^2 U_2^2 = 0$. Thus $Z_1 = 0$ or $U_2 = 0$. When $Z_1 = 0$, then $V_1 = W_1 = 0$ from $aU^2 + V^2 = Z^2$ and $bU^2 + W^2 = Z^2$.

Therefore $P = (0,0,0,0)$, which is contradict to $P \in E_{a,b}$. When $U_2 = 0$, then $V_1Z_1V_2Z_2 = 0$ from $V_3 = V_1Z_1V_2Z_2 - aU_1W_1U_2W_2 = 0$. We can get $Q = (0,0,0,0)$ by the similar argument as above. Contradict to $Q \in E_{a,b}$.

The similar argument works for the cases when $U_2 = 0$, $Z_1 = 0$, $Z_2 = 0$, $V_2 = 0$, $W_2 = 0$, $V_1 = 0$ or $W_1 = 0$.

If $P \neq Q$, From Theorem 7 we know that $P+Q = R = S$ if $R \neq (0,0,0,0)$ and $S \neq (0,0,0,0)$. □

Remark. The above Theorem give a complete addition laws for the curve $E_{a,b}: aU^2+V^2 = Z^2,\ bU^2+W^2 = Z^2$ defined over K with $ab(a-b) \neq 0$. The addition laws in the theorem cover all possible pairs of points on curves $E_{a,b}$.

New Addition algorithm use Theorem 7. The following formulae compute $(U_3 : V_3 : W_3 : Z_3) = (U_1 : V_1 : W_1 : Z_1) + (U_2 : V_2 : W_2 : Z_2)$ in $15M$, We denote the algorithm by "Independent.1".

$$\begin{aligned}
A &= U_1Z_2;\ B = U_2Z_1;\ C = V_1W_2;\ D = V_2W_1;\\
E &= U_1Z_1;\ F = V_1W_1;\ G = U_2Z_2;\ H = V_2W_2;\\
U_3 &= (A+B)(A-B);\\
V_3 &= AC - BD;\ W_3 = AD - BC;\ Z_3 = EH - FG.
\end{aligned}$$

Note that $U_3 = U_1^2(bU_2^2 + W_2^2) - U_2^2(bU_1^2 + W_1^2) = U_1^2W_2^2 - U_2^2W_1^2$. If the points represented by the sextuplet (U, V, W, Z, UW, VZ), then the addition formula can by modified by: $(U_3 : V_3 : W_3 : Z_3 : M_3 : N_3) = (U_1 : V_1 : W_1 : Z_1 : M_1 : N_1) + (U_2 : V_2 : W_2 : Z_2 : M_2 : N_2)$, where $M_1 = U_1W_1, N_1 = V_1Z_1, M_2 = U_2W_2, N_2 = V_2Z_2$, the cost are $13M$. We denote the algorithm be "MIndependent.2".

$$\begin{aligned}
A &= U_1W_2;\ B = U_2W_1;\ C = V_1Z_2;\ D = V_2Z_1;\\
U_3 &= (A+B)(A-B);\\
V_3 &= AC - BD;\ W_3 = M_1N_2 - M_2N_1;\ Z_3 = AD - BC;\\
M_3 &= U_3W_3, N_3 = V_3Z_3.
\end{aligned}$$

The comparison of the costs of above addition formulae in this paper to those in previous works is listed in Table 2.

Note that, Table 2 show that the addition in twisted Jacobi intersections are almost as fast as that in the Jacobi intersections. The new algorithm based on the formula independent of parameters of curves is more effectively than the best result in literature for Jacobi intersection curves when $D > 0.6M$.

Table 2: Algorithm comparison with other algorithms in addition

Coordinates	Source	Addition	$D=0M$	$S=D=1M$
Jacobi Intersections	[8]	13M+2S+1D	14.6M	16M
Jacobi Intersections	[6](projective)	13M+1S+2D	13.8M	16M
Jacobi Intersections	[6](modified)	11M+1S+2D	11.8M	14M
Twisted Jacobi	AProjective.1	13M+2S+5D	14.6M	20M
Twisted Jacobi	AProjective.2	14M+1S+4D	14.8M	19M
Twisted Jacobi	MProjective.1	11M+2S+5D	12.6M	18M
Twisted Jacobi	MProjective.2	12M+1S+4D	12.8M	17M
Twisted Jacobi(a square)	MProjective.2	11M+1S+6D	11.8M	18M
Twisted Jacobi	Independent.1	15M	15M	15M
Twisted Jacobi	MIndependent.2	13M	13M	13M

4 Jacobi versus Twisted Jacobi

The twisted Jacobi intersection curve is a generalization of Jacobi intersections, and twisted Jacobi intersection curve cover more elliptic curves than Jacobi intersections curves do. An example in [2] shows that for prime $p = 2^{255} - 19$, one multiplication by 121665 and one multiplication by 121666, which together are faster than a multiplication by 20800338683988658368647408995589388737092878452977063003340006470870624536394 $\equiv 121665/121666 \pmod{p}$. That is, for a large parameter b of Jacobi intersections curves $U^2 + V^2 = Z^2,\ bU^2 + W^2 = Z^2$, we can choose smaller a' and b' such that the twisted Jacobi intersections $a'U^2 + V^2 = Z^2,\ b'U^2 + W^2 = Z^2$ is quadratic twisted to it, but can save computation costs. For example, in algorithms MProjective.1, if a, b are smaller and $a = \varepsilon^2$ is a square element in the field, then we can omit the multiplications by the small constants. Thus $Z_3 = F^2 + a \cdot E^2 = (F + \varepsilon E)^2 - 2\varepsilon H$, and the algorithm cost $11M + 1S$, which is more efficient than the algorithm in [6](modified).

5 Conclusion

In this paper, the twisted Jacobi intersections which contains Jacobi intersections as a special case is introduced. We show that every elliptic curve over the prime field with three points of order 2 is isomorphic to a twisted Jacobi intersections curve. Some fast explicit formulae for twisted Jacobi intersections curve in projective coordinates are presented. These explicit formulae for addition and doubling are almost as fast as the Jacobi intersections. In addition, the scalar multiplication can be more effective in twisted Jacobi intersections than in Jacobi intersections. Finally, new addition formulae which are independent of parameters of curves are proposed and it can be more effective than the previous results in literature when $D > 0.6M$. At last, we hope the faster point operation formulae on twist Jacobi intersection can be proposed.

References

[1] D. J. Bernstein, and T. Lange, Explicit-formulae database. URL: http://www.hyperelliptic.org/EFD.

[2] D. J. Bernstein, P. Birkner, M. Joye, T. Lange, and C. Peters, Twisted Edwards curves, In AFRICACRYPT 2008, LNCS 5023, 389-405, Springer, 2008.

[3] D. J. Bernstein and T. Lange, Analysis and optimization of elliptic-curve single-scalar multiplication, Cryptology ePrint Archive, Report 2007/455.

[4] O. Billet and M. Joye, The Jacobi model of an elliptic curve and side-channel analysis, AAECC 2003, LNCS 2643, 34-42, Spriger-Verlag, 2003.

[5] D. V. Chudnovsky, and G. V. Chudnovsky, Sequences of numbers generated by addition in formal groups and new primality and factorization tests, Advances in Applied Mathematics 7(1986), 385-434.

[6] H. Hisil, G. Carter, and Ed Dawson, New formulae for efficient elliptic curve arithmetic, Indocrypt 2007, LNCS 4859, 138-151, Springer, 2007.

[7] H. Hisil, K. Koon-Ho Wong, G. Carter and Ed Dawson, Faster group operations on elliptic curves, In Proc. Seventh Australasian Information Security Conference (AISC 2009), Wellington, New Zealand. CRPIT, 98. Brankovic, L. and Susilo, W., Eds. ACS. 7-19.

[8] P.-Y. Liardet, and N. P. Smart, Preventing SPA/DPA in ECC systems using the Jacobi form, CHES 2001, LNCS 2162, 391-401, Springer, 2001.

[9] Lawrence C. Washington, Elliptic Curves: Number Theory and Cryptography, CRC Press, 2003.

[10] Joseph H. Silverman, The Arithmetic of Elliptic Curves, Springer-Verlag, 1986.

Appendix. Proof of Theorem 1

Proof. Let $\mathcal{V}$ be a projective variety given by the equation

$$\begin{cases} au^2 + v^2 = z^2 \\ bu^2 + w^2 = z^2. \end{cases}$$

Let $P = [u, v, w, z]$ be a point of $\mathcal{V}$. Suppose that $z \neq 0$, then we can consider the equation

$$\begin{cases} au^2 + v^2 = 1 \\ bu^2 + w^2 = 1. \end{cases}$$

Let $Q = (u, v, w)$ be a point on the curve defined by this equation. If the point Q is singular, then the rank of the following matrix cannot be 2.

$$\begin{pmatrix} 2au & 2v & 0 \\ 2bu & 0 & 2w \end{pmatrix}$$

so $-4buv = 4vw = 4auw = 0$, i.e. $uv = vw = uw = 0$. Suppose $u = 0$, then $v^2 = 1, w^2 = 1$, contrary to $vw = 0$, hence $u \neq 0$, so $v = w = 0$. But then $u^2 = a^{-1} = b^{-1}$ contradicts to the condition $a \neq b$. Therefore, there is not any singular point on $\mathcal{V}$ with $z \neq 0$. Similarly we can show that there is not any singular point on $\mathcal{V}$ with $z = 0$ either. So $E_{a,b}$ is a smooth curve.

Next we show that $E_{a,b}$ is isomorphic to an elliptic curve of the form $E : y^2 = x(x - a)(x - b)$.

Let $(u_0, v_0, w_0) = (0, 1, 1)$ be a point on E_{ab}. First, we parameterize the solutions to $au^2 + v^2 = 1$. similar to the Example 2.3 in [9], Let $u = t, v = 1 + mt$. Then we have

$$at^2 + (1 + mt)^2 = 1,$$

which yields $2mt + (a + m^2)t^2 = 0$. Discarding the solution $t = 0$, we obtain $t = -2m/(a + m^2)$, hence

$$u = -\frac{2m}{a + m^2}, v = \frac{a - m^2}{a + m^2}.$$

Since the tangent at this point has slope $m = 0$, that $m = 0$ corresponds to $(u, v) = (0, 1)()$. Substituting into $bu^2 + w^2 = 1$ yields

$$((a + m^2)w)^2 = (a + m^2)^2 - 4bm^2 = m^4 + (2a - 4b)m^2 + a^2.$$

Let $r = (a + m^2)w$, then

$$r^2 = m^4 + 2(a - 2b)m^2 + a^2.$$

Let

$$x = \frac{2a(r + a)}{m^2}, y = \frac{4a^2(r + a) + 4a(a - 2b)m^2}{m^3}.$$

By Theorem 2.17 in [9] with $q = a$, the formulae then change this curve to the Weierstrass equation

$$y^2 = x^3 + 2(a - 2b)x^2 - 4a^2x - 8a^2(a - 2b) = (x + 2a)(x - 2a)(x + 2a - 4b).$$

The inverse transformation is

$$m = \frac{2a(x + 2a - 4b)}{y}, r = -a + \frac{m^2 x}{2a}.$$

The point $(m, r) = (0, a)$ corresponds to the point $(x, y) = \infty$ and $(m, r) = (0, -a)$ corresponds to $(x, y) = (4b - 2a, 0)$. To synthesize the forward two steps, we obtain the following transformation.

$$\varphi : \begin{cases} x = \frac{2a(\frac{au^2+(v-1)^2}{u^2}w+a)}{\frac{(v-1)^2}{u^2}} = \frac{2(au)^2(w+1)}{(v-1)^2} + 2aw \\ y = \frac{4a^2(\frac{au^2+(v-1)^2}{u^2}w+a)+4a(a-2b)(\frac{v-1}{u})^2}{\frac{(v-1)^3}{u^3}} = \frac{2au}{v-1}(\frac{2(au)^2(w+1)}{(v-1)^2} + 2aw + 2a - 4b). \end{cases}$$

The inverse transformation is

$$\psi:\begin{cases} u &= -\dfrac{\frac{4a(x+2a-4b)}{y}}{a+\frac{4a^2(x+2a-4b)^2}{y^2}} &= -\dfrac{4y(x+2a-4b)}{y^2+4a(x+2a-4b)^2} \\ v &= \dfrac{a-\frac{4a^2(x+2a-4b)^2}{y^2}}{a+\frac{4a^2(x+2a-4b)^2}{y^2}} &= \dfrac{y^2-4a(x+2a-4b)^2}{y^2+4a(x+2a-4b)^2} \\ w &= \dfrac{-a+\frac{4a^2(x+2a-4b)^2x}{2ay^2}}{a+\frac{4a^2(x+2a-4b)^2}{y^2}} &= \dfrac{-y^2+2x(x+2a-4b)^2}{y^2+4a(x+2a-4b)^2}. \end{cases}$$

The point $(u, v, w) = (0, 1, 1)$ corresponds to the point $(x, y) = \infty$ and $(u, v, w) = (0, 1, -1)$ corresponds to $(x, y) = (4b-2a, 0)$. The points $(u, v, w) = (0, -1, 1)$and $(u, v, w) = (0, -1, -1)$ correspond to the points $(x, y) = (2a, 0)$ and $(x, y) = (-2a, 0)$ respectively.

Substituting $(x - 2a)(x + 2a)(x + 2a - 4b)$ for y^2 in the expression of ψ, and replacing (x, y) by $(4x - 2a, 8y)$ yield the simpler equation

$$E : y^2 = x(x - a)(x - b).$$

and simpler transformations.

$$\varphi:\begin{cases} x &= -\frac{a(w+1)}{v-1} \\ y &= \frac{au}{v-1}(x-b). \end{cases}, \qquad \psi:\begin{cases} u &= -\frac{2y}{x^2-ab} \\ v &= \frac{x^2-2ax+ab}{x^2-ab} \\ w &= \frac{x^2-2bx+ab}{x^2-ab}. \end{cases}$$

Now the point $(u, v, w) = (0, 1, 1)$ corresponds to the point $(x, y) = \infty$ and $(u, v, w) = (0, 1, -1)$ corresponds to $(x, y) = (b, 0)$. The points $(u, v, w) = (0, -1, 1)$and $(u, v, w) = (0, -1, -1)$ correspond to the points $(x, y) = (a, 0)$ and $(x, y) = (0, 0)$ respectively.

Since the curve $E_{a,b}$ and E are both smooth, then the rational map φ and its inverse map ψ are both morphisms by Proposition 2.1 in [10]. Therefore $E_{a,b}$ and E are isomorphic over K. □