Isogeny Computation on Twisted Jacobi Intersections

Zhi Hu[1], Lin Wang[2], and Zijian Zhou[3,4](✉)

[1] School of Mathematics and Statistics, Central South University, Changsha, China
huzhi_math@csu.edu.cn
[2] Science and Technology on Communication Security Laboratory, Chengdu, China
[3] College of Liberal Arts and Sciences, National University of Defense Technology, Changsha, China
[4] Hunan Engineering Research Center of Commercial Cryptography Theory and Technology Innovation, Changsha, China

Abstract. Isogenies between elliptic curves act as a key role in isogeny-based cryptography. Formulas for isogenies on different elliptic curve models such as Weierstrass, Edwards, Huff and Hessian have been proposed. In this paper, we construct isogenies on twisted Jacobi intersections for the first time including a 2-isogeny and a generalized ℓ-isogeny for any odd ℓ. We also introduces ω-coordinate systems for twisted Jacobi intersections which provides biquadratic relations like the Montgomery model. As a result, such ω-coordinate systems would significantly simplify the computation of isogenies on twisted Jacobi intersections.

Keywords: Isogenies · Post-quantum cryptography · Twisted Jacobi intersection · ω-coordinate

1 Introduction

The supersingular isogeny-based cryptography is the most recent suggestion for post quantum cryptosystem and is founded on the hardness of finding an isogeny between two given supersingular elliptic curves over a finite field. It is drawing increased attention due to its relative small key sizes and messages compared to other post-quantum candidates. One of the instantiations is the key exchange protocol SIDH (Supersingular Isogeny Diffie-Hellman) proposed by De Feo and Jao [9]. Its secure key encapsulation mechanism version, named SIKE [10], was submitted to NIST's post-quantum cryptography standardization process and has been selected as an alternative candidate of PKE&KE in Round 3. There are also many other instantiations due to different choices of supersingular elliptic curves and isogenies. For example, the CSIDH [2] proposed by Castryck et al. in ASIACRYPT 2018 with supersingular elliptic curves over $\mathbb{F}_p$, the BSIDH [4] offered by Costello and the SiGamal [12] by Moriya et al. in ASIACRYPT 2020.

R. Deng et al. (Eds.): ISPEC 2021, LNCS 13107, pp. 46–56, 2021.
https://doi.org/10.1007/978-3-030-93206-0_4

As such, isogenies are a topic of interest in the isogeny-based cryptography as well as in elliptic curve cryptography. However, the bottleneck of isogeny-based cryptography is that its implementation efficiency does not meet the requirement of real-world application. The main contributor of this is that the isogeny computation is much more complicated than the traditional operations like scalar multiplications in elliptic curve cryptography.

It is well known that the existence of isogenies between two elliptic curves is independent of curve models. However, similar to the algebraic group arithmetic in traditional elliptic curve cryptography, the complexity of computing isogenies varies greatly from one model to another. The most famous method for efficiently presenting explicit isogeny with Weierstrass model is given by Vélu's formulas [16], which is based on point addition formulas. Moody and Shumow [13] presented formulas similar to Vélu's for isogenies on Edwards and Huff models of elliptic curves with efficient isogeny computation. Xu et al. [17] also gave explicit formulas for isogenies on Jacobi quartic curves.

Using the results above, cryptographers could choose corresponding curve models to accelerate the isogeny computation in the implementation of isogeny-based cryptography, for instants see the adaption of Montgomery model in SIDH [9]. Hence it is motivated to study the explicit and fast formulas for isogenies between other curve models such as the so-called twisted Jacobi intersection.

The twisted Jacobi intersections is the intersection of two quadratic surfaces in the three dimensional space such that they are birational equivalent to elliptic curves. It is a generalization of Jacobi intersections and was first introduced by Feng et al. [7]. Compared to Jacobi intersections, the twisted version has faster addition and doubling formulas. Furthermore, it was shown that every elliptic curve in positive characteristic with three points of order 2 is isomorphic to a twisted Jacobi intersection [7]. In [14], Silva et al. gave the explicit formula for odd isogeny of Jacobi intersections.

In this work, we study the fast isogeny computation between twisted Jacobi intersections model of elliptic curves. The following demonstrates the main contributions of this work:

- *Explicit Isogeny Formulas on Twisted Jacobi Intersections.* We present the explicit formulas for 2-isogeny and odd isogenies between twisted Jacobi intersections, extending Silva et al.'s results [14]. Our formula for computing the coefficients of curves of odd isogenies has a simple expression.
- *Differential Arithmetic on Twisted Jacobi Intersections.* Similar to the ω-coordinate system on Edwards model [6] and Huff Model [8], we construct a ω-coordinate system on twisted Jacobi intersections and prove a Montgomery-like group law formulas on these curves. Such ω-coordinate system also induces simple isogeny formulas for twisted Jacobi intersections, which share the same form as those on Montgomery curves with only x-coordinate.

Our work is organized as follows. Section 2 reviews basic facts about isogenies and twisted Jacobi intersections. Section 3 presents formulas for 2-isogenies and odd isogenies between twisted Jacobi intersections. In Sect. 4, we construct a new ω-coordinate system on twisted Jacobi intersections and give simplified isogeny

formulas with this system. Finally, Sect. 5 concludes with a discussion about further study.

2 Preliminaries

An isogeny between two elliptic curves E_1 and E_2 is a dense morphism $\phi : E_1 \to E_2$ preserves the basepoints, i.e. ϕ preserves the identity element with $\phi(E_1) = E_2$. Note that ϕ is also an endomorphism if $E_1 = E_2$. Two elliptic curves E_1, E_2 are said to be isogenous if there is an isogeny $\phi : E_1 \to E_2$. The degree of an isogeny is its degree as a rational map. In particular, a separable isogeny ϕ of degree ℓ has a kernel of size ℓ.

Recall that given an elliptic curve E and a subgroup G of E, there is a unique isogeny $E \to E'$ with kernel G up to isomorphism [15, III.4.12]. Hence one can identify an isogeny by specifying its kernel. Vélu's formula and its analogues shed a light on computing the isogeny that corresponds to a given subgroup. This correspondence may allow for compact representation and efficient computation of isogeny, especially for kernels generated by points of prime order.

Let K be a finite field with $\mathrm{char}(K) = p > 3$. A twisted Jacobi intersection model of elliptic curve over K is given by

$$J_{a,b} : \begin{cases} au^2 + v^2 = 1 \\ bu^2 + w^2 = 1 \end{cases} \tag{1}$$

where $a, b \in K$ and $ab(a-b) \neq 0$. Note that a Jacobi intersection is a twisted Jacobi intersection with $a = 1$. The j-invariant of $J_{a,b}$ is

$$j(J_{a,b}) = \frac{256(a^2 - ab + b^2)^3}{a^2b^2(a-b)^2}.$$

Note that $(0, 1, 1)$ is the identity point in the group $J_{a,b}(K)$, and the negative point of (u, v, w) is $(-u, v, w)$.

A twisted Jacobi intersection $J_{a,b} : au^2 + v^2 = 1, bu^2 + w^2 = 1$ is birationally equivalent to an elliptic curve $E_W : y^2 = x^3 - (a+b)x^2 + abx$, via the transformations [7]:

$$\begin{aligned}
\sigma : J_{a,b} &\longrightarrow E_W, \\
(0,1,1) &\longmapsto \infty, \\
(0,1,-1) &\longmapsto (b, 0), \\
(u,v,w) &\longmapsto (-\frac{a(w+1)}{v-1}, -\frac{au}{v-1}(\frac{a(w+1)}{v-1} + b)). \\
\sigma^{-1} : E_W &\longrightarrow J_{a,b}, \\
\infty &\longmapsto (0,1,1), \\
(b,0) &\longmapsto (0,1,-1), \\
(x,y) &\longmapsto (-\frac{2y}{x^2-ab}, \frac{x^2-2ax+ab}{x^2-ab}, \frac{x^2-2bx+ab}{x^2-ab}).
\end{aligned} \tag{2}$$

The group law on $J_{a,b}$ in affine coordinates is presented as follows [7]: given two points (u_1, v_1, w_1) and (u_2, v_2, w_2), the sum $(u_3, v_3, w_3) = (u_1, v_1, w_1) + (u_2, v_2, w_2)$ is

$$\begin{aligned} u_3 &= \frac{u_1v_2w_2 + u_2v_1w_1}{v_2^2 + au_2^2w_1^2}, \\ v_3 &= \frac{v_1v_2 - au_1w_1u_2w_2}{v_2^2 + au_2^2w_1^2}, \\ w_3 &= \frac{w_1w_2 - bu_1v_1u_2v_2}{v_2^2 + au_2^2w_1^2}. \end{aligned} \tag{3}$$

The above formulas are complete (i.e., defined for all inputs).

3 Isogenies on Twisted Jacobi Intersections

In this section we show how to present explicit (and simplified) formulas for isogenies on twisted Jacobi intersections. For a twisted Jacobi intersection $J_{a,b}$ over K with coefficient a, b, we denote by $\sqrt{a}$ (resp. $\sqrt{b}$) a square root of a (resp. b) and write simply $\sqrt{ab}$ for $\sqrt{a} \cdot \sqrt{b}$.

3.1 2-Isogeny

Theorem 1. *Let $J_{a,b}$ be a twisted Jacobi intersection over K, then there is a 2-isogeny from the curve $J_{a,b}$ as*

$$\phi_2(u, v, w) = (\frac{-u}{vw}, \frac{-\sqrt{ab}u^2 + 1}{vw}, \frac{\sqrt{ab}u^2 + 1}{vw}), \tag{4}$$

the image of ϕ_2 is the curve $J_{\hat{a},\hat{b}}$, where $\hat{a} = -(\sqrt{a} - \sqrt{b})^2$ and $\hat{b} = -(\sqrt{a} + \sqrt{b})^2$.

Proof. The desired 2-isogeny ϕ_2 can be derived as

$$\phi : J_{a,b} \xrightarrow{\sigma} E_1 \xrightarrow{\psi} E_2 \xrightarrow{\sigma'} J_{\hat{a},\hat{b}}.$$

Here $\sigma : J_{a,b} \to E_1$ is given as $(u, v, w) \longmapsto (-\frac{a(w+1)}{v-1}, -\frac{au}{v-1}(\frac{a(w+1)}{v-1} + b))$, with $E_1 : y^2 = x^3 - (a + b)x^2 + abx$.

The kernel of the desired isogeny is the set $\{(0, -1, -1), (0, 1, 1)\}$. For this kernel, it suffices to explicitly find the maps ψ, σ'. Formulas for 2-isogenies on Weierstrass curves are well known, see Example 4.5 of [15] for the 2-isogeny $\psi : E_1 \to E_2$ as

$$\psi(x, y) = (\frac{y^2}{x^2}, \frac{y(ab - x^2)}{x^2}),$$

where $E_2 : y^2 = x^3 + 2(a + b)x^2 + (a - b)^2x$.

Therefore, we can get the corresponding map $\sigma' : E_2 \to J_{\hat{a}_i,\hat{b}_i}$ by pulling Weierstrass model back to a desired Jacobi intersection using the maps in Eq. (2).

Composing the maps as $\sigma' \circ \psi \circ \sigma$ leads to the stated formulas for ϕ_2. Since the arithmetic details are straightforward and thus we omitted them for brevity.

3.2 Odd Degree Isogenies

Let F be a subgroup of E of odd order ℓ, the well known Vélu formulas [16] on a Weierstrass elliptic curve for an isogeny $\phi : E \to E'$ with kernel F are presented here. Given a point $P = (x_P, y_P) \in E$, define

$$\phi(P) = \begin{cases} (x_P + \sum_{Q\in F-\{\infty\}}(x_{P+Q} - x_Q), y_P + \sum_{Q\in F-\{\infty\}}(y_{P+Q} - y_Q), & P \notin F, \\ \infty, & P \in F. \end{cases}$$

Silva et al. in [14] gave a formula for odd degree isogeny ϕ on the Jacobi intersection as

$$\phi(P) = \begin{cases} \infty, & P \in F, \\ (u_P \prod_{Q\in F-\{\infty\}} \frac{u_{P+Q}}{u_Q}, v_P \prod_{Q\in F-\{\infty\}} \frac{v_{P+Q}}{v_Q}, w_P \prod_{Q\in F-\{\infty\}} \frac{w_{P+Q}}{w_Q}), & P \notin F, \end{cases}$$

based on which they also gave an explicit formula for isogeies of degree ℓ.

In this work, we imitate the above work and present a new formula for the degree ℓ-isogeny, which yields the following result:

Theorem 2. *Let $F = \{(0,1,1), (\pm\alpha_1, \beta_1, \gamma_1), ..., (\pm\alpha_s, \beta_s, \gamma_s)\}$ be a subgroup of the twisted Jacobi intersection $J_{a,b}$ with odd order $\ell = 2s + 1$. Define*

$$\phi_\ell(P) = (\prod_{Q\in F} \frac{u_{P+Q}w_Q}{v_Q}, \prod_{Q\in F} \frac{v_{P+Q}}{v_Q}, \prod_{Q\in F} \frac{w_{P+Q}}{w_Q}). \tag{5}$$

Then ϕ_ℓ is an ℓ-isogeny with kernel F, from $J_{a,b}$ to $J_{\hat{a},\hat{b}}$ where $\hat{a} = a^\ell$ and $\hat{b} = b^\ell \prod_{i=1}^{s} \frac{(1-a\alpha_i^2)^4}{(1-b\alpha_i^2)^4}$. The coordinate maps are given by

$$\begin{aligned} \phi_\ell(u,v,w) = (u \prod_{i=1}^{s} \frac{(u^2 - \alpha_i^2)\gamma_i^2}{(1 - ab\alpha_i^2u^2)\beta_i^2}, v \prod_{i=1}^{s} \frac{1 + ab\alpha_i^2u^2 - a(u^2 + \alpha_i^2)}{(1 - ab\alpha_i^2u^2)\beta_i^2}, \\ w \prod_{i=1}^{s} \frac{1 + ab\alpha_i^2u^2 - b(u^2 + \alpha_i^2)}{(1 - ab\alpha_i^2u^2)\gamma_i^2}). \end{aligned} \tag{6}$$

Proof. We have $\phi_\ell((0,1,1)) = (0,1,1)$ and ϕ_ℓ is invariant under the translation by elements of F, thus $F \subseteq \ker(\phi_\ell)$. Conversely, if $P \in \ker(\phi_\ell)$, then there exists some $Q \in F$ such that $P + Q = (0,1,1)$, which implies that $P = -Q \in F$, and hence $F = \ker(\phi_\ell)$. Moreover, suppose $P = (u,v,w)$, and $Q = (\alpha_i, \beta_i, \gamma_i) \neq (0,1,1)$, then we have

$$\begin{aligned} u_{P+Q}u_{P-Q} &= \frac{(\beta_i^2\gamma_i^2u^2 - \alpha_i^2v^2w^2)}{(\beta_i^2 + a\alpha_i^2w^2)^2} = \frac{u^2 - \alpha_i^2}{1 - ab\alpha_i^2u^2}, \\ v_{P+Q}v_{P-Q} &= \frac{a^2u^2w^2\alpha_i^2\gamma_i^2 - v^2\beta_i^2}{(\beta_i^2 + a\alpha_i^2w^2)^2} = \frac{1 - a(\alpha_i^2 + u^2) + abu^2\alpha_i^2}{1 - ab\alpha_i^2u^2}, \\ w_{P+Q}w_{P-Q} &= \frac{b^2u^2v^2\alpha_i^2\beta_i^2 - \gamma_i^2w^2}{(\beta_i^2 + a\alpha_i^2w^2)^2} = \frac{1 - b(u^2 + \alpha_i^2) + abu^2\alpha_i^2}{1 - ab\alpha_i^2u^2}. \end{aligned}$$

Thus it is straightforward to derive the above coordinate maps by the twisted Jacobi intersection addition law.

It remains to derive the formulas for $\hat{a}$ and $\hat{b}$ on the image curve

$$J_{\hat{a},\hat{b}} : \begin{cases} \hat{a}U^2 + V^2 = 1 \\ \hat{b}U^2 + W^2 = 1 \end{cases}, \tag{7}$$

where $U(P), V(P), W(P)$ are the coordinate maps of ϕ_ℓ. Consider the function

$$\begin{aligned} G_1(u,v,w) &= (\hat{a}U^2 + V^2 - 1)(\prod_{i=1}^{s}(1 - ab\alpha_i^2u^2)^2\beta_i^4) \\ &= \hat{a}(u^2\prod_{i=1}^{s}((u^2-\alpha_i^2)^2\gamma_i^4)) + (1-au^2)\prod_{i=1}^{s}(1 - a(\alpha_i^2+u^2) + ab\alpha_i^2u^2)^2 - \prod_{i=1}^{s}(1-ab\alpha_i^2u^2)^2\beta_i^4 \\ &= (\hat{a} - a^\ell)\prod_{i=1}^{s}\gamma_i^4u^{2\ell} + \text{lower terms with respect to } u. \end{aligned}$$

Setting the coeffcients of $u^{2\ell}$ to zero and thus we obtain $\hat{a} = a^\ell$. Similarly we consider

$$\begin{aligned} G_2(u,v,w) &= (\hat{b}U^2 + W^2 - 1)(\prod_{i=1}^{s}(1 - ab\alpha_i^2u^2)^2\beta_i^4\gamma_i^4) \\ &= \hat{b}(u^2\prod_{i=1}^{s}((u^2-\alpha_i^2)^2\gamma_i^8)) + (1-bu^2)\prod_{i=1}^{s}(1 - b(\alpha_i^2+u^2) + ab\alpha_i^2u^2)^2\beta_i^4 - \prod_{i=1}^{s}(1-ab\alpha_i^2u^2)^2\beta_i^4\gamma_i^4 \\ &= (\hat{b}\prod_{i=1}^{s}\gamma_i^8 - b^\ell\prod_{i=1}^{s}\beta_i^8)u^{2\ell} + \text{lower terms with respect to } u. \end{aligned}$$

By using the fact that $\beta_i^2 = 1 - a\alpha_i^2$, $\gamma_i^2 = 1 - b\alpha_i^2$ and by setting the coeffcients of $u^{2\ell}$ to zero, we obtain that

$$\hat{b} = b^\ell\prod_{i=1}^{s}\frac{\beta_i^8}{\gamma_i^8} = b^\ell\prod_{i=1}^{s}\frac{(1-a\alpha_i^2)^4}{(1-b\alpha_i^2)^4}.$$

Remark 1. While Silva et al. in [14] also gave similar formulas for odd isogeny on Jacobi intersections, we proved it in a different way for the twisted Jacobi intersections. Moreover, our formulas for the curve coefficients are easily transformed into inversion-free version, which are expected to provide performance advantage in isogeny computation.

4 ω-Coordinate on Twisted Jacobi Intersections

To evaluate the elliptic curve arithmetic efficiently, Farashahi and Hosseini proposed ω-coordinate system on Edwards curves [6], which was also applied to isogeny computation by Kim et al. [11]. Huang et al. [8] and Drylo et al. in [5] presented similar ω-coordinate systems on Huff curves which provide faster formulas for point addition and isogeny computation. In fact, such ω-coordinate systems could be generalized to other elliptic curve models, and induce analogous Montgomery-like formulas for group and isogeny arithmetic.

4.1 ω-Coordinate System for Differential Addition

In this work, we introduce such kind ω-coordinate system on twisted Jacobi intersections. We define a rational function ω by $\omega(u, v, w) = \sqrt{ab}u^2$, which is well computed for all affine points on a twisted Jacobi intersection. Let $P = (u, v, w)$ be a point on the curve, one can easily deduce that $\omega(P) = \omega(-P)$. Moreover, $\omega((0, 1, 1)) = 0$. Denote by $c = \frac{\sqrt{b}}{\sqrt{a}}$, then the equation of the twisted Jacobi intersection can be written as:

$$J_c : \begin{cases} \omega + cv^2 = c \\ c\omega + w^2 = 1 \end{cases} \tag{8}$$

Theorem 3. *Let $\omega_i = \omega(P_i)$ with $P_i \in J_{a,b}$ for $i = 1, 2$, and let $\omega_0 = \omega(P_1 - P_2)$, $\omega_3 = \omega(P_1 + P_2)$ and $\omega_4 = \omega(2P_1)$. We have the following differential addition formulas*

$$\omega_3\omega_0 = \frac{(\omega_1 - \omega_2)^2}{(\omega_1\omega_2 - 1)^2},\ \omega_4 = \frac{4\omega_1(\omega_1^2 + (c + \frac{1}{c})\omega_1 + 1)}{(1 - \omega_1^2)^2}.$$

Proof. This can be derived from the addition formula give by Eq. (3) and hence we omit the detail.

4.2 ω-Coordinate for Isogenies

Based on the above, we present the isogeny formulas using the ω-coordinate on twisted Jacobi intersection J_c as Eq. (8). Note that the j-invariant

$$j(J_c) = j(J_{a,b}) = \frac{256(1 - c^2 + c^4)^3}{c^4(1 - c^2)^2}.$$

We can use the parameter c to represent the isogenous curve instead of parameters (a, b) in $J_{a,b}$.

Recall that $\omega(u, v, w) = \sqrt{ab}u^2$ for $J_{a,b}$ and write $c = \frac{\sqrt{b}}{\sqrt{a}}$.

Theorem 4. *Let ϕ_2 be the 2-isogeny from $J_{a,b}$ to $J_{\hat{a},\hat{b}}$ defined as in Theorem 1. Then the evaluation of $\omega = \omega(P), P = (u, v, w) \in J_{a,b}(K)$ under ϕ_2 is given by*

$$\phi_2(\omega) = \frac{(\frac{1}{c} - c)\omega}{(1 - c\omega)(1 - \frac{\omega}{c})}, \tag{9}$$

where the parameter for the image curve is $\hat{c} = \frac{1+c}{1-c}$.

Proof. Suppose $P = (u, v, w)$ and denote by $\phi(u, v, w) = (U, V, W)$ the image point. Then the ω-coordinate in $J_{\hat{a},\hat{b}}$ is given by $\omega(\phi(u, v, w)) = \sqrt{\hat{a}\hat{b}}U^2$.

By Theorem 1, one has

$$\begin{aligned}\sqrt{\hat{a}\hat{b}}U^2 &= \sqrt{(\sqrt{a}-\sqrt{b})^2(\sqrt{a}+\sqrt{b})^2}\frac{u^2}{v^2w^2}\\ &= \frac{(a-b)u^2}{(1-au^2)(1-bu^2)}\\ &= \frac{(\frac{1}{c}-c)\omega}{(1-c\omega)(1-\frac{\omega}{c})}.\end{aligned}$$

Moreover, we have

$$\hat{c} = \sqrt{\frac{\hat{b}}{\hat{a}}} = \frac{(\sqrt{a}+\sqrt{b})}{(\sqrt{a}-\sqrt{b})} = \frac{1+c}{1-c}.$$

We have the following odd isogeny formula using the $\omega-$coordinate:

Theorem 5. *Let $F = \{(0,1,1),(\pm\alpha_1,\beta_1,\gamma_1),...,(\pm\alpha_s,\beta_s,\gamma_s)\}$ be a subgroup of the twisted Jacobi intersection $J_{a,b}$ with odd order $\ell = 2s+1$. Write $\omega_i = \omega(\alpha_i,\beta_i,\gamma_i)$ for $i = 1,..,s$ and let ϕ_ℓ be the ℓ-isogeny from $J_{a,b}$ to $J_{\hat{a},\hat{b}}$ with kernel F. Then the evaluation of $\omega = \omega(P), P = (u,v,w) \in J_{a,b}(K)$ under ϕ_ℓ is given by*

$$\phi_\ell(\omega) = \omega\prod_{i=1}^{s}(\frac{\omega-\omega_i}{1-\omega\omega_i})^2, \tag{10}$$

with the codomain curve coefficient

$$\hat{c} = c\prod_{i=1}^{s}\frac{(c-\omega_i)^2}{(1-c\omega_i)^2}. \tag{11}$$

Proof. Note that $c = \sqrt{b/a}$ and $\omega = \sqrt{ab}\omega^2$, which implies $bu^2 = c\omega, au^2 = \omega/c$. Let $P = (u,v,w)$ and write $U(P)$ the coordinate maps of ϕ_ℓ give in Theorem 2.

Recall that by Theorem 2, we have $\hat{a} = a^\ell$ and

$$\hat{b} = b^\ell\prod_{i=1}^{s}\frac{(1-a\alpha_i^2)^4}{(1-b\alpha_i^2)^4} = b^\ell\prod_{i=1}^{s}\frac{\beta_i^8}{\gamma_i^8}.$$

Then

$$\begin{aligned}\hat{\omega} = \sqrt{\hat{a}\hat{b}}U(P)^2 &= \sqrt{a^lb^l}u^2\prod_{i=1}^{s}(\frac{\beta_i^4}{\alpha_i^4}\frac{(u^2-\alpha_i^2)\gamma_i^2}{(1-ab\alpha_i^2u^2)\beta_i^2})^2\\ &= \sqrt{a^lb^l}u^2\prod_{i=1}^{s}\frac{(\sqrt{ab}u^2-\sqrt{ab}\alpha_i^2)^2}{(1-ab\alpha_i^2u^2)^2}\\ &= \omega\prod_{i=1}^{s}\frac{(\omega-\omega_i)^2}{(1-\omega\omega_i)^2}.\end{aligned}$$

Furthermore, one has

$$\hat{c} = \sqrt{\frac{\hat{b}}{\hat{a}}} = \sqrt{\frac{b}{a}} \prod_{i=1}^{s} \frac{(1 - a\alpha_i^2)^2}{(1 - b\alpha_i^2)^2} = c \prod_{i=1}^{s} \frac{(c - \omega_i)^2}{(1 - c\omega_i)^2}.$$

4.3 Computational Cost

Let **M** stand for a field multiplication, **S** for a field squaring, **C** for a multiplication by a curve constant, and **I** for a field inversion. In the following table we list the costs of our odd isogenies compared with those proposed by Silva et al. in [14].

Table 1. The computational costs of $\ell = 2s + 1$ isogeny evaluation on (twisted) Jacobi intersections

Work	Operation cost (affine)	Operation cost (projective)
Silva et al. [14]	$(4s + 2)\mathbf{M} + 3\mathbf{S} + (5s + 1)\mathbf{C} + \mathbf{I}$	$(4s + 7)\mathbf{M} + 5\mathbf{S} + (6s + 2)\mathbf{C}$
This work (ω-coordinate)	$3s\mathbf{M} + 1\mathbf{S} + \mathbf{I}$	$4s\mathbf{M} + 2\mathbf{S}$

It should be noted that Silva et al. in [14, Theorem 4.1] proposed the codomain curve parameter for Jacobi intersection (setting $b = 1$ in the twisted case) as $\hat{a} = a - 2a \sum_{i=1}^{s} (\frac{-\alpha_i^2 \beta_i^2}{\gamma_i^2} + 2\alpha_i^2 - 1)$, the evaluation of which costs much more than that of our $\hat{c}$ in Eq. (11).

Remark 2. The above result implies an interesting result that, the formulas of odd ℓ isogeny with ω-coordinate system on twisted Jacobi intersections share the same form with those on Montgomery model in [3]. Thus we would gain comparable cost for the isogeny computation by adopting the above formulas for twisted Jacobi intersections. Furthermore, due to the well form of the formulas in Eqs. (10) and (11), we can adapt the fast isogeny computation technique proposed by Bernstein et al. in [1] to twisted Jacobi intersections, and thus the ℓ-isogeny mapping and its codomain curve coefficient could be evaluated in $\tilde{O}(\sqrt{\ell})$ finite field operations.

5 Conclusion

In this work, we exploit the ω-coordinates to optimize the elliptic curve group arithmetic formulas as well as the isogenous formulas on twisted Jacobi intersections. Our results implies that the twisted Jacobi intersections also serve as an ideal model for isogeny-based cryptography. It was also noticed that the formulas of odd ℓ isogeny with w-coodinate system on twisted Jacobi intersections have the same expression as the Kummer line in Montgomery model. We hope that further research could find the connection between the w-coordinate systems (resp. Kummer line) on different curve models.

Acknowledgements. We would like to thank the reviewers for their helpful comments. Zhi Hu was supported by the National Natural Science Foundation of China (61972420, 61602526) and the Natural Science Foundation of Hunan Province (2020JJ3050, 2019JJ50827). Zijian Zhou (corresponding author of this paper) was supported by the Natural Science Foundation of Hunan Province (2021JJ40701) and The Research Fund of National University of Defense Technology (ZK20-42).

References

1. Bernstein, D., De Feo, L., Leroux, A., Smith, B.: Faster computation of isogenies of large prime degree. Cryptology ePrint Archive 2020/341 (2020)
2. Castryck, W., Lange, T., Martindale, C., Panny, L., Renes, J.: CSIDH: an efficient post-quantum commutative group action. In: Peyrin, T., Galbraith, S. (eds.) ASIACRYPT 2018. LNCS, vol. 11274, pp. 395–427. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-03332-3_15
3. Costello, C., Hisil, H.: A simple and compact algorithm for SIDH with arbitrary degree isogenies. In: Takagi, T., Peyrin, T. (eds.) ASIACRYPT 2017. LNCS, vol. 10625, pp. 303–329. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-70697-9_11
4. Costello, C.: B-SIDH: supersingular isogeny Diffie-Hellman using twisted torsion. Cryptology ePrint Archive 2019/1145 (2019)
5. Drylo, R., Kijko, T., Wronski, M.: Efficient montgomery-like formulas for general Huff's and Huff's elliptic curves and their applications to the isogeny-based cryptography. Cryptology ePrint Archive 2020/526 (2020)
6. Farashahi, R.R., Hosseini, S.G.: Differential addition on twisted Edwards curves. In: Pieprzyk, J., Suriadi, S. (eds.) ACISP 2017. LNCS, vol. 10343, pp. 366–378. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-59870-3_21
7. Feng, R., Nie, M., Wu, H.: Twisted Jacobi intersections curves. In: Kratochvíl, J., Li, A., Fiala, J., Kolman, P. (eds.) TAMC 2010. LNCS, vol. 6108, pp. 199–210. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13562-0_19
8. Huang, Y., Zhang, F., Hu, Z., Liu, Z.: Optimized arithmetic operations for isogeny-based cryptography on Huff curves. In: Liu, J.K., Cui, H. (eds.) ACISP 2020. LNCS, vol. 12248, pp. 23–40. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-55304-3_2
9. Jao, D., De Feo, L.: Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In: Yang, B.-Y. (ed.) PQCrypto 2011. LNCS, vol. 7071, pp. 19–34. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-25405-5_2
10. Jao, D., et al.: Supersingular isogeny key encapsulation. In: NIST Post-Quantum Cryptography Standardization Round 2 Submission. 16 April 2020. http://www.sike.org/
11. Kim, S., Yoon, K., Park, Y.-H., Hong, S.: Optimized method for computing odd-degree isogenies on Edwards curves. In: Galbraith, S.D., Moriai, S. (eds.) ASIACRYPT 2019. LNCS, vol. 11922, pp. 273–292. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-34621-8_10
12. Moriya, T., Onuki, H., Takagi, T.: SiGamal: a supersingular isogeny-based PKE and its application to a PRF. In: Moriai, S., Wang, H. (eds.) ASIACRYPT 2020. LNCS, vol. 12492, pp. 551–580. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-64834-3_19
13. Moody, D., Shumow, D.: Analogues of Velu's formulas for isogenies on alternate models of elliptic curves. Math. Comput. **85**(300), 1929–1951 (2016)

14. Silva, J., Lopez, J., Dahab, R.: Isogeny formulas for Jacobi intersection and twisted hessian curves. Adv. Math. Commun. **14**(3), 507–523 (2020)
15. Silverman, J.H.: The Arithmetic of Elliptic Curves, 2nd edn. Springer-Verlag, New York (2009)
16. Isogenies entre courbes elliptiques: Vélu. J. CR Acad. Sci. Paris Ser. AB **273**, A238–241 (1971)
17. Xu, X., Yu, W., Wang, K., He, X.: Constructing isogenies on extended Jacobi quartic curves. In: Chen, K., Lin, D., Yung, M. (eds.) Inscrypt 2016. LNCS, vol. 10143, pp. 416–427. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-54705-3_26