ISOGENY FORMULAS FOR JACOBI INTERSECTION AND TWISTED HESSIAN CURVES

JOÃO PAULO DA SILVA*, JULIO LÓPEZ AND RICARDO DAHAB

Institute of Computing
University of Campinas
Av. Albert Einstein 1251
Cidade Universitária “Zeferino Vaz”, 13083-852, Campinas, SP, Brazil

ABSTRACT. The security of public-key systems is based on the difficulty of solving certain mathematical problems. With the possible emergence of large-scale quantum computers several of these problems, such as factoring and computing discrete logarithms, would be efficiently solved. Research on quantum-resistant public-key cryptography, also called post-quantum cryptography (PQC), has been productive in recent years. Public-key cryptosystems based on the problem of computing isogenies between supersingular elliptic curves appear to be good candidates for the next generation of public-key cryptography standards in the PQC scenario. In this work, motivated by a previous work by D. Moody and D. Shumow [17], we derived maps for elliptic curves represented in Jacobi Intersection and Twisted Hessian models. Our derivation follows a multiplicative strategy that contrasts with the additive idea presented in the Vélu formula. Finally, we present a comparison of computational cost to generate maps for isogenies of degree $l$, where $l = 2k + 1$. In affine coordinates, our formulas require 46.8% less computation than the Huff model and 48% less computation than the formulas given for the Extended Jacobi Quartic model when computing isogenies of degree 3. Considering higher degree isogenies as 101, our formulas require 23.4% less computation than the Huff model and 24.7% less computation than the formula for the Extended Jacobi Quartic model.

1. Introduction

1.1. Isogenies in cryptography. One of the first appearances of the concept of isogenies in the field of cryptography was the need to improve the complexity of the polynomial time algorithm proposed by Schoof [19] in order to compute the number of points on an elliptic curve defined over a finite field. This algorithm was later renamed SEA [11] (in honor of the improvements made by N. Elkies and A. Atkin).

For the supersingular elliptic curve scenario, there are three main problems that have emerged as potential hardness assumptions related to isogenies computation. The first is the problem of computing isogenies between supersingular elliptic curves. The second consist of computing the endomorphism ring of a supersingular elliptic curve, and the third one is to compute a maximal order isomorphic to $\text{End}(E)$, where $E$ is a supersingular elliptic curve. For a long time, these problems were believed to be interrelated and polynomial-time equivalent. Nevertheless, the first

*First author is supported by Intel/FAPESP grant 14/50704-7 under project “Secure Execution of Cryptographic Algorithms”.

2010 Mathematics Subject Classification: Primary: 58F15, 58F17; Secondary: 53C35.

Key words and phrases: Isogeny, isogeny-based cryptography, twisted hessian model, Jacobi Intersection model.
1.2. CONSTRUCTIONS BASED ON ISOGENIES AND APPLICATIONS. Due to the fact that the most commonly used cryptosystems (e.g., RSA and ECDSA) are vulnerable to Shor’s quantum algorithm [3], it is necessary to search for new options. More recently, Cryptography based on Isogenies was proposed. Couveignes [8] mentioned about isogenies in cryptography but only published in 2006; In 2009 Charles, Goren and Lauter [5] introduced an isogeny-based hash function and showed that it is collision resistant based on hardness of computing isogenies between supersingular elliptic curves. In 2010, Stolbunov [18] presented the first published isogeny-based public-key cryptosystem based on isogenies between ordinary curves, and Childs et al. [7] showed a quantum subexponential attack on Stolbunov’s public-key cryptosystem based on isogenies between ordinary curves. In 2006; In 2009 Charles, Goren and Lauter [5] introduced an isogeny-based hash function and showed that it is collision resistant based on hardness of computing isogenies between supersingular elliptic curves. In 2010, Stolbunov [18] presented the first published isogeny-based public-key cryptosystem based on isogenies between ordinary curves, and Childs et al. [7] showed a quantum subexponential attack on Stolbunov’s public-key cryptosystem based on a reduction to a hidden shift problem, together with a subexponential-time algorithm for evaluating isogenies from kernel ideals assuming the Generalized Riemann Hypothesis. The authors in [13] presented a Diffie-Hellman-like key exchange algorithm for supersingular elliptic curves (SIDH) and an encryption algorithm that can be easily derived from it. The problems on which these authors based the difficulty of their proposals, and related to the problems presented in subsection 1.1, can be defined as

- **Computational Supersingular Isogeny (CSSI) Problem**: Let $\phi_A : E_0 \to E_A$ be an isogeny whose kernel is $\langle [m_A]P_A + [n_A]Q_A \rangle$, with $m_A, n_A \in R 0 \rightarrow Z_{\ell_A}^*$ not both divisible by $\ell_A$. So, given $E_A$ and the values $\phi_A(P_B), \phi_A(Q_B)$, find a generator for $\langle [m_A]P_A + [n_A]Q_A \rangle$.

- **Supersingular Computational Diffie-Hellman (SSCDH) Problem**: Let $\phi_A : E_0 \to E_A$ be an isogeny whose kernel is $\langle [m_A]P_A + [n_A]Q_A \rangle$, and let $\phi_B : E_0 \to E_B$ be an isogeny whose kernel is $\langle [m_B]P_B + [n_B]Q_B \rangle$, with $m_A, n_A \in R 0 \rightarrow Z_{\ell_A}^*$, respectively $m_B, n_B \in R 0 \rightarrow Z_{\ell_B}^*$, and not both divisible by $\ell_A$, respectively $\ell_B$. Then, given supersingular elliptic curves $E_A, E_B$ and points $\phi_A(P_B), \phi_A(Q_B), \phi_B(P_A), \phi_B(Q_A)$, find the $j$-invariant of $E_0/\langle [m_A]P_A + [n_A]Q_A, [m_B]P_B + [n_B]Q_B \rangle$.

In [4] the authors presented a non-interactive key exchange protocol named CSIDH (**commutative**-Supersingular Isogeny Diffie-Hellman) with even shorter keys than the SIDH protocol. A construction named SIKE [14] is the representative of isogeny-based algorithms among 69 candidates submitted to the first round of NIST’s Post-Quantum Cryptography Standardization process [6]. In January 2019, the SIKE protocol was moved to the second round of NIST PQC standardization process. In addition, the SIDH was included in an experiment for a quantum-resistant version of TLS 1.3. So, there are important real applications for isogenies in cryptography.

1.3. OUR CONTRIBUTIONS. One of the main problems in isogeny-based algorithms is the computation of rational functions that make up the isogeny map. Vélu’s formula [21] does this for curves in the Weierstrass model, but there are several other models for elliptic curves. Addition formulas for alternative models can present good features for cryptography purposes as symmetry and possibility of using for point doubling. Finding efficient formulas for curve operations on different models can improve the computation and evaluation of isogenies. In this work, we present
formulas for evaluating isogenies given a specification of the kernel for some models of elliptic curves. In particular, we derived explicit formulas for isogeny computation in Jacobi Intersection and Twisted Hessian models when a kernel representation of the isogeny is given. For the Twisted Hessian curves mentioned before, we only claim the application of the multiplication-based derivation technique as well as the computational cost analysis of such formulas. All these formulas are a multiplication version of Vélu’s, constructed over the addition law of these alternative representation models for elliptic curves.

1.4. Organization of this document. This paper is organized as follows: Section 2 presents the elliptic curve models treated in this work, named Jacobi Intersection and Twisted Hessian, as the models of related work used for comparison, namely Edwards, Huff, and Extended Jacobi Quartic; Section 3 introduces concepts related to isogenies and how to construct them via Vélu’s formula in the Weierstrass model; in Section 4 we present the explicit formulas for degree \( l \) isogeny computation and evaluation in Jacobi Intersection model; in Section 5 we present the explicit formulas for degree \( l \) isogeny computation and evaluation in Twisted Hessian model and our advances on construct a formal proof; in Section 6, we analyze the complexity of the formulas for both models and compare them with related formulas obtained from related works; finally, in Section 7 we put forward conclusions and directions for future work.

2. Elliptic curve models

Although elliptic curves are more commonly specified by the reduced and generalized Weierstrass equations, in this section we will present alternative models for representing elliptic curves, discuss some aspects about them and show how they are related to the Weierstrass model.

2.1. Edwards’ model. Introduced by H. Edwards [9] in 2007, the named Edwards’ model for an elliptic curve can be expressed by the equation

\[ E_d : x^2 + y^2 = 1 + dx^2 y^2, \]

with \( d \neq 0, 1 \). Given points on \( E_d \), \( P_1 = (x_1, y_1) \) and \( P_2 = (x_2, y_2) \), the addition formula for \( P_1 + P_2 \) is given by

\[
(x_1, y_1) + (x_2, y_2) = \left( \frac{x_1 y_2 + x_2 y_1}{1 + dx_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - dx_1 x_2 y_1 y_2} \right).
\]

The point \((0, 1)\), whose order is 2, is the identity element of \( E_d \). Moreover, given a point \( P = (x, y) \), \(-P = (-x, y)\) is the inverse element of \( P \) under point addition. Generalizations of such curves, known as Twisted Edwards Curves, were proposed [1] in 2008. Such curves are given by the equation \( E_{a,d} : ax^2 + y^2 = 1 + dx^2 y^2 \), where \( a \) and \( d \neq 1 \) are distinct and non-zero elements of a field \( K \) over which the elliptic curve is defined. Given points \( P_1 = (x_1, y_1) \) and \( P_2 = (x_2, y_2) \) on \( E_{a,d} \), the point addition formula for \( P_1 + P_2 \) is

\[
P_1 + P_2 = (x_1, y_1) + (x_2, y_2) = \left( \frac{x_1 y_2 + x_2 y_1}{1 + dx_1 x_2 y_1 y_2}, \frac{y_1 y_2 - ax_1 x_2}{1 - dx_1 x_2 y_1 y_2} \right).
\]

The point \((0, 1)\) is the identity element of \( E_{a,d} \). Moreover, given the point \( P = (x, y) \), \(-P = (x, -y)\) is the inverse element of \( P \). A birational map between an
elliptic curve given by $E_{a,d}$ [17] and another curve $E$, given in the Weierstrass model, is given by

$$\psi: (x, y) \mapsto \left( \frac{1+y}{1-y}, \frac{a-d}{x(1-y)} \right),$$

which sends the points on curve $E_{a,d}$ onto points on curve $E: y^2 = x^3 + 2(a + d)x^2 + (a - d)^2x$. The inverse transformation is given by the map $\psi^{-1}$,

$$\psi^{-1}: (x, y) \mapsto \left( 2x \frac{x - (a - d)}{y}, \frac{x + (a - d)}{y} \right).$$

2.2. Huff’s model. The Huff curves were reintroduced in [16] and defined, as presented here, in [23]. The Huff curves can be expressed by $H_{a,b} : x(ay^2 - 1) = y(bx^2 - 1)$, with $ab(a - b) \neq 0$. The point $(0, 0)$ is the identity element of $H_{a,b}$ and, given the point $P = (x, y)$, $-P = (-x, -y)$ is the inverse element of $P$. Given two points in the Huff’s model, $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$, the formula for point addition is given by

$$(x_1, y_1) + (x_2, y_2) = \left( \frac{(x_1 + x_2)(1 + ay_1y_2)}{(1 + bx_1x_2)(1 - ay_1y_2)}, \frac{(y_1 + y_2)(1 + bx_1x_2)}{(1 - bx_1x_2)(1 + ay_1y_2)} \right).$$

The addition formula given above works for every point on $H_{a,b}$ except for the points at infinity $(1:0:0)$, $(0:1:0)$ and $(a:b:0)$, expressed in projective coordinates. In [16] the authors present a birational map between a Huff curve $H_{a,b}$ and a curve $E$ in the Weierstrass form. This map is given as

$$\psi: (x, y) \mapsto \left( bx - ay, \frac{b - a}{y - x} \right),$$

and sends the points on $H_{a,b}$ onto the points on $E: y^2 = x^3 + (a + b)x^2 + abx$. The inverse transformation is given by the map $\psi^{-1}$ as

$$\psi^{-1}: (x, y) \mapsto \left( \frac{x + a}{y}, \frac{x + b}{y} \right).$$

2.3. Hessian and twisted Hessian’s models. Another parameterization of elliptic curves is given by curves in the Hessian model [15]. We can express such curves by the equation $H_d : u^3 + v^3 + 1 = 3dvw$ or, in projective coordinates, $H_d : U^3 + V^3 + W^3 = 3dUVW$, with $d \in K$, where $K$ is the underlying field and $d^3 \neq 1$. The identity point, in projective coordinates is $(1 : -1 : 0)$ and, for a given point $P = (u, v)$, $-P = (v, u)$ is the inverse element of $P$. For the addition law, let $P_1 = (u_1, v_1)$ and $P_2 = (u_2, v_2)$ be points on $H_d$ with $P_1 \neq P_2$; then, the coordinates of the resulting point $P_3 = (u_3, v_3) = P_1 + P_2$ are given by

$$u_3 = \frac{v_1^2u_2 - v_2^2u_1}{u_2v_2 - u_1v_1}, \quad v_3 = \frac{u_1^2v_2 - u_2^2v_1}{u_2v_2 - u_1v_1}.$$

For point doubling, the coordinates of $P_3 = (u_3, v_3) = [2]P_1$ are given by

$$u_3 = \frac{v_1(1 - u_1^3)}{u_1^3 - v_1^3}, \quad v_3 = \frac{u_1(v_1^3 - 1)}{u_1^3 - v_1^3}.$$

There are some interesting properties of the addition law for a curve in the Hessian form. For example, taking a point $P_1 = (U_1 : V_1 : W_1)$ in projective coordinates, we have $[2]P_1 = (W_1 : U_1 : V_1) \bigoplus (V_1 : W_1 : U_1)$, where the operation $\bigoplus$ is
the operand for Hessian’s addition law in projective coordinates. This fact enables us to use the addition formula for point doubling. In this sense, one can obtain a unified formula for point addition as a tool to improve the resistance of the point multiplication algorithm against side-channel attacks. In [15] the authors present a birational map between an elliptic curve given by $H_d$ and one $E$ in Weierstrass form. The coordinate map is given by

$$
\psi : (u, v) \mapsto (-9d^2 + \xi u, 3\xi(v - 1)),
$$

where $\xi = \frac{12(d^3 - 1)}{+v + 1}$, which sends points on $H_d$ onto points on $E : y^2 = x^3 - 27d(d^3 + 8)x + 54(d^6 - 20d^3 - 8)$. The inverse map is given by

$$
\psi^{-1} : (x, y) \mapsto (\eta(x + 9d^2), -1 + \eta(7d^3 - dx - 12)),
$$

where $\eta = \frac{6(d^3 - 1)(y + 9d^6 - yd - 36)}{(x + 9d^2)^2 + (dx - 12)^2}$.

An extension of the Hessian model for covering a greater range of elliptic curves was introduced by D. Bernstein, C. Chuengsatiansup, D. Kohel and T. Lange [2]. This model is given by $H_{a,d} : au^3 + v^3 + 1 = dwv$, and one can see that it is isomorphic to the Hessian curve $H_{a,d} : \hat{w}^3 + \hat{v}^3 + 1 = (a/a^{1/3})\hat{w}^3$ over an extension field $L$. For this, just take $\hat{u} = a^{1/3}$, $1 = v$ with $a^{1/3}$ a cubic root of $a$ in the extension $L$. For completeness, the Hessian curve is a special case of the Twisted Hessian curve where $a = 1$. Let $P_1 = (u_1, v_1)$ and $P_2 = (u_2, v_2)$ be points on $H_{a,d}$ with $P_1 \neq P_2$; then, the coordinates of the resulting point $P_3 = (u_3, v_3) = P_1 + P_2$ are given by

$$
\begin{align*}
&u_3 = \frac{u_1 - v_1^2u_2v_2}{auv_1u_2^2 - v_2}, \\
&v_3 = \frac{v_1v_2^2 - au_2u_3v_2}{auv_1u_2^2 - v_2}.
\end{align*}
$$

For point doubling, the coordinates of $P_3 = (u_3, v_3) = [2]P_1$ are given by

$$
\begin{align*}
&u_3 = \frac{u_1 - v_1^3u_1}{av_1u_1^3 - v_1}, \\
&v_3 = \frac{v_1^3 - au_1^3}{av_1u_1^3 - v_1}.
\end{align*}
$$

The curve $H_{a,d}$ is birationally equivalent over a field $K$ to the Weierstrass curve $E_W : y^2 = x^3 - \frac{d^3 + 216da}{48} + \frac{d^6 - 54d^3a - 8\pi a^2}{864}$ via the maps

$$
\begin{align*}
\psi : H_{a,d} \rightarrow E_W, (u, v) \mapsto &\left(\frac{(d^3 - 27a)u}{3(3v + du)} - \frac{d^2}{4}, \left(\frac{(d^3 - 27a)(1 - v)}{2(3 + 3v + du)}\right)\right), \\
\phi : E_W \rightarrow E_{a,d}, (x, y) \mapsto &\left(-\frac{18d^2 + 72x}{d^3 - 12dx - 108a + 24y}, \left(\frac{48y}{d^3 - 12dx - 108a + 24y}\right)\right).
\end{align*}
$$

The map $\psi$ is regular on every point of $H_{a,d}$, except the point $(0, -1)$. The map $\phi$ is regular on every point of $E_W$, except the points $(x, y)$ where $d^3 - 12dx - 108a + 24y = 0$.

2.4. Jacobi Intersection’s Model. The last model presented in this paper is named Jacobi Intersection Model [12]. Each curve in this model is given by the intersection of two quadratic surfaces in three dimensional space over a base field. Jacobi Intersection curves, defined over a field $K$, can be expressed by

$$
J_a : \begin{cases}
s^2 + c^2 = 1 \\
as^2 + d^2 = 1,
\end{cases}
$$

with $a \in K$, $a(1 - a) \neq 0$ and $a \neq 0, 1$. The point $(0, 1, 1)$ is the identity element of $J_a$ and, given the point $P = (s, c, d)$, $-P = (-s, c, d)$ is the inverse element of...
Given two points in the Jacobi Intersection model, e.g. \( P_1 = (s_1, c_1, d_1) \) and \( P_2 = (s_2, c_2, d_2) \), the expression for the result point \( P_3 = P_1 + P_2 = (s_3, c_3, d_3) \) via point addition is given by

\[
s_3 = \frac{c_2 s_1 d_2 + d_1 s_2 c_1}{c_2^2 + (d_1 s_2)^2}, \quad c_3 = \frac{c_2 s_1 - d_1 s_2 c_1}{c_2^2 + (d_1 s_2)^2}, \quad d_3 = \frac{d_1 d_2 - a s_1 c_2}{c_2^2 + (d_1 s_2)^2}.
\]

For point doubling, the coordinates of \( P_3 = (s_3, c_3, d_3) = [2]P_1 \) are given by

\[
s_3 = \frac{2c_2 s_1 d_1}{c_1^2 + (d_1 s_1)^2}, \quad c_3 = \frac{c_1^2 - s_1^2 d_1^2}{c_1^2 + (d_1 s_1)^2}, \quad d_3 = \frac{d_1^2 - a s_1^2 c_1^2}{c_1^2 + (d_1 s_1)^2}.
\]

3. Isogenies

For our purposes, we will define and work with isogenies between elliptic curves over finite fields, but this definition is not limited to these fields. A more general and abstract approach can be found in [20]. Fix a prime \( p \) and a power \( q = p^k \), with \( k \in \mathbb{N} \), and let \( E_1 \) and \( E_2 \) be elliptic curves over \( K = \mathbb{F}_q \). An isogeny \( \phi : E_1 \to E_2 \) is a non-constant algebraic morphism

\[
\phi(x, y) = \left( \frac{f_1(x, y)}{g_1(x, y)}, \frac{f_2(x, y)}{g_2(x, y)} \right),
\]

with \( \phi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2} \) and \( f_i, g_i \) polynomials for \( i \in \{1, 2\} \).

More specifically, \( \phi \) is a group homomorphism between \( E_1(\mathbb{F}_q) \) and \( E_2(\mathbb{F}_q) \), i.e., given \( P, Q \in E_1(\mathbb{F}_q) \) we have \( \phi(P + Q) = \phi(P) + \phi(Q) \), where + is the elliptic curve point addition. The degree of an isogeny is its degree as a rational map and, for separable isogenies, it is the size of its kernel. Theorem 3.1 from [22, Section 12.5] gives us a necessary and sufficient condition for two elliptic curves to be isogenous. In order to explicitly compute the polynomials that make up the isogeny of the form defined above, we can use a formula due to Vélu [21] which is given in Theorem 3.2.

**Theorem 3.1 (Tate).** Let \( E_1 \) and \( E_2 \) be elliptic curves defined over \( \mathbb{F}_q \), where \( q = p^k \) and \( k \in \mathbb{N} \). \( E_1 \) is isogenous to \( E_2 \) if, and only if, \( \#E_1 = \#E_2 \).

**Theorem 3.2 (Vélu’s Formula).** Consider the underlying field \( K \) such that \( char(K) \) is not equal to 2 or 3. Let \( E : y^2 = x^3 + Ax + B \) be an elliptic curve in Short Weierstrass form. Let \( G \) be a subgroup of \( E(K) \) with order \( l \), \( l \) prime. Let \( S \) be the set of representatives of \( G/\sim \), where \( \sim \) is such that \( P \sim Q \iff P = \pm Q \). Then, there exists an isogeny \( \phi : E \to E' \), where \( ker(\phi) = G \), given by

\[
\phi(x, y) = \left( x + \sum_{Q \in S} \left[ \frac{t_Q}{x - x_Q} + \frac{\mu_Q}{(x - x_Q)^2} \right], \right.
\]

\[
y - \sum_{Q \in S} \left[ \frac{2y}{(x - x_Q)^3} + \frac{y - y_Q}{(x - x_Q)^2} - \frac{g_Q^y g_Q^x}{(x - x_Q)^2} \right], \right)
\]

where \( Q = (x_Q, y_Q) \), \( \mu_Q = (g_Q^y)^2 \), with \( t_Q = g_Q^y \) (if \( Q = -Q \)) or \( t_Q = -2g_Q^x \) (if \( Q \neq -Q \)), \( g_Q^x = 3x_Q^2 + A \), and \( g_Q^y = -2y_Q \). Furthermore, we have \( t = \sum_{Q \in S} t_Q, \ w = \sum_{Q \in S} \mu_Q + \mu_Q t_Q \). The application of Vélu’s formula gives us the coefficients of \( E' \): \( y^2 = x^3 + (A - 5t)x + (B - 7w) \) and a normalized isogeny whose kernel is \( S \).

A straight observation of the above formula shows that in order to compute an isogeny we need \( \mathcal{O}(|G|) \) operations in the underlying field \( K \).
4. Jacobi Intersection Curve Isogenies

We initiate this section with the purpose of presenting an approach for isogeny evaluation and computation for curves given in the Jacobi Intersection model. Instead of Vélu’s addition version for the isogeny formula, our multiplicative version is compact and is derived mainly from exploring a simple point negation formula in this model. Theorem 4.1 states our approach in full.

**Theorem 4.1.** Suppose \( F \) is a subgroup of the Jacobi Intersection curve \( J_a \) with odd order \( l = 2k + 1 \), and points

\[
F = \{(0, 1, 1), (\pm \alpha_1, \beta_1, \gamma_1), \ldots, (\pm \alpha_k, \beta_k, \gamma_k)\}.
\]

Define

\[
\psi(P) = \begin{cases} 
O, & \text{if } P \in F \\
\left( s_P \prod_{Q \in F} \frac{s_{P+Q}}{s_Q}, c_P \prod_{Q \in F} \frac{c_{P+Q}}{c_Q}, d_P \prod_{Q \in F} \frac{d_{P+Q}}{d_Q} \right), & \text{if } P \notin F.
\end{cases}
\]

Then \( \psi \) is an \( l \)-isogeny, with kernel \( F \), from the curve \( J_a \) to the curve \( J_{\hat{a}} \) where

\[
\hat{a} = a - 2a \sum_{i=1}^{k} \left( \frac{\alpha_i^3}{\beta_i^2} + 2 \alpha_i^2 - 1 \right).
\]

When \( P \notin F \), the coordinate maps are given by \( \psi(S(s, c, d), C(s, c, d), D(s, c, d)) \) as

\[
S(s, c, d) = \frac{A^2}{s} \prod_{i=1}^{k} \frac{\beta_i^2 s^2 \gamma_i^2 - d^2 \alpha_i^2 c^2}{(\beta_i^2 + d^2 \alpha_i^2)^2},
\]

\[
C(s, c, d) = \frac{c}{B^2} \prod_{i=1}^{k} \frac{\beta_i^2 c^2 - d^2 \alpha_i^2 s^2 \gamma_i^2}{(\beta_i^2 + d^2 \alpha_i^2)^2},
\]

\[
D(s, c, d) = \frac{d}{G^2} \prod_{i=1}^{k} \frac{d^2 \gamma_i^2 - a^2 s^2 c^2 \alpha_i^2 \beta_i^2}{(\beta_i^2 + d^2 \alpha_i^2)^2},
\]

with \( A = \prod_{i=1}^{k} \alpha_i, \) \( B = \prod_{i=1}^{k} \beta_i \) and \( G = \prod_{i=1}^{k} \gamma_i \).

**Proof.** It is easy to see that \( F \) is the kernel of the isogeny \( \psi \) and \( \psi(0, 1, 1) = (0, 1, 1) \).

Now, we need to derive \( \hat{a} \) in the image curve \( J_{\hat{a}} : \begin{cases} S^2 + C^2 = 1 \\
\hat{a}S^2 + D^2 = 1
\end{cases} \), where \( S, C, D \) are functions of the coordinate maps. To accomplish this, we consider the functions

\[
G(s, c, d) = S^2(s, c, d) + C^2(s, c, d) - 1
\]

\[
H(s, c, d) = \hat{a}S^2(s, c, d) + D^2(s, c, d) - 1
\]

and solve them for \( \hat{a} \). We can use the fact that if \( 5 \) is identically zero, the codomain curve will be a Jacobi Intersection curve. One more step is to notice that the maps \( 2, 3, \) and \( 4 \) preserve the points \((0, 1, 1), (0, -1, 1), (0, 1, -1), (0, -1, -1)\) and these four points are the points with the \( s \)-coordinate equal to zero. Looking at the codomain curve, these points are also the unique points with \( s \)-coordinate equal to zero. Following this, we can observe that \( \begin{cases} G(s, c, d) = S^2(s, c, d) + C^2(s, c, d) - 1 \\
H(s, c, d) = \hat{a}S^2(s, c, d) + D^2(s, c, d) - 1
\end{cases} \) has four zeros at \( s = 0 \). Now, we will analyze if either theses points are singular or not.
and then classify the zeros of $5$ as simple zeros or not. We start by computing the partial derivatives of $5$:

\begin{equation}
\begin{aligned}
G_s(s, c, d) &= 2SS_s + 2CC_s \\
H_s(s, c, d) &= 2aSS_s + 2DD_s,
\end{aligned}
\end{equation}

\begin{equation}
\begin{aligned}
G_c(s, c, d) &= 2SS_c + 2CC_c \\
H_c(s, c, d) &= 2aSS_c + 2DD_c.
\end{aligned}
\end{equation}

\begin{equation}
\begin{aligned}
G_d(s, c, d) &= 2SS_d + 2CC_d \\
H_d(s, c, d) &= 2aSS_d + 2DD_d.
\end{aligned}
\end{equation}

For the point $(0, 1, 1)$ we have 6, 7, and 8 as

\begin{equation}
\begin{aligned}
G_s(0, 1, 1) &= 2C_s(0, 1, 1) \\
H_s(0, 1, 1) &= 2D_s(0, 1, 1), \\
G_c(0, 1, 1) &= 2C_c(0, 1, 1) \\
H_c(0, 1, 1) &= 2D_c(0, 1, 1), \\
G_d(0, 1, 1) &= 2C_d(0, 1, 1) \\
H_d(0, 1, 1) &= 2D_d(0, 1, 1).
\end{aligned}
\end{equation}

Let

\begin{equation}
\begin{aligned}
R_i &= \frac{\beta_i^2\gamma_i^2 - a_2^2\alpha_i^2\gamma_i^2}{(\beta_i^2 + d^2\alpha_i^2)^2}, \\
S_i &= \frac{\beta_i^2\alpha_i^2 - a_2^2\alpha_i^2\gamma_i^2}{(\beta_i^2 + d^2\alpha_i^2)^2}, \\
T_i &= \frac{d^2\gamma_i^2 - a_2^2\alpha_i^2\gamma_i^2}{(\beta_i^2 + d^2\alpha_i^2)^2},
\end{aligned}
\end{equation}

be the coordinate maps of 2, 3, and 4, respectively. We have that

\begin{equation}
\begin{aligned}
R_i(0, 1, 1) &= -\frac{\alpha_i^2}{(\beta_i^2 + d^2\alpha_i^2)^2} = -\alpha_i^2, \\
S_i(0, 1, 1) &= \frac{\beta_i^2}{(\beta_i^2 + d^2\alpha_i^2)^2} = \beta_i^2, \\
T_i(0, 1, 1) &= \frac{\gamma_i^2}{(\beta_i^2 + d^2\alpha_i^2)^2} = \gamma_i^2, \\
\end{aligned}
\end{equation}

where $(\beta_i^2 + \alpha_i^2)^2 = 1$ by the curve equation. Next, by applying the chain rule for partial derivatives related to $s$, $c$, and $d$ of 2, 3 and 4 we obtain

\begin{equation}
\begin{aligned}
C_s(0, 1, 1) &= \frac{1}{B^2} \left( S_{i_1} \prod_{i=2}^{k} (\beta_i^2) + S_{i_2} \prod_{i=1, i \neq 2}^{k} (\beta_i^2) + ... + S_{i_k} \prod_{i=1}^{k-1} (\beta_i^2) \right) = \sum_{i=1}^{k} \frac{S_{i_1}(0, 1, 1)}{\beta_i^2},
\end{aligned}
\end{equation}

\begin{equation}
\begin{aligned}
C_c(0, 1, 1) &= \frac{1}{B^2} \prod_{i=2}^{k} S_{i_1} + \frac{1}{B^2} \left( S_{i_1} \prod_{i=2}^{k} (\beta_i^2) + S_{i_2} \prod_{i=1, i \neq 2}^{k} (\beta_i^2) + ... + S_{i_k} \prod_{i=1}^{k-1} (\beta_i^2) \right) \\
&= 1 + \sum_{i=1}^{k} \frac{S_{i_1}(0, 1, 1)}{\beta_i^2},
\end{aligned}
\end{equation}

\begin{equation}
\begin{aligned}
C_d(0, 1, 1) &= \frac{1}{B^2} \left( S_{i_1} \prod_{i=2}^{k} (\beta_i^2) + S_{i_2} \prod_{i=1, i \neq 2}^{k} (\beta_i^2) + ... + S_{i_k} \prod_{i=1}^{k-1} (\beta_i^2) \right) = \sum_{i=1}^{k} \frac{S_{i_1}(0, 1, 1)}{\beta_i^2}.
\end{aligned}
\end{equation}

In order to compute the partial derivatives given above at $(0, 1, 1)$, we need to compute $S_{i_1}(0, 1, 1)$, $S_{i_2}(0, 1, 1)$, and $S_{i_k}(0, 1, 1)$.}

\begin{equation}
S_{i_1} = \frac{-2d^2\alpha_i^2\gamma_i^2 - \beta_i^2\alpha_i^2\gamma_i^2}{(\beta_i^2 + d^2\alpha_i^2)^2}, \quad S_{i_2}(0, 1, 1) = 0,
\end{equation}
Isogeny formulas for Jacobi intersection and twisted Hessian curves

\[(10) \quad S_{t_e} = \frac{2 \beta_i^2 c}{(\gamma_i^2 + d \alpha_i^2)^2}, \quad S_{t_e}(0, 1, 1) = 2 \beta_i^2,\]

\[(11) \quad S_{t_d} = \frac{-2 \alpha_i^2 s \gamma_i^2}{(\gamma_i^2 + d \alpha_i^2)^2}, \quad S_{t_d}(0, 1, 1) = 0.\]

From 9, 10, and 11, we have \(C_s(0, 1, 1) = 0, C_c(0, 1, 1) = 1 + 2k,\) and \(C_d(0, 1, 1) = 0.\) Similar computation can be done to obtain \(D_s(0, 1, 1), D_c(0, 1, 1),\) and \(D_d(0, 1, 1)\) as follows:

\[
D_s(0, 1, 1) = \frac{1}{G^2} \left( T_{t_e} \prod_{i=2}^{k} (\gamma_i^2) + T_{t_s} \prod_{i=1, i \neq 2}^{k} (\gamma_i^2) + \ldots + T_{t_k} \prod_{i=1}^{k-1} (\gamma_i^2) \right) = \sum_{i=1}^{k} \frac{T_{t_e}(0, 1, 1)}{\gamma_i^2},
\]

\[
D_c(0, 1, 1) = \frac{1}{G^2} \left( T_{t_e} \prod_{i=2}^{k} (\gamma_i^2) + T_{t_s} \prod_{i=1, i \neq 2}^{k} (\gamma_i^2) + \ldots + T_{t_k} \prod_{i=1}^{k-1} (\gamma_i^2) \right) = \sum_{i=1}^{k} \frac{T_{t_c}(0, 1, 1)}{\gamma_i^2},
\]

\[
D_d(0, 1, 1) = \frac{1}{G^2} \prod_{i=2}^{k} T_{t_d} + \frac{1}{G^2} \left( T_{t_d} \prod_{i=2}^{k} (\gamma_i^2) + T_{t_s} \prod_{i=1, i \neq 2}^{k} (\gamma_i^2) + \ldots + T_{t_k} \prod_{i=1}^{k-1} (\gamma_i^2) \right)
\]

\[
= 1 + \sum_{i=1}^{k} \frac{T_{t_d}(0, 1, 1)}{\gamma_i^2},
\]

with

\[(12) \quad T_{t_e} = -\frac{2 a_i^2 c^2 c \gamma_i^2}{(\beta_i^2 + d \alpha_i^2)^2}, \quad T_{t_e}(0, 1, 1) = 0,\]

\[(13) \quad T_{t_c} = -\frac{2 a_i^2 s^2 c \alpha_i^2 \beta_i^2}{(\beta_i^2 + d \alpha_i^2)^2}, \quad T_{t_c}(0, 1, 1) = 0,\]

\[(14) \quad T_{t_d} = \frac{2 \gamma_i^2 d^2}{\beta_i^2 + d \alpha_i^2}, \quad T_{t_d}(0, 1, 1) = 2 \gamma_i^2.\]

From 12, 13, and 14, we have \(D_s(0, 1, 1) = 0, D_c(0, 1, 1) = 0,\) and \(D_d(0, 1, 1) = 1 + 2k.\) Therefore, we conclude that 6, 7, and 8 are not simultaneously zero when evaluated at \((0, 1, 1),\) consequently, they have simple zeros at \((0, 1, 1).\) Similar computation can be done for the other points with s-coordinate equal to zero. Now, with the purpose of deriving \(\hat{a}\) in the codomain curve equation, we will work with the power series of 2, 3, and 4 at \(s = 0.\) First, we replace \(c^2 = 1 - s^2\) and \(d^2 = 1 - a s^2\) and then obtain \(S(s), C(s),\) and \(D(s)\) as univariate rational functions.

\[
S(s) = s \prod_{i=1}^{k} \left( -1 + \left( \frac{\beta_i^2 \gamma_i^2}{\alpha_i^2} - 2 a \alpha_i^2 + a + 1 \right) s^2 + O(s^4) \right),
\]

\[
C(s) = c \prod_{i=1}^{k} \left( 1 + \left( \frac{-\alpha_i^2 \gamma_i^2}{\beta_i^2} + 2 a \alpha_i^2 - 1 \right) s^2 + O(s^4) \right),
\]

\[
D(s) = d \prod_{i=1}^{k} \left( 1 + \left( \frac{-a \alpha_i^2 \beta_i^2}{\gamma_i^2} + 2 a \alpha_i^2 - a \right) s^2 + O(s^4) \right).
\]
Then,

\[
S^2(s) = s^2 \prod_{i=1}^{k} \left( -1 + \left( \frac{\beta_i^2 \gamma_i^2}{\alpha_i^2} - 2a\alpha_i^2 + a + 1 \right) s^2 + O(s^4) \right)^2
\]

\[
= s^2 + \left( 2 \sum_{i=1}^{k} \left( \frac{\beta_i^2 \gamma_i^2}{\alpha_i^2} - 2a\alpha_i^2 + a + 1 \right) \right) s^4 + O(s^5),
\]

(15)

\[
C^2(s) = 1 + \left( -1 + 2 \sum_{i=1}^{k} \left( \frac{-\alpha_i \gamma_i}{\beta_i^2} + 2a\alpha_i^2 - 1 \right) \right) s^2 + O(s^4),
\]

(16)

\[
D^2(s) = 1 + \left( -a + 2 \sum_{i=1}^{k} \left( \frac{-a\alpha_i \gamma_i}{\beta_i^2} + 2a\alpha_i^2 - a \right) \right) s^2 + O(s^4).
\]

(17)

Our next step is to replace 15, 16, and 17 into 5, name it \( \left\{ \begin{array}{l} G'(s) \\ H'(s) \end{array} \right\} \) and obtain

\[
G'(s) = s^2 + O(s^4) + 1 + \left( -1 + 2 \sum_{i=1}^{k} \left( \frac{-\alpha_i \gamma_i}{\beta_i^2} + 2a\alpha_i^2 - 1 \right) \right) s^2 + O(s^4) - 1
\]

\[
= \left( 2 \sum_{i=1}^{k} \left( \frac{-\alpha_i \gamma_i}{\beta_i^2} + 2a\alpha_i^2 - 1 \right) \right) s^2 + O(s^4),
\]

\[
H'(s) = \hat{a}(s^2 + O(s^4)) + 1 + \left( -a + 2 \sum_{i=1}^{k} \left( \frac{-a\alpha_i \gamma_i}{\beta_i^2} + 2a\alpha_i^2 - a \right) \right) s^2 + O(s^4) - 1
\]

\[
= \left( \hat{a} - a + 2a \sum_{i=1}^{k} \left( \frac{-\alpha_i \gamma_i}{\beta_i^2} + 2a\alpha_i^2 - 1 \right) \right) s^2 + O(s^4).
\]

If we suppose that the coefficient of \( s^2 \) is equal to zero in \( H'(s) \), then \( H'(s) \) has a zero of order greater than two in \( s = 0 \). Consequently, \( H'(s) \) must be identically zero. Now, we can set the coefficient of \( s^2 \) to zero in \( H'(s) \) and solve for \( \hat{a} \) which yields to

\[
\hat{a} = a - 2a \sum_{i=1}^{k} \left( \frac{-\alpha_i \gamma_i}{\beta_i^2} + 2a\alpha_i^2 - 1 \right).
\]

Thus, by choosing \( \hat{a} \) of this form, the functions \( G \) and \( H \) are identically zero and the codomain of this map is another valid Jacobi Intersection curve. Hence, the transformations in 2, 3, and 4 form rational maps from a Jacobi Intersection curve to another one that preserves the identity point.

5. Twisted Hessian curve isogenies

In this section, we present a similar isogeny map construction given for Jacobi Intersection curves presented in Section 4. Here, we just present the maps used as isogeny evaluation for Twisted Hessian curves. Our goal in this section is to highlight how efficient isogenies formulas in the Twisted Hessian model could be produced using the same technique as applied for Jacobi Intersection curves. So, it is an open problem to know if these proposed maps send points on an initial Twisted Hessian curve to points on an isogenous curve with specified coefficients \( \hat{a} \) and \( \hat{d} \) in
the base field $K$. Following, we present analogous construction for isogenies in the Twisted Hessian model. We start supposing $F$ is a subgroup of the Twisted Hessian curve $H_{a,d}$ with odd order $l = 2k + 1$, and points

$$F = \{(0, -1), (\alpha_1, \beta_1), ..., (\alpha_k, \beta_k), \left(\frac{\alpha_1}{\beta_1}, 1\right), ..., \left(\frac{\alpha_k}{\beta_k}, 1\right)\}.$$ 

Define

$$\psi(P) = \begin{cases} 
O, & \text{if } P \in F \\
\left(u_P \prod_{Q \in F} \frac{u_{P+Q}}{u_Q}, v_P \prod_{Q \in F} v_{P+Q}\right), & \text{if } P \notin F.
\end{cases}$$

Then $\psi$ is supposed to be an $l$-isogeny, with kernel $F$, from curve $H_{a,d}$ to a curve $H_{\hat{a},\hat{d}}$. When $P \notin F$, the coordinate maps are given by $\psi(U(u,v), V(u,v))$ as

$$U(u,v) = u \prod_{i=1}^{k} \frac{(u - \alpha_i \beta_i v^2)(\beta_i^2 u - \alpha_i v^2)}{(\alpha \beta_i^2 u v - \beta_i)^2},$$

$$V(u,v) = v \prod_{i=1}^{k} \frac{(\beta_i^2 v - a \alpha_i \beta_i u^2)(v - a \alpha_i \beta_i u^2)}{(\alpha \beta_i^2 u v - \beta_i)^2},$$

with $A = \prod_{i=1}^{k} \alpha_i$ and $B = \prod_{i=1}^{k} \beta_i$. We present below the idea that should be used to show that the above maps are, indeed, an isogeny between Twisted Hessian elliptic curves. The first step is to notice that $F$ is the kernel of the map $\psi$ and $\psi(0, -1) = (0, -1)$. Next step is to derive $\hat{a}$ and $\hat{d}$ in the image curve $H_{\hat{a},\hat{d}}$: $\hat{a}U^3 - V^3 + 1 = \hat{d}UV$, where $U, V$ are functions of the coordinate maps. For accomplish this, we consider the function

$$G(u,v) = \hat{a}U^3(u,v) + V^3(u,v) + 1 - \hat{d}U(u,v)V(u,v),$$

and solve them for $\hat{a}$ and $\hat{d}$. We can assume that $21$ is identically zero and the codomain curve will be a Twisted Hessian curve. One more step is to notice that the maps $19$ and $20$ preserve the point $(0, -1)$ which is the point with $u$-coordinate equal to zero. Looking at the codomain curve, this point is the unique point with $u$-coordinate equal to zero. Following this, we can observe that $G(u,v)$ has one zero at $u = 0$. Following, we analyze if theses points are singular or not and then classify the zeros of $21$ as simple zeros or not. We start by computing the partial derivatives of $21$:

$$G_u(u,v) = 3\hat{a}U^2 U_u + 3V^2 V_u - \hat{d}(U_u V + V_u U),$$

$$G_v(u,v) = 3\hat{a}U^2 U_v + 3V^2 V_v - \hat{d}(U_v V + V_v U).$$

Now, evaluating the point $(0, -1)$ at $22$ and $23$ we have $G_u(0, -1) = 3V_u + \hat{d}U_u$ and $G_v(0, -1) = 3V_v + \hat{d}U_v$. Let

$$R_i = \frac{(u - \alpha_i \beta_i v^2)(\beta_i^2 u - \alpha_i v^2)}{(\alpha \beta_i^2 u v - \beta_i)^2}, \quad S_i = \frac{(\beta_i^2 v - a \alpha_i \beta_i u^2)(v - a \alpha_i \beta_i u^2)}{(\alpha \beta_i^2 u v - \beta_i)^2},$$

be the coordinate maps of $19$ and $20$, respectively. We have that

$$R_i(0, -1) = \frac{-\alpha_i \beta_i \beta_i^2}{\beta_i^2} = \frac{\alpha_i^2}{\beta_i}, \quad S_i(0, -1) = \frac{-\beta_i^2 (-1)}{\beta_i} = \frac{\beta_i^2}{\beta_i} = 1.$$
Next, applying the chain rule for partial derivatives related to \( u \) and \( v \) of 19 and 20 we obtain

\[
U_u(0, -1) = \prod_{i=1}^{k} R_i(0, -1) = \prod_{i=1}^{k} \frac{\alpha_i^2}{\beta_i} = \frac{A^2}{B},
\]

\[
U_v(0, -1) = 0,
\]

\[
V_u(0, -1) = - \left( S_{1_u} \prod_{i=2}^{k} (1) + S_{2_u} \prod_{i=1, i \neq 2}^{k} (1) + \ldots + S_{k_u} \prod_{i=1}^{k-1} (1) \right)
= - \sum_{i=1}^{k} S_{i_u}(0, -1),
\]

\[
V_v(0, -1) = \sum_{i=2}^{k} S_i - \left( S_{1_v} \prod_{i=2}^{k} (1) + S_{2_v} \prod_{i=1, i \neq 2}^{k} (1) + \ldots + S_{k_v} \prod_{i=1}^{k-1} (1) \right) = 1 - \sum_{i=1}^{k} S_{i_v}(0, -1).
\]

The computation of partial derivatives given above at the point \((0, -1)\) depends of the values \( S_{i_u}(0, -1) \) and \( S_{i_v}(0, -1) \). Firstly, we need to compute the partial derivatives of \( S_i \) and then evaluate the result at \((0, -1)\):

\[
(24) \quad S_{i_u}(0, -1) = \frac{-2a\alpha_i^2}{\beta_i},
\]

\[
(25) \quad S_{i_v}(0, -1) = \frac{2}{\beta_i}.
\]

From 24 and 25, we have \( V_u(0, -1) = -\sum_{i=1}^{k} \frac{-2a\alpha_i^2}{\beta_i} \) and \( V_v(0, -1) = 1 + \sum_{i=1}^{k} \frac{2}{\beta_i} \).

Replacing \( V_u(0, -1) \) and \( V_v(0, -1) \) in \( G_u(0, -1) \) and \( G_v(0, -1) \) we have

\[
G_u(0, -1) = -3 \sum_{i=1}^{k} \frac{2a\alpha_i^2}{\beta_i} + \hat{d}A^2/B,
\]

\[
G_v(0, -1) = 3 \left( 1 + \sum_{i=1}^{k} \frac{2}{\beta_i} \right) + \hat{d}0 = 3 \left( 1 + \sum_{i=1}^{k} \frac{2}{\beta_i} \right).
\]

So, we see that the points of coordinate \( u = 0 \) are simple zeros of the coordinate maps. After showing this, it is necessary to derive the coefficients of the isogenous curve. Following the exact procedure as did for Jacobi Intersection could not allows to construct the coefficients of the isogenous curve.

A way to get around this situation and, at least, generate the coefficient of the isogenous curve (but we would not be properly demonstrating that they are, in fact, isogenous) would be to find a particular point in the curve. Such a point would probably be defined over some extension of the base field. The choice of this point should be such that by replacing it in \( G(u, v) = \hat{a}U^3(u, v) + V^3(u, v) + 1 - dU(u, v)V(u, v) \) would obtain a simple expression for the coefficients \( \hat{a} \) and \( d \).
6. Analysis of Operation Count

In this section we will analyze the cost of computing isogenies from a kernel points in Jacobi Intersection and Twisted Hessian models. We do not intend to give an exhaustive analysis of the computational complexity, but just an operation count to allow us to be able to compare it with other formulas. Following convention in open literature, $M$ stands for a field multiplication, $S$ for a field squaring, $C$ for a multiplication by a curve constant, and $I$ for a field inversion. We avoid to count additions and subtractions since their cost is much less than the cost of squarings and multiplications in the field. We initially analyze the functions derived for isogeny between Jacobi Intersection curves in affine coordinates:

$$S(s, c, d) = s \prod_{i=1}^{k} \frac{\beta_i^2 s^2 \gamma_i^2 - d^2 c^2}{(\beta_i^2 + d^2 \alpha_i^2)^2},$$

$$C(s, c, d) = c \prod_{i=1}^{k} \frac{c^2 - d^2 \alpha_i^2 s^2 \gamma_i^2}{(\beta_i^2 + d^2 \alpha_i^2)^2},$$

$$D(s, c, d) = d \prod_{i=1}^{k} \frac{d^2 - a^2 s^2 c^2 \alpha_i^2 \beta_i^2}{(\beta_i^2 + d^2 \alpha_i^2)^2}.$$

We start computing $s^2, s^4, c^2 = 1 - s^2, d^2 = 1 - a s^2, d^2 c^2 = (d^2 - a s^2 + a s^4), d^2 s^2 = s^2 - a s^4$ and $c^2 s^2 = s^2 - s^4$ at the cost of $2S + 1C$. Next, for each $i$ we need to compute $\frac{\beta_i^2 s^2 \gamma_i^2 - d^2 c^2}{(\beta_i^2 + d^2 \alpha_i^2)^2}$, $c^2 - d^2 \alpha_i^2 s^2 \gamma_i^2$, $d^2 - a^2 s^2 c^2 \alpha_i^2 \beta_i^2$, $e (\beta_i^2 + d^2 \alpha_i^2)^2$, which cost $(4C + 1S)k$. Now, the cost of computing $s \prod_{i=1}^{k} \frac{(s^2 \gamma_i^2 - d^2 c^2)^2}{(\beta_i^2 + d^2 \alpha_i^2)^2}$, $c \prod_{i=1}^{k} (c^2 - d^2 \alpha_i^2 s^2 \gamma_i^2)$, $d \prod_{i=1}^{k} (d^2 - a^2 s^2 c^2 \alpha_i^2 \beta_i^2)$, and $\prod_{i=1}^{k} (\beta_i^2 + d^2 \alpha_i^2)^2$ which cost $(3 + 4(k - 1))M$. In order to complete the calculation of the isogeny, we need to compute the inverse of $\prod_{i=1}^{k} (\beta_i^2 + d^2 \alpha_i^2)^2$ and perform 3 more multiplications $M$. Thus, the total cost (in affine coordinates) is given by $(4k + 2)M + (k + 2)S + (4k + 1)C + I$. Among the operations obtained so far to evaluate a point through isogeny is an inversion. Such an operation is very costly (about 100 times more costly than a multiplication one). To avoid it, we can work with projective coordinates. For

$$\psi(s, c, d, z) = (sz^3 \prod_{i=1}^{k} \frac{\beta_i^2 s^2 z^2}{\alpha_i^4 \gamma_i^2} - d^2 c^2 : cz^3 \prod_{i=1}^{k} \frac{c^2 z^2}{\alpha_i^2 \beta_i^2} - d^2 \alpha_i^2 \gamma_i^2,$$

we compute $z^2, c^2, \beta^2, d^2, z^2, c^2, s^2, d^2, s^2, d^2 c^2, c^2 s^2, s^2 z^2, c^2 z^2, d^2 z^2$ and, following similar computation made for the affine case, we obtain a total cost of $(4k + 7)M + 5S + (6k + 2)C$.

Following this analysis, we estimate the cost of isogeny evaluation for curves given in Twisted Hessian model, based on coordinate maps 19 and 20:

$$U(u, v) = u \prod_{i=1}^{k} \frac{(u - \alpha_i \beta_i v^2)(\beta_i^2 u - \alpha_i v^2)}{(\alpha_i u v - \beta_i^2 v^2)},$$
\[ V(u, v) = u \prod_{i=1}^{k} -\beta_i(\alpha_i^2 u^2 - v^2)(\beta_i v^2 - \alpha_i u^2). \]

First, we need to compute \( u^2, v^2 \) and \( uv \) which cost \( 1M + 2S \). For each value of \( i \) we need to compute \( (u - \alpha_i \beta_i v^2), (\beta_i^2 u - \alpha_i v^2), (u - \alpha_i \beta_i v^2)(\beta_i^2 u - \alpha_i v^2), -\beta_i(\alpha_i^2 u^2 - v^2), (\beta_i v^2 - \alpha_i u^2), -\beta_i(\alpha_i^2 u^2 - v^2)(\beta_i v^2 - \alpha_i u^2), \) and \((\alpha_i^2 u^2 v - \beta_i^2)^2\) with cost \((2M + 1S + 8C)k\). After that, we need to compute \( u \prod_{i=1}^{k} (u - \alpha_i \beta_i v^2)(\beta_i^2 u - \alpha_i v^2), v \prod_{i=1}^{k} -\beta_i(\alpha_i^2 u^2 - v^2)(\beta_i v^2 - \alpha_i u^2), \) and \( \prod_{i=1}^{k} (\alpha_i^2 u^2 v - \beta_i^2)^2 \) at the cost of \((2 + 3(k - 1))M\). To complete the evaluation of isogenies, we need to compute the inverse element of \( \prod_{i=1}^{k} (\alpha_i^2 u^2 v - \beta_i^2)^2 \) and two more multiplications \( M \) with cost \( 2M + I \). Finally, adding all the above costs to evaluate isogenies between curves in the Twisted Hessian model we get the total cost of \((5k + 2)M + (k + 2)S + (8k)C + I\).

Just as it was done for isogenies between curves in the Jacobi Intersection model, we will avoid inverse computations by working with projective coordinates. For isogenies of degree 101, our formula requires 23.4% less computation than the Huff model and 24.7% less computation than the Vélu formula for the Extended Model Jacobi Quartic. They showed that isogeny evaluation in this model can achieve performance comparable to that obtained for the Huff model if the constants are chosen carefully. Table 1 summarizes the operation cost for models presented in previous works as well as the cost obtained in our work. Table 2 seeks to present the results so that they can more easily be compared. In this case, the cost of operations is taken concerning the multiplication cost in the base field. Taking into account the values of the table, we can observe that the isogeny formula obtained for the Extended Jacobi Quartic model is more efficient than the formulas obtained for the Huff and Extended Jacobi Quartic models. It is noteworthy that the efficiency difference varies according to the values of \( k \) (i.e., the degree of isogeny we are computing). For example, for \( S = 0.8M \) and \( I = 100M \), our formula requires 46.8% less computation than the Huff model and 48% less computation than the given formula for the Extended Model Jacobi Quartic when computing isogenies of 3 degree. For the case in which one needs to compute isogenies of degree 101, our formula requires 23.4% less computation than the Huff model and 24.7% less computation than the formula for the Extended Jacobi Quartic model. Finally, Table 3 brings the comparison of the models of the literature to represent the isogenies formulas in projective coordinates. In Table 4, the total cost of each formula is compared after the conversion of the cost of operations to the cost of multiplying elements in the field on which the elliptic curve is defined.

\[1\text{Upper bound for the cost of evaluating a point on a Weierstrass curve via an \((2k+1)-\text{isogeny}.} \]
Table 1. Operation Counting for Isogenies Evaluation in Alternative Models in affine coordinates.

| MODEL                  | OPERATION COST                          |
|------------------------|-----------------------------------------|
| Edwards [17]           | \((3k + 1)M + 2S + 3kC + I\)            |
| Huff [17]              | \((4k - 2)M + 2S + 2kC + 2I\)          |
| Ext. Jacobi Quartic [24]| \((4k + 2)M + 3S + (7k + 4)C + 2I\)    |
| Weierstrass [17]       | \((3 + o(1))(2k + 1)M + S + (3 + o(1))(2k + 1)C + I\) |
| Intersec. de Jacobi    | \((4k + 2)M + 3S + (5k + 1)C + I\)     |
| Twisted Hessian        | \((5k + 2)M + 3S + (9k)C + I\)         |

Table 2. Operations Counting for Evaluation of Isogenies in Alternative Models, given in affine coordinates, as a function of the number of multiplications in the base field.

| MODEL                  | OPERATION COST                          |
|------------------------|-----------------------------------------|
| Edwards [17]           | \(I = 100M, S = 1M, *const = 0M\)     |
| Huff [17]              | \(I = 100M, S = 0.8M, *const = 0M\)    |
| Ext. Jacobi Quartic [24]| \(I = 100M\)                          |
| Weierstrass [17]       | \(I = 100M\)                          |
| Jacobi Intersection    | \((4k + 103)M\)                        |
| Twisted Hessian        | \((4k + 200)M\)                        |
|                       | \((4k + 199.6)M\)                     |
|                       | \((4k + 199.34)M\)                    |
|                       | \((4k + 205)M\)                       |
|                       | \((4k + 204.4)M\)                     |
|                       | \((4k + 204.01)M\)                    |
|                       | \((4k + 105)M\)                       |
|                       | \((4k + 104.4)M\)                     |
|                       | \((4k + 104.01)M\)                    |
|                       | \((5k + 105)M\)                       |
|                       | \((5k + 104.4)M\)                     |
|                       | \((5k + 104.01)M\)                    |

Table 3. Operations Counting for Isogenies Evaluation in Alternative Models using Projective Coordinates.

| MODEL                  | OPERATION COST                          |
|------------------------|-----------------------------------------|
| Edwards [17]           | \((3k + 3)M + 4S + 3kC\)               |
| Huff [17]              | \((4k + 3)M + 3S + 4kC\)               |
| Ext. Jacobi Quartic [24]| -                                       |
| Weierstrass [17]       | -                                       |
| Jacobi Intersection    | \((4k + 7)M + 5S + (6k + 2)C\)         |
| Twisted Hessian        | \((5k + 2)M + 3S + (9k)C\)             |

7. Conclusion

This work presents isogeny formulas for isogenies between curves in Jacobi Intersection and Twisted Hessian models, which complement the works of [17] and [24] for other elliptic curve models. These formulas are multiplicative and based on the addition law of each model in question. To the best of our knowledge, this is the first work to present this kind of formulas for both models. Our formulas achieve the cost of \((4k + 2)M + 3S + (5k + 1)C + I\) operations for Jacobi Intersection model and \((5k + 2)M + 3S + (9k)C + I\) for Twisted Hessian model, in affine coordinates. For projective coordinates, our formulas require \((4k + 7)M + 5S + (6k + 2)C\) operations for Jacobi Intersection model and \((5k + 2)M + 3S + (9k)C\) for Twisted Hessian model. We showed that our formula, for Jacobi Intersection isogenies, requires 46.8% less
Table 4. Operations Counting for Isogeny Evaluation on Alternative Models, using projective coordinates, as a function of the number of multiplications in the base field.

| MODEL                | OPERATION COST                                      |
|----------------------|-----------------------------------------------------|
|                      | $S = 1M,$                                           |
|                      | *$\text{const} = 0M$                                |
|                      | $S = 0.8M,$                                         |
|                      | *$\text{const} = 0M$                                |
|                      | $S = 0.67M,$                                        |
|                      | *$\text{const} = 0M$                                |
| Edwards [17]         | $(3k + 7)M$                                         |
|                      | $(3k + 6.2)M$                                       |
|                      | $(3k + 5.68)M$                                      |
| Huff [17]            | $(4k + 6)M$                                         |
|                      | $(4k + 5.4)M$                                       |
|                      | $(4k + 5.01)M$                                      |
| Ext. Jacobi Quartic [24] | -                                                 |
|                      | -                                                   |
|                      | -                                                   |
| Weierstrass [17]     | -                                                   |
|                      | -                                                   |
|                      | -                                                   |
| Jacobi Intersection  | $(4k + 12)M$                                        |
|                      | $(4k + 11)M$                                        |
|                      | $(4k + 10.35)M$                                     |
| Twisted Hessian      | $(5k + 5)M$                                         |
|                      | $(5k + 4.4)M$                                       |
|                      | $(5k + 4.01)M$                                      |

Computation than the Huff model and 48% less computation than the given formula for the Extended Model Jacobi Quartic when computing isogenies of 3 degree. In addition, when computing isogenies of degree 101, our formula requires 23.4% less computation than the Huff model and 24.7% less computation than the formula for the Extended Jacobi Quartic model. These costs are result of a brief analysis of the formulas obtained. Thus, the cost can be better estimated with a deeper analysis. We point out that as these formulas are constructed using the addition law; future improvements on formulas for adding points in these models may improve the isogeny formulas. As a future work, we plan to demonstrate that the formulas given for the Twisted Hessian model are, in fact, isogenies between curves in this model. Another research direction is to improve these formulas through the search for new addition formulas and evaluate using the composition of $l$-isogeny maps as point multiplication to speed up elliptic curve applications.

References
[1] D. J. Bernstein, P. Birkner, M. Joye, T. Lange and C. Peters, Twisted Edwards curves, Progress in cryptology—AFRICACRYPT 2008, Lecture Notes in Comput. Sci., Springer, Berlin, 5023 (2008), 389–405.
[2] D. J. Bernstein, C. Chuengsatiansup, D. Kohel and T. Lange, Twisted hessian curves, Progress in cryptology—LATINCRYPT 2015, Lecture Notes in Comput. Sci., Springer, Cham, 9230 (2015), 269–294, https://eprint.iacr.org/2015/781.
[3] D. Boneh and R. J. Lipton, Quantum cryptanalysis of hidden linear functions (extended abstract), Advances in Cryptology—CRYPTO ’95 (Santa Barbara, CA, 1995), Lecture Notes in Comput. Sci., Springer, Berlin, 963 (1995), 424–437.
[4] W. Castryck, T. Lange, C. Martindale, L. Panny and J. Renes, CSIDH: An efficient post-quantum commutative group action, Advances in cryptology—ASIACRYPT 2018. Part III, Lecture Notes in Comput. Sci., Springer, Cham, 11274 (2018), 395–427, https://eprint.iacr.org/2018/383.
[5] D. Charles, E. Goren and K. Lauter, Cryptographic hash functions from expander graphs, Journal of Cryptology, 22 (2009), 93–113, https://eprint.iacr.org/2006/021.
[6] L. Chen, D. Moody and Y.-K. Liu, National institute of standards and technology’s post-quantum cryptography standardization, (2017).
[7] A. Childs, D. Jao and V. Soukharev, Constructing elliptic curve isogenies in quantum subexponential time, Journal of Mathematical Cryptology, 8 (2014), 1–29.
[8] J.-M. Couveignes, Hard Homogeneous Spaces, Cryptology ePrint Archive, Report 2006/291, 2006, https://eprint.iacr.org/2006/291.
[9] H. M. Edwards, A normal form for elliptic curves, Bull. Amer. Math. Soc. (N.S.), 44 (2007), 393–422.
Isogeny formulas for Jacobi intersection and twisted Hessian curves

[10] K. Eisentraeger, S. Hallgren and T. Morrison, On the Hardness of Computing Endomorphism Rings of Supersingular Elliptic Curves, Cryptology ePrint Archive, Report 2017/986, 2017, https://eprint.iacr.org/2017/986.

[11] N. D. Elkies, Elliptic and modular curves over finite fields and related computational issues, Computational Perspectives on Number Theory (Chicago, IL, 1995), AMS/IP Stud. Adv. Math., Amer. Math. Soc., Providence, RI, 7 (1998), 21–76.

[12] R. Q. Feng, M. L. Nie and H. F. Wu, Twisted Jacobi intersections curves, Theory and Applications of Models of Computation, Berlin, Heidelberg, Springer Berlin Heidelberg, (2010), 199–210.

[13] L. De Feo and D. Jao, Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies, Post-Quantum Cryptography, Lecture Notes in Comput. Sci., Springer, Heidelberg, 7071 (2011), 19–34.

[14] D. Jao, R. Azarderakh, M. Campagna, C. Costello, L. De Feo, B. Hess, A. Jalali, B. Koziol, B. LaMacchia, P. Longa, M. Naehrig, J. Renes, V. Soukharev and D. Urbanik, Supersingular isogeny key encapsulation, NIST Post-Quantum Cryptography Standardization, Round 1 Submission, (2017).

[15] M. Joye and J.-J. Quisquater, Hessian elliptic curves and side-channel attacks, Cryptographic Hardware and Embedded Systems—CHES 2001 (Paris), Lecture Notes in Comput. Sci., Springer, Berlin, 2162 (2001), 402–410.

[16] M. Joye, M. Tibouchi and D. Vergnaud, Huff’s model for elliptic curves, ANTS 2010: Algorithmic Number Theory, (2010), 234–250.

[17] D. Moody and D. Shumow, Analogues of Vélu’s formulas for isogenies on alternate models of elliptic curves, Math. Comp., 85 (2016), 1929–1951.

[18] A. Rostovtsev and A. Stolbunov, Public-key cryptosystem based on isogenies, Cryptology ePrint Archive, Report 2006/145, 2006, https://eprint.iacr.org/2006/145.

[19] R. Schoof, Elliptic curves over finite fields and the computation of square roots mod p, Math. Comp., 44 (1985), 483–483.

[20] J. H. Silverman, The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics, 106, Springer-Verlag, New York, 1986.

[21] J. Vélu, Isogénies entre courbes elliptiques, C. R. Acad. Sci. Paris Sér. A-B, (273) (1972), A238–A241.

[22] L. C. Washington, Elliptic Curves: Number Theory and Cryptography, Second edition, Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2008.

[23] H. F. Wu and R. Q. Feng, Elliptic curves in Huff’s model, Wuhan University Journal of Natural Sciences, 17 (2012), 473–480.

[24] X. Xu, W. Yu, K. P. Wang and X. Y. He, Constructing isogenies on extended Jacobi quartic curves, Information Security and Cryptology, Lecture Notes in Comput. Sci., Springer, Cham, 10143 (2017), 416–427.

Received December 2018; revised December 2018.

E-mail address: jsilva@lasca.ic.unicamp.br
E-mail address: jlopez@ic.unicamp.br
E-mail address: rdahab@ic.unicamp.br