Analogues of Vélu's formulas for Isogenies on Alternate Models of Elliptic Curves

Dustin Moody*and Daniel Shumow†

October 18, 2011

Abstract

Isogenies of elliptic curves have been well-studied, in part because there are several cryptographic applications. Using Vélu's formula, isogenies can be evaluated explicitly given their kernel. However, Vélu's formula applies to elliptic curves given by a Weierstrass equation. In this paper we show how to similarly evaluate isogenies on Edwards curves and Huff curves. Edwards and Huff curves are new normal forms for elliptic curves, different than the traditional Weierstrass form.

1 Introduction

Isogenies are the structure preserving mappings between elliptic curves. As such, isogenies are an important mathematical object, and accordingly are also present in many different areas of elliptic curve cryptography. They have been used to analyze the complexity of the elliptic curve discrete logarithm [21], are used in the SEA point counting algorithm [13],[17], [31] and have been proposed as a mathematical primitive in the construction of cryptographic one-way functions such as hashes [8] and pseudo-random number generators [9]. Isogenies also play key roles in determining the endomorphism ring of an elliptic curve [4],[24], computing modular and Hilbert class polynomials [7], [33], and in the construction of new public key cryptosystems [20], [28],[32],[34].

Traditionally, elliptic curves have been specified by Weierstrass equations. However, this is merely one possible way to describe an elliptic curve. There are alternate models of elliptic curves which have been proposed for use in cryptography. Edwards curves, and to a lesser extent Huff curves, have been proposed as such alternative models. Expressing an elliptic curve with these models can lead to more efficient and secure arithmetic. The more efficient arithmetic comes from simpler point addition formulas which require less expensive operations like

*Computer Security Division, National Institute of Standards and Technology (NIST), Gaithersburg MD, USA, Email:dbmoody25@gmail.com

†eXtreme Computing Group, Microsoft Research, Redmond WA, USA. Email:danshu@microsoft.com

multiplication and division. These curves can also lead to improved security because the point addition formulas can be implemented with fewer special cases, reducing information leakage through side channels.

In an abstract sense, isogenies of elliptic curves are no different if the curve is specified with a Weierstrass equation, Edwards or Huff form. After all, these forms are all birationally equivalent (with the caveat that this may be over some extension of the field of definition.) However, in a computational sense, the model for the curve is important. We have explicit formulas for isogenies, derived from Vélu's formulas [35]. However, these formulas are tied to the Weierstrass equation of the curve. This paper presents explicit formulas for isogenies for Edwards and Huff curves. This is convenient as it allows one to compute isogenies directly on these alternate models, without converting back to Weierstrass form. However, this is also interesting from a computational perspective. Vélu's formulas are based on point addition formulas, and as these alternate models have more efficient addition formulas one may ask if the isogeny formulas for these models are also more efficient.

We note there are several computational problems pertaining to isogenies:

1. Given two elliptic curves E_1 and E_2, find an isogeny between them.
2. Given a compact representation of an isogeny, explicitly determine the kernel of the isogeny.
3. Given the kernel of an isogeny, determine the rational function form of the isogeny.
4. Given the rational function form of an isogeny, evaluate the isogeny on input points.

This paper primarily focuses on problem 3, while also touching upon problem 4. We will see that the formulas in this paper provide a more efficient solution for problem 4 than known results. For previous work on computing isogenies efficiently for Weierstrass curves see [5], [6], [10]. The only work on isogenies directly on Edwards curves we found in the literature is a recent article by Ahmadi and Granger where they find the number of isogeny classes of Edwards curve over a finite field [1].

This paper is organized as follows. In section 2 we review basic facts about elliptic curves, including isogenies and Vélu's formula. Section 3 covers Edwards curves and Huff curves. In sections 4 and 5, we present the analogue of Vélu's formula for Edwards and Huff curves respectively. We take a brief look at the computational cost (problem 4) of computing our formulas in section 6. Finally, we conclude in section 7 with directions for future study.

2 Elliptic Curves

2.1 Elliptic Curves

For the remainder of this paper, let K be a field with characteristic $\neq 2$. An elliptic curve E is a smooth complete projective curve of genus one with a given rational point. The curve can be written in Weierstrass form

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

with the $a_i \in K$. If the characteristic of K is also not 3, then E can also be written in short Weierstrass form,

$$E : y^2 = x^3 + ax + b.$$

For a curve in Weierstrass form, the given rational point is the point at infinity, denoted ∞. The condition that E be smooth means that there is no point of $E(\overline{K})$ where the partial derivatives simultaneously vanish.

The points of E with coordinates in K can be made into an abelian group under a suitable addition law. The addition law is given by rational functions. The identity element is the point ∞, and the inverse of a point $(x, y) \neq \infty$ is $(x, -y - a_1x - a_3)$.

2.2 Isomorphisms and isogenies

We recall a few basic facts about isogenies. For a more complete reference, see [30] or [36]. An isogeny is a nonconstant rational homomorphism (defined over K) from the curve E to another elliptic curve. Clearly if ϕ is an isogeny, then it must preserve the group identity. Conversely, it is known that any nonconstant rational map ϕ from E to another elliptic curve which preserves the group identity must be an isogeny. We will need this fact later on in sections 4 and 5. If the kernel of a (separable) isogeny ϕ is finite and has order l, then ϕ is known as an l-isogeny, and l is the degree of the isogeny. Any l-isogeny with l composite can be decomposed into a composition of prime degree isogenies, hence for the purposes of this paper we will assume that l is prime.

Two elliptic curves are isomorphic if and only if they have the same j-invariant. The j-invariant of the curve $y^2 = x^3 + ax + b$ is

$$j = 1728\frac{4a^3}{4a^3 + 27b^2}.$$

If two elliptic curves in Weierstrass form are isomorphic, there is a change of variables from one curve to the other of the form

$$(x, y) \to (u^2x + r, u^3y + u^2sx + t).$$

2.3 Vélu's formulae

For simplicity, we'll assume the characteristic of $K \neq 2, 3$. Let $E : y^2 = x^3 + ax + b$ be an elliptic curve. In [35], Vélu showed how to find the rational function form of an isogeny explicitly, given its kernel. Let ℓ be an odd prime. Let F be a subgroup of E of order ℓ, which we desire to be the kernel of our isogeny.

We define ϕ in the following way. For $P = (x_P, y_P) \notin F$, let

$$\phi(P) = \left(x_P + \sum_{Q \in F - \{\infty\}} (x_{P+Q} - x_Q), y_P + \sum_{Q \in F - \{\infty\}} (y_{P+Q} - y_Q) \right).$$

The points of F cause some difficulty, as x_∞ and y_∞ don't make sense. To get around this, we could use projective coordinates. We omit the details, because the basic idea is clear. For any point $P \in F$, we set $\phi(P) = \infty$. It is easy to see that ϕ is invariant under translation by elements of F, and that the kernel of ϕ is F. Using the group law on the curve, we also see that ϕ can be written in terms of rational functions.

To compute ϕ, first remove the point ∞ from F. Notice that if a point P is in F, then necessarily its inverse is also in F. Partition F into two sets F^+ and F^- such that $F = F^+ \cup F^-$, and $P \in F^+$ iff $-P \in F^-$. For each point $P \in F^+$, define the following quantities

$$g_P^x = 3x_P^2 + a, \qquad g_P^y = -2y_P,$$
$$v_P = 2g_P^x, \qquad u_P = (g_P^y)^2,$$
$$v = \sum_{P \in F^+} v_P, \qquad w = \sum_{P \in F^+} u_P + x_P v_P.$$

Then the ℓ-isogeny $\phi : E \to E'$ is given by

$$\phi(x, y) \to \left(x + \sum_{P \in F^+} \frac{v_P}{x - x_P} - \frac{u_P}{(x - x_P)^2}, y - \sum_{P \in F^+} \frac{2u_P y}{(x - x_P)^3} + v_P \frac{y - y_P - g_P^x g_P^y}{(x - x_P)^2} \right).$$

The equation for the image curve is $E' : y^2 = x^3 + (a - 5v)x + (b - 7w)$.

D. Kohel also showed how the isogeny ψ can be written in terms of its kernel polynomial [24]. The kernel polynomial is defined as

$$D(x) = \prod_{Q \in F - \{\infty\}} (x - x_Q) = x^{\ell-1} - \sigma x^{\ell-2} + \sigma_2 x^{\ell-3} - \sigma_3 x^{\ell-4} + \dots.$$

Then

$$\phi(x, y) = \left(\frac{N(x)}{D(x)}, y \left(\frac{N(x)}{D(x)} \right)' \right)$$

where $N(x)$ is related to $D(x)$ by

$$\frac{N(x)}{D(x)} = \ell x - \sigma - (3x^2 + a)\frac{D'(x)}{D(x)} - 2(x^3 + ax + b)\left(\frac{D'(x)}{D(x)} \right)'.$$

The polynomial $N(x)$ has degree ℓ. We can also determine the equation of the image E'. Set $v = a(\ell - 1) + 3(\sigma^2 - 2\sigma_2)$ and $w = 3a\sigma + 2b(\ell - 1) + 5(\sigma^3 - 3\sigma\sigma_2 + 3\sigma_3)$. Then the isogenous curve is $E' : y^2 = x^3 + (a - 5v)x + (b - 7w)$.

More generally, neither Vélu's paper nor Kohel's requires that l be odd or prime, nor E be given by a simplified Weierstrass equation, although the equations are easier in this case.

3 Edwards and Huff curves

3.1 Edwards curves

In 2007, H. Edwards introduced a new model for elliptic curves [12]. After a simple change of variables, these Edwards curves can be written in the form

$$E_d : x^2 + y^2 = 1 + dx^2y^2,$$

with $d \neq 1$. Twisted Edwards curves are a generalization of Edwards curves, proposed in [2]. These twisted curves are given by the equation

$$E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2,$$

where a and $d \neq 1$ are distinct, non-zero elements of K . Edwards curves are simply twisted Edwards curves with $a = 1$. The addition law for points on $E_{a,d}$ is given by:

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2} \right).$$

If a is a square and d is not a square in K, then the addition law is complete. This means that the addition formula is valid for all points, with no exceptions. The addition law for Weierstrass curves is not complete, which is one of the advantages of Edwards curves. A complete addition law provides some resistance to side-channel attacks. The addition law can also be implemented efficiently, which is important for cryptography [3].

The additive identity on $E_{a,d}$ is the point $(0, 1)$, and the inverse of the point (x, y) is $(-x, y)$. Note that the curve E_d always has a subgroup of order 4, namely $\{(0, 1), (0, -1), (1, 0),$ and $(-1, 0)\}$.

We can perform a birational transformation from $E_{a,d}$ to change its equation to a curve in Weierstrass form. The map

$$\phi_1 : (x, y) \to \left((a - d)\frac{1 + y}{1 - y}, (a - d)\frac{2(1 + y)}{x(1 - y)} \right) \tag{1}$$

sends the curve $E_{a,d}$ to the curve

$$E : y^2 = x^3 + 2(a + d)x^2 + (a - d)^2x.$$

Two points of order 4 on E are $(a - d, \pm 2\sqrt{a}(a - d))$, while $(0, 0)$ has order 2. The inverse transformation is the map

$$\phi_1^{-1} : (x, y) \to \left(\frac{2x}{y}, \frac{x - (a - d)}{x + (a - d)} \right).$$

3.2 Huff's curves

Joye, Tibouchi, and Vergnaud re-introduced the Huff model for elliptic curves in [22]. The model was used by Huff in 1948 to solve a certain diophantine equation [19]. The authors of [22] showed how the addition law makes Huff curves resistant to side-channel attacks, which is important in cryptographic settings. They also showed how to compute pairings on Huff curves. In [16], Wu and Feng gave an equivalent way to define Huff curves:

$$H_{a,b} : x(ay^2 - 1) = y(bx^2 - 1),$$

with $ab(a - b) \neq 0$. We will use this equation for Huff curves. The inverse of a point $P = (x, y)$ is $-P = (-x, -y)$, with the additive identity being $(0, 0)$. There are three points at infinity, and in projective coordinates these are $(1 : 0 : 0), (0 : 1 : 0)$, and $(a : b : 0)$. These points at infinity are also the three points of order two on the curve. Addition (for points which are not these points at infinity) is given by

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

There is also a simple birational transformation from a curve in Huff form to a curve in Weierstrass form [19]. The map is

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

with the equation of the curve in Weierstrass form $y^2 = x^3 + (a + b)x^2 + abx$. The inverse transformation is given by

$$(x, y) \to \left(\frac{x + a}{y}, \frac{x + b}{y} \right).$$

4 Isogenies on Edwards curves

4.1 Isomorphisms

We begin by examining isomorphisms between Edwards curves. For some $u \neq 0$, consider the map $I_u(x, y) = (x/u, y)$ from the twisted Edwards curve $E_{a,d}$. The image lies on the curve E_{u^2a,u^2d}, and it is easy to see this is an isomorphism. We also consider the map $I(x, y) = (x, 1/y)$, which takes a point on $E_{a,d}$ to a point on $E_{d,a}$. We now look for isomorphisms beyond these obvious ones.

Suppose Ψ is an isomorphism from E_d to some other Edwards curve $E_{\hat{d}}$. Let ϕ be the birational transformation from the curve E_d to a Weierstrass curve $E : y^2 = x^3 + 2(1 + d)x^2 + (1 - d)^2x$ and similarly let $\hat{\phi}$ be the birational transformation from $E_{\hat{d}}$ to a Weierstrass curve $\hat{E}$. Then it follows that E and $\hat{E}$ are isomorphic. From section 2.2, it is easy to check that the only isomorphisms between curves of the form $y^2 = x^3 + Ax^2 + Bx$ have as a map

$$I'(x, y) = (u^2x + r, u^3y),$$

for some $u \neq 0$. The easiest case is when $r = 0$. Composing the maps $I' \circ \phi$ we have a map from E_d to $y^2 = x^3 + 2(1+d)u^2x^2 + (1-d)^2u^4x$. This needs to be the same as $\hat{E} : y^2 = x^3 + 2(1+\hat{d})x^2 + (1-\hat{d})^2x$, from which we see that we require

$$(1+d)u^2 = 1+\hat{d},$$
$$(1-d)^2u^4 = (1-\hat{d})^2.$$

Solving for $\hat{d}$ in the first equation, and substituting this into the second equation yields that $u = \pm 1$, or $u^2 = 1/d$. When $u = \pm 1$ we get the identity or the negation map and $\hat{d} = d$. When $u^2 = 1/d$, then $\hat{d} = 1/d$ and the isomorphism is $I_{1/\sqrt{d}} : (x, y) \to (\pm\sqrt{d}x, 1/y)$ which maps E_d to $E_{1/d}$. Note that we define $I_{1/\sqrt{d}}(\pm 1, 0) = (\pm 1, 0)$.

In the case $r \neq 0$, then it can be checked that we must have $r^2 + 2(1+d)r + (1-d)^2 = 0$, so $r = -1 - d \pm \sqrt{d}$. We then have the equations

$$2(1+\hat{d}) = (-(d+1) \pm 6\sqrt{d})u^2,$$
$$(1-\hat{d})^2 = (8d \mp 4(d+1)\sqrt{d})u^4.$$

This system can be solved for u and $\hat{d}$, but is more complicated than the above case with $r = 0$. The solution shows that there are other non-trivial isomorphisms. Composing the above maps, it turns out these isomorphisms are of the form

$$(x, y) \to \left(x\frac{(\gamma+r)y + \gamma - r}{-u\gamma(y+1)}, \frac{(\gamma + r - 1 + \hat{d})y + \gamma - r + 1 - \hat{d}}{(\gamma + r + 1 - \hat{d})y + \gamma - r - 1 + \hat{d}} \right),$$

where $\gamma = u^2(1-d)$.

We note that [1] also includes discusses explicit Edwards isomorphisms. The number of Edwards curve isomorphism classes over finite fields has been studied in [14], [15], [27].

4.2 Edwards 2-isogenies

We saw in section 3.1 there are birational maps from Edwards curves to Weierstrass curves. An intuitive method to find explicit isogenies for Edwards curves would be to use these maps, combined with Vélu's formula. We show how to do this for 2-isogenies.

Let ϕ_1 be the transformation from the Edwards curve E_d to a Weierstrass curve E_1 given in (1). Let ϕ_2 be an l-isogeny from E_1 to the curve E_2, given by Vélu's formula. The image under an isogeny computed by Vélu's formula is not likely to be in the form

$$y^2 = x^3 + 2(1+\hat{d})x^2 + (1-\hat{d})^2x,$$

for some $\hat{d}$, so we cannot use ϕ_1^{-1} to map this image curve to an Edwards curve. The birational transformation which does work is described in [3]. Let P be a

point of order 2 on the image curve E'. Write $P = (r_2, s_2)$. Then the change of variables $(x, y) \to (x - r_2, y_2)$ maps P to $(0, 0)$, and the new curve has its equation of the form $y^2 = x^3 + ax^2 + bx$. Let $Q = (r_1, s_1)$ be a point of order 4 on this curve, and let $\hat{d} = 1 - 4r_1^3/s_1^2$. Then in fact, we actually have that $a = 2\frac{1+\hat{d}}{1-\hat{d}}r_1$ and $b = r_1^2$. The map

$$\phi_3 : (x, y) \to \left(2\sqrt{\frac{r_1}{1-\hat{d}}}\frac{x}{y}, \frac{x - r_1}{x + r_1}\right)$$

takes us to the Edwards curve

$$x^2 + y^2 = 1 + \hat{d}x^2y^2.$$

If we compose the three maps ϕ_1, ϕ_2, and ϕ_3, we get an explicit l-isogeny ψ from E_d to $E_{d'}$.

Theorem 1 *Let E_d be an Edwards curve, $\gamma = \sqrt{1-d}$, and $i = \sqrt{-1}$. Then there are 2-isogenies from the curve E_d given by the maps ψ_1, ψ_2, and ψ_3 below.*

The first is

$$\psi_1(x, y) \to \left((\gamma \mp 1)xy, \frac{(\gamma \mp 1)y^2 \pm 1}{(\gamma \pm 1)y^2 \mp 1}\right).$$

The image of ψ_1 is the curve $E_{\hat{d}} : x^2 + y^2 = 1 + d'x^2y^2$, with $\hat{d} = \left(\frac{\gamma \pm 1}{\gamma \mp 1}\right)^2$.

The second is

$$\psi_2(x, y) \to \left((i\gamma \pm \sqrt{d})\frac{x}{y}, -\frac{\sqrt{d}y^2 \mp i\gamma - \sqrt{d}}{\sqrt{d}y^2 \pm i\gamma - \sqrt{d}}\right).$$

The image of ψ_2 is the curve $E_{\hat{d}}$, with $\hat{d} = \left(\frac{i\gamma \mp \sqrt{d}}{i\gamma \pm \sqrt{d}}\right)^2$.

Finally, we have

$$\psi_3(x, y) \to \left(\sqrt{-1}(\sqrt{d} \mp 1)\frac{x}{y}\frac{1 - dy^2}{1 - d}, \frac{d \mp \sqrt{d}}{d \pm \sqrt{d}}\frac{\sqrt{d}y^2 \pm 1}{\sqrt{d}y^2 \mp 1}\right),$$

with image curve $E_{\hat{d}}$, where $\hat{d} = \left(\frac{\sqrt{d} \pm 1}{\sqrt{d} \mp 1}\right)^2$.

Proof For $l = 2$, the kernel of a 2-isogeny is the set $\{(0, 1), (0, -1)\}$. We prove the theorem by explicitly finding the maps ϕ_1, ϕ_2, and ϕ_3 as described above. The map $\phi_1 : E_d \to E_1$ was already given in (1). Using Vélu's formula, we find a 2-isogeny $\phi_2 : E_1 \to E_2$

$$\phi_2(x, y) \to \left(\frac{x^2 + (1 - d)^2}{x}, y\frac{x^2 - (1 - d)^2}{x^2}\right).$$

The equation for E_2 is the curve

$$E_2 : y^2 = x^3 + 2(1 + d)x^2 - 4(1 - d)^2x - 8(1 + d)(1 - d)^2.$$

The points $(\pm 2(1-d), 0)$, and $(-2(1+d), 0)$ each have order 2. For the first map we use the linear transformation $(x, y) \to (x - 2(1-d), y)$. This maps the curve E_2 to the curve

$$E_3 : y^2 = x^3 - 4(d-2)x^2 + 16(1-d)x.$$

As $a = -4(d-2) = 2\frac{1+\hat{d}}{1-\hat{d}} r_1$ and $b = 16(1-d) = r_1^2$, we easily find that the x-coordinate of a point of order 4 is $r_1 = \pm 4\gamma$, and $\hat{d} = \left(\frac{\gamma \pm 1}{\gamma \mp 1}\right)^2$. Then the map ϕ_3 is as explained above the statement of Theorem 1, with these values of r_1 and $\hat{d}$. Composing the maps and simplifying the equations leads to the formula for ψ_1 shown in the theorem. We omit the algebraic details. The other 2-isogenies are similarly obtained by using the other two points of order 2, $(-2(1-d), 0)$ and $(-2(1+d), 0)$. □

Ahmadi and Granger independently obtained equivalent formulas for 2-isogenies [1]. We remark that the 2-isogenies in Theorem 1 may not be defined over the same field as E_d is. This is the case when $d, d-1$, or $1-d$ is not a square in K. A simple argument shows that we cannot do any better.

Let ψ be a 2-isogeny on E_d. Then necessarily, we must have $\psi(0, \pm 1) = (0, 1)$ and $\psi(\pm 1, 0) = (0, -1)$. It is easy to use the addition law to derive the identities $(x, y) + (0, -1) = (-x, -y)$, and $(x, y) + (1, 0) = (y, -x)$. As ψ is a homomorphism, this imposes the following conditions on ψ. Denoting $\psi(x, y) = (X, Y)$, then

$$\begin{aligned} \psi(-x, -y) &= (X, Y), \\ \psi(y, -x) &= (-X, -Y), \\ \psi(-x, y) &= (-X, Y). \end{aligned} \tag{2}$$

As functions on E_d, we can write $(X, Y) = (xR(y), S(y))$ for some rational functions R and S (see section 4 of [18] or [23]). Using (2), we conclude that $R(0) = 0, S(0) = -1$, $S(\pm 1) = 1$, and that R is an odd function, while S is even. We must also have $S(-x) = -S(y)$ for points (x, y) on E_d. As we are looking for the simplest possible 2-isogenies, it can be checked that no rational functions with smaller degrees than those in Theorem 1 will work. The simplest of these rational functions is of the form $\psi(x, y) = \left(cxy, \frac{ay^2+1}{my^2+n}\right)$. Imposing the conditions on $S(0)$ and $S(\pm 1)$, then this becomes $\psi(x, y) = \left(cxy, \frac{ay^2+1}{(a+2)y^2-1}\right)$. Using $S(-x) = -S(y)$, we can deduce $a^2 + 2a + d = 0$, or $a = -1 \pm \sqrt{1-d}$. Some further algebra on the equation $X^2 + Y^2 - 1 - \hat{d}X^2Y^2 = 0$ shows that we must have $c = \pm a = \pm(-1 \pm \sqrt{1-d})$. Thus, we cannot define ψ over the ground field, unless $1-d$ is a square. A similar analysis can be done for the other isogenies in Theorem 1.

4.3 Edwards curve isogenies

For ℓ larger than 2, the approach in the last subsection of mapping to and from a Weierstrass curve does not seem feasible. In this section we give a formula for isogenies on Edwards curves analogous to Vélu's formulas in section 2. Let F be the kernel of the desired isogeny. The motivating idea is that we are seeking to find rational functions which are invariant under translation by the points in F, and map the point $(0, 1)$ to itself.

Theorem 2 *Suppose F is a subgroup of the Edwards curve E_d with odd order $\ell = 2s + 1$, and points*

$$F = \{(0, 1), (\pm\alpha_1, \beta_1), \ldots, (\pm\alpha_s, \beta_s)\}.$$

Define

$$\psi(P) = \left(\prod_{Q \in F} \frac{x_{P+Q}}{y_Q}, \prod_{Q \in F} \frac{y_{P+Q}}{y_Q} \right).$$

Then ψ is an ℓ-isogeny, with kernel F, from the curve E_d to the curve $E_{\hat{d}}$ where $\hat{d} = B^8 d^\ell$ and $B = \prod_{i=1}^{s} \beta_i$. The coordinate maps are given by:

$$\psi(x, y) = \left(\frac{x}{B^2} \prod_{i=1}^{s} \frac{\beta_i^2 x^2 - \alpha_i^2 y^2}{1 - d^2 \alpha_i^2 \beta_i^2 x^2 y^2}, \frac{y}{B^2} \prod_{i=1}^{s} \frac{\beta_i^2 y^2 - \alpha_i^2 x^2}{1 - d^2 \alpha_i^2 \beta_i^2 x^2 y^2} \right). \tag{3}$$

Proof It is easy to see that $\psi(0, 1) = (0, 1)$, and that ψ is invariant under translation by elements of F. So then $F \subseteq \ker(\psi)$. Conversely, if $P \in \ker(\psi)$, then $x_{P+Q} = 0$ for some $Q \in F$. This implies that $P = \pm Q \in F$, so that $F = \ker(\psi)$. Furthermore, it is straightforward to derive the coordinate maps given by equation (3) from the Edwards curve addition law.

We now derive the formula for $\hat{d}$ on the image curve:

$$X^2 + Y^2 = 1 + \hat{d} X^2 Y^2,$$

where $X(P)$ and $Y(P)$ are the coordinate maps of ϕ. In order to do this, we look at the function

$$G(x, y) = X(x, y)^2 + Y(x, y)^2 - 1 - dX(x, y)^2 Y(x, y)^2,$$

and solve for the value of $\hat{d}$ that makes G identically zero.

It is easy to see that the coordinate maps X and Y preserve the points $(0, 1)$ and $(0, -1)$. Furthermore, these two points are the only points on the domain curve with the x-coordinate equal to 0. Likewise, the only points on the codomain curve with $X = 0$ are $(0, \pm 1)$. Hence $G(x, y)$ has two zeros when $x = 0$, specifically $y = \pm 1$. We can explicitly calculate the partial derivatives of the codomain curve with respect to x and y at the points $(0, 1)$ and $(0, -1)$. This shows that neither of these points are singular, and hence G has only simple

zeros at these points. Thus, the zeros of $G(x,y)$ are also simple at the points $(0,1)$ and $(0,-1)$.

Now, we explicitly examine the zeros of $G(x,y)$ at $x=0$ by looking at this function as a power series about $x=0$. Note that y^2 can be written as a rational function in terms of x, and the square of the coordinate maps contain only even powers of y. Hence the square of these maps can be written entirely in terms of x. Specifically, from the Edwards curve equation we have $y^2=(1-x^2)/(1-dx^2)$. Expanding as power series, we see

$$X(x,y)=\frac{x}{B^2}\prod_{i=1}^{s}(-\alpha_i^2+O(x^2)),$$

$$Y(x,y)=\frac{y}{B^2}\prod_{i=1}^{s}(\beta_i^2+(d\beta_i^4-1)x^2+O(x^4)).$$

Then with $A=\prod_{i=1}^{s}\alpha_i$,

$$X(x)^2=\frac{A^4}{B^4}x^2+O(x^4),$$

$$Y(x)^2=\frac{1-x^2}{1-dx^2}\prod_{i=1}^{s}(1+\frac{1}{\beta_i^2}(d\beta_i^4-1)x^2+O(x^4))^2,$$

$$Y(x)^2=(1+(d-1)x^2+O(x^4))\prod_{i=1}^{s}(1+\frac{2}{\beta_i^2}(d\beta_i^4-1)x^2+O(x^4)),$$

$$Y(x)^2=1+\Big(d-1+2\sum_{i=1}^{s}(d\beta_i^2-\frac{1}{\beta_i^2})\Big)x^2+O(x^4).$$

If we substitute these into the equation of the image of ψ, we find

$$\begin{aligned}G(x,y)&=X(x)^2+Y(x)^2-1-\hat{d}X(x)^2Y(x)^2,\\&=\frac{A^4}{B^4}x^2+(d-1+2\sum_{i=1}^{s}(d\beta_i^2-\frac{1}{\beta_i^2}))x^2-\hat{d}\frac{A^4}{B^4}x^2+O(x^4),\\&=\left(\frac{A^4}{B^4}-\hat{d}\frac{A^4}{B^4}+d-1+2\sum_{i=1}^{s}(d\beta_i^2-\frac{1}{\beta_i^2})\right)x^2+O(x^4).\end{aligned}$$

Suppose that the coefficient of x^2, in the above expansion is zero, then G has a zero of order greater than 2 at $x=0$. However, we showed above that that G has a zero of order 2 at $x=0$. So we conclude that either G is identically zero. Setting the coefficient of x^2 to zero and solving this for $\hat{d}$ yields

$$\hat{d}=1+\frac{B^4}{A^4}\left(d-1+2\sum_{i=1}^{s}(d\beta_i^2-\frac{1}{\beta_i^2})\right).$$

Thus with this choice for $\hat{d}$, the function G is identically zero, and we conclude that the codomain of this map is another Edwards curve. We have a rational map from an Edwards curve to another which preserves the identity point, which is necessarily an isogeny by Proposition 1.

By looking at the image of a specific point on the domain curve, we can further simplify the formula for $\hat{d}$, the coefficient of the codomain curve. Particularly, we choose the point $P = \left(\frac{1}{\gamma}, \frac{i}{\gamma}\right)$, where $i^2 = -1$ and $\gamma^4 = d$. This point may not be defined over K, but rather over an extension of K.

First, we evaluate the value on the inside of the product on the x-coordinate map at our point P:

$$\frac{1}{\gamma^2}\left(\frac{\alpha_i^2 + \beta_i^2}{1 + d\alpha_i^2\beta_i^2}\right).$$

As (α_i, β_i) is a point on the domain curve $x^2+y^2 = 1+dx^2y^2$ this simplifies to $\frac{1}{\gamma^2}$. Hence, the X-coordinate of the image point is $\frac{1}{B^2\gamma^\ell}$. A similar calculation for the Y-coordinate shows that $Y(P)$ is $\frac{(-1)^s i}{B^2\gamma^\ell}$. Then, because we know $\left(\frac{1}{B^2\gamma^\ell}, \frac{(-1)^s i}{B^2\gamma^\ell}\right)$ is on the curve $X^2 + Y^2 = 1 + \hat{d}X^2Y^2$. We are able to calculate that $\hat{d} = B^8 d^\ell$. □

We note the formula for isogenies given in Theorem 1 also works for twisted Edwards curves $E_{a,d}$. This is easiest to see by noting that the map $(x, y) \to (x/\sqrt{a}, y)$ maps $E_{a,d}$ to $E_{1,d/a}$. We can then apply Theorem 2, which maps to the curve $E_{1,B^8(d/a)^\ell}$. Mapping back to the twisted Edwards form by sending $(X, Y) \to (\sqrt{a^\ell}X, Y)$ gives an isogeny from $E_{a,d}$ to E_{a^ℓ,B^8d^ℓ} This argument establishes the following corollary.

Corollary 1 *Suppose F is a subgroup of the twisted Edwards curve $E_{a,d}$ with odd order $\ell = 2s + 1$, and points*

$$F = \{(0, 1), (\pm\alpha_1, \beta_1), \ldots, (\pm\alpha_s, \beta_s)\}.$$

Define

$$\psi(P) = \left(\prod_{Q\in F} \frac{x_{P+Q}}{y_Q}, \prod_{Q\in F} \frac{y_{P+Q}}{y_Q}\right).$$

Then ψ is an l-isogeny, with kernel F, from the curve $E_{a,d}$ to the curve $E_{\hat{a},\hat{d}}$ where $\hat{a} = a^\ell$, $\hat{d} = B^8d^\ell$ and $B = \prod_{i=1}^s \beta_i$.

4.4 Another approach

We now state and prove another formula for Edwards curve isogenies. Let $\ell = 2s + 1$ be the degree of the isogeny. We can assume the isogeny ψ satisfies $\psi(1, 0) = (1, 0)$. If not simply compose with the negation map.

Theorem 3 *Let E_d be an Edwards curve with subgroup $F = \{(0,1), (\pm\alpha_i, \beta_i) : i = 1 \dots s\}$. Then an isogeny with kernel F is given by*

$$\psi(x,y) \to \left(x\frac{\prod_{i=1}^{s} y^2 - \beta_i^2}{f(y)}, y\frac{\prod_{i=1}^{s} y^2 - \alpha_i^2}{g(y)} \right),$$

where the polynomials $f(y)$ and $g(y)$ are the unique even polynomials of degree $2s$ satisfying:

$$\begin{aligned} f(0) &= (-1)^s \prod_{i=1}^{s} \beta_i^2 & f(\alpha_j) &= \beta_j \prod_{i=1}^{s} (\alpha_j^2 - \beta_i^2), \\ g(1) &= \prod_{i=1}^{s} (1 - \alpha_i^2), & g(\beta_j) &= \beta_j \prod_{i=1}^{s} (\beta_j^2 - \alpha_i^2). \end{aligned} \tag{4}$$

This isogeny is the same as the isogeny given by Theorem 2. The image is the curve $E_{B^s d^l}$. We include Theorem 3, as it shows how to write an isogeny (almost) entirely in terms of one variable.

Proof Let $\psi : E_d \to E_{\hat{d}}$ be the isogeny described above. If we write $\psi(x,y) = (X(x,y), Y(x,y))$, then both X and Y are rational functions of x and y. Hitt, Moloney, and McGuire have shown (see [18],[23]) that over E_d, we can uniquely write $X = p(y) + xq(y)$ and $Y = r(y) + xs(y)$, for some rational functions $p(y), q(y), r(y)$, and $s(y)$. We first show that $p(y) = 0$ and $s(y) = 0$.

As ψ is a homomorphism, then it follows that for any (x,y) on E_d

$$\begin{aligned} \psi(-x,y) &= \Big(p(y) - xq(y), r(y) - xs(y)\Big) \\ &= \psi\Big(-(x,y)\Big) \\ &= -\psi(x,y) \\ &= \Big(-p(y) - xq(y), r(y) + xs(y)\Big). \end{aligned}$$

So $p(y) - xq(y) = -p(y) - xq(y)$, and also $r(y) - xs(y) = r(y) + xs(y)$, from which we easily see that $p(y) = 0$ and $s(y) = 0$.

Now we use the fact that $(\pm\alpha_i, \beta_i)$ is in the kernel of ψ, so

$$(0,1) = \psi(\pm\alpha_i, \beta_i) = (\pm\alpha_i q(\beta_i), r(\beta_i)).$$

The only other point on $E_{\hat{d}}$ with x-coordinate 0 is $(0,-1)$. Since $(\pm\alpha_i, \beta_i) + (0,-1) = (\mp\alpha_i, -\beta_i)$, then we have $\psi(\mp\alpha_i, -\beta_i) = \psi(0,-1) = (0,-1)$. In summary, the only points mapping to $(0,1)$ are the points $(0,1)$ and $(\pm\alpha_i, \beta_i)$, and the only points mapping to $(0,-1)$ are $(0,-1)$ and $(\pm\alpha_i, -\beta_i)$. This means that

$$q(y) = \frac{\prod_{i=1}^{s} (y^2 - \beta_i^2)}{f(y)},$$

for some polynomial $f(y)$.

Similarly, using the identities$(x,y)+(1,0)=(y,-x)$, and $(x,y)+(-1,0)=(-y,x)$, we find that $\psi(\pm\beta_i,\alpha_i)=(\pm 1,0)$ and $\psi(\pm\beta_i,-\alpha_i)=(\mp 1,0)$. Trivially we also have $\psi(\pm 1,0)=(1,0)$. We likewise conclude that

$$r(y)=y\frac{\prod_{i=1}^{s}(y^2-\alpha_i^2)}{g(y)},$$

for some polynomial $g(y)$.

Evaluating at the points in the kernel, we come up with the equations in (4). If f and g are of degree $2s$, then they are uniquely determined and can be found by the Lagrange polynomial interpolation formula. It is easy to see that f and g are even. Write $\psi(x,y)=(X,Y)$, so then $\psi(x,-y)=(X,-Y)$. Comparing both sides of this equation we find $f(-y)=f(y)$ and $g(-y)=g(y)$ for all y, so both f and g are even functions.

The final point to check is that f and g cannot have degree more than $2s$. Suppose that the degree of g were more than $2s$. Then there would exist some $\tilde{y}\in(\overline{K})$, $\tilde{y}\neq 1,\beta_i$ such that

$$g(\tilde{y})-\tilde{y}\prod_{j=1}^{s}(\tilde{y}^2-\alpha_i^2)=0.$$

Equivalently, the y-coordinate of $\psi(x,\tilde{y})$ is equal to 1. Then let $\tilde{x}=\sqrt{\frac{1-\tilde{y}^2}{1-d\tilde{y}^2}}\in\overline{K}$. It follows that $(\tilde{x},\tilde{y})$ is a point on E_d, and that since $\tilde{y}\neq 1,\beta_i$ then $\tilde{x}\neq 0,\alpha_i$. Thus $\psi(\tilde{x},\tilde{y})=(\gamma,1)$ on $E_{\hat{d}}$, for some γ. But the only point on an Edwards curve with y-coordinate 1 is $(0,1)$. This is a contradiction as we have just found another point in the kernel. So the degree of g is $2s$. Likewise, the same argument applied to f and the points $\{(1,0),(-\beta_i,-\alpha_i)\}$ being the only points which map to $(1,0)$ show the degree of f is $2s$, and finishes the proof. □

4.5 The kernel polynomial

D. Kohel, in his thesis showed how the kernel polynomial of an isogeny can also be used to explicitly write down the isogeny [24]. This was seen in the section on Vélu's formula. We now look at the kernel polynomial for Edwards curves. If the kernel is $\{(0,1),(\pm\alpha_1,\beta_1),\ldots,(\pm\alpha_s,\beta_s)\}$, then one kernel polynomial could be

$$g(x)=\prod_{i=1}^{s}(x^2-\alpha_i^2),$$

which has as roots the $\pm\alpha_i$. Alternatively we could take

$$h(y)=\prod_{i=1}^{s}(y^2-\beta_i^2).$$

By Theorem 2, we can write the isogeny as $\psi(x,y) = (X,Y)$ with

$$X = \frac{x}{B^2}\prod_{i=1}^{s}\frac{x^2-\alpha_i^2}{1-d\alpha_i^2x^2} \quad \text{or} \quad X = \frac{x}{B^2}\prod_{i=1}^{s}\frac{y^2-\beta_i^2}{d\beta_i^2y^2-1},$$

$$Y = \frac{y}{B^2}\prod_{i=1}^{s}\frac{x^2-\beta_i^2}{d\beta_i^2x^2-1} \quad \text{or} \quad Y = \frac{y}{B^2}\prod_{i=1}^{s}\frac{y^2-\alpha_i^2}{1-d\alpha_i^2y^2}.$$

Note that we can compute X solely in terms of x (and not y), and a similar statement for Y. Writing these in terms of the kernel polynomials, we see

$$X = \frac{g(1/\sqrt{d})xg(x)}{g(1)x^{2s}g(1/\sqrt{d}x)} = \frac{xh(y)}{h(0)(dy^2)^sh(1/\sqrt{d}y)},$$

$$Y = \frac{yh(x)}{h(0)(dx^2)^sh(1/\sqrt{d}x)} = \frac{g(1/\sqrt{d})yg(y)}{g(1)y^{2s}g(1/\sqrt{d}y)}.$$

The codomain is $\hat{d} = d^{2s+1}\prod_{i=1}^{s}\beta_i^8 = d^{2s+1}h(0)^4 = dg(1)^2/g(1/\sqrt{d})^2$. We note that if we have an algorithm to evaluate g (or h) efficiently, then we see we can efficiently compute the isogeny.

5 Isogenies on Huff curves

5.1 Isomorphisms

Suppose Ψ is an isomorphism from $H_{a,b}$ to some other Huff curve $H_{\hat{a},\hat{b}}$. Let ϕ be the birational transformation from the curve $H_{a,b}$ to a Weierstrass curve $E : y^2 = x^3+(a+b)x^2+abx$ and similarly let $\hat{\phi}$ be the birational transformation from $H_{\hat{a},\hat{b}}$ to the Weierstrass curve $\hat{E}$. Then it follows that E and $\hat{E}$ are isomorphic. The only isomorphisms between curves of the form $y^2 = x^3 + Ax^2 + Bx$ have as a map

$$I'(x,y) = (u^2x + r, u^3y),$$

for some $u \neq 0$. When $r = 0$, we can compose the maps $I' \circ \phi$ to get a map from $H_{a,b}$ to $y^2 = x^3 + (a+b)u^2x^2 + abu^4x$. We see that $\hat{a} = u^2a$ and $\hat{b} = u^2b$. An easy calculation shows

$$(\hat{\phi}^{-1} \circ I' \circ \phi)(x,y) = I_u(x,y) = \left(\frac{x}{u}, \frac{y}{u}\right).$$

When $r \neq 0$, we require the isomorphism I' to have a codomain curve of the form $y^2 = x^3 + Ax^2 + Bx$. It is easy to check that this only happens when $r = -a$ or $r = -b$. When $r = -a$, the codomain curve is $y^2 = x^3 + (b-2a)u^2x^2 + a(a-b)u^4x$, from which we see we that $\hat{a} = -au^2$ and $\hat{b} = (b-a)u^2$. The composition of these maps is the isomorphism $(x,y) \to \left(\frac{bx-ay}{u(b-a)}, \frac{y}{u}\right)$ from $H_{a,b}$ to $H_{-au^2,(b-a)u^2}$.

By symmetry, when $r = -b$ then $\hat{a} = (a-b)u^2$ and $\hat{b} = -bu^2$. The composition map is $H_{a,b}$ to $H_{(a-b)u^2,-bu^2}$ given by $(x,y) \to \left(\frac{x}{u}, \frac{bx-ay}{u(b-a)}\right)$.

We also have $(x,y) \to (y,x)$ which sends $H_{a,b}$ to $H_{b,a}$.

5.2 Huff isogenies

We now look at isogenies for Huff curves. We derive a formula for isogenies on Huff curves similar to Vélu's formulae in section 2, just as we did for Edwards curves. Let F be the desired kernel of an isogeny. We seek a rational function invariant under translation by the points in F, which maps the point $(0,0)$ to itself. We denote the points in F by $F = \{(0,0), (\alpha_i, \beta_i), (-\alpha_i, -\beta_i) : i = 1 \dots s\}$. Let $A = \prod_{i=1}^{s} \alpha_i$ and $B = \prod_{i=1}^{s} \beta_i$.

Theorem 4 *Define*

$$\psi(P) = \left(x_P \prod_{Q \neq (0,0) \in F} \frac{x_{P+Q}}{x_Q}, y_P \prod_{Q \neq (0,0) \in F} \frac{y_{P+Q}}{y_Q} \right).$$

Then ψ is an ℓ-isogeny from the curve $H_{a,b}$ to the curve $H_{\hat{a},\hat{b}}$ where $\hat{a} = a^\ell B^4$ and $\hat{b} = b^\ell A^4$. Using the addition law, we can write

$$\psi(x,y) = \left(x \prod_{i=1}^{s} \frac{x^2 - \alpha_i^2}{\alpha_i^2(1 - b^2\alpha_i^2 x^2)}, y \prod_{i=1}^{s} \frac{y^2 - \beta_i^2}{\beta_i^2(1 - a^2\beta_i^2 y^2)} \right). \tag{5}$$

The equation (5) *is valid for points which are not points at infinity.*

Proof It is easy to see that $\psi(0,0) = (0,0)$, and that ψ is invariant under translation by elements of F. Therefore, the set F is contained in the set that ψ maps to the point $(0,0)$. Conversely, if $\psi(P) = (0,0)$, then either $x_P = 0$ or $x_{P+Q} = 0$ for some $Q \in F$. If $x_P = 0$, then $P = (0,0) \in F$. If $x_{P+Q} = 0$, then $P + Q = (0,0)$, and $P = -Q \in F$. Thus the preimage of $(0,0)$ under ψ is exactly the set F.

It is well known that the function u/v has a simple zero at ∞ on an elliptic curve given by a Weierstrass equation $E_{a,b}: \; v^2 = u^3 + (a+b)u^2 + abu$. Using the birational transformation given in section 3.2, this function becomes $t = ay - bx$ on the Huff curve $H_{a,b}$ which has a simple zero at the identity point $(0,0)$. Similarly, as v has a simple zero at the three points of order 2 on $E_{a,b}$, then the function $r = \frac{1}{y-x}$ has simple zeroes at the three points of infinity $(1 : 0 : 0), (0 : 1 : 0)$, and $(a : b : 0)$ on the Huff curve. The function r

has a triple pole at $(0,0)$, as

$$\begin{aligned} r &= \frac{1}{y-x} \\ &= -t^{-3}\frac{(ay-bx)^2}{xy} \\ &= -t^{-3}\left((a^2\frac{y}{x} - 2ab + b^2\frac{x}{y}\right) \\ &= -t^{-3}\left(a^2\frac{ay^2-1}{bx^2-1} - 2ab + b^2\frac{bx^2-1}{ay^2-1}\right). \end{aligned}$$

Similarly, it can be checked that t has a simple zero at $(a : b : 0)$ and simple poles at $(1 : 0 : 0)$ and $(0 : 1 : 0)$. There are no other zeroes or poles of r or t.

We now consider the function x over the Huff curve. Note that

$$\begin{aligned} x &= \frac{1}{a-b}\left(t - \frac{a}{r}\right), \\ &= \frac{1}{a-b}\left(t - at^3\frac{(bx^2-1)(ay^2-1)}{(b-a+a^2y^2-b^2x^2)^2}\right), \\ &= \frac{1}{a-b}t\left(1 - at^2\frac{(bx^2-1)(ay^2-1)}{(b-a+a^2y^2-b^2x^2)^2}\right), \end{aligned}$$

and so x has a simple zero at $(0,0)$. Furthermore,

$$x - \frac{1}{a-b}t = -\frac{a}{a-b}t^3\left(\frac{(bx^2-1)(ay^2-1)}{(b-a+a^2y^2-b^2x^2)^2}\right),$$

and a more detailed computation yields

$$x = \frac{1}{a-b}t - \frac{a}{(b-a)^3}t^3 + O(t^5).$$

Here the notation $O(t^5)$ means a function which has at least a fifth order zero at $(0,0)$. An analogous calculation shows that y also has a simple zero at $(0,0)$, with

$$y = \frac{1}{a-b}t - \frac{b}{(b-a)^3}t^3 + O(t^5).$$

For the points at infinity, we use projective coordinates and see that

$$\begin{aligned} x &= \frac{x}{z} \\ &= \frac{y-x}{z}\left(\frac{x}{y-x}\right) \\ &= r^{-1}\left(\frac{x}{y-x}\right), \end{aligned}$$

and so x has simple poles at $(1 : 0 : 0)$ and $(a : b : 0)$. At $(0 : 1 : 0)$

$$\begin{aligned} x &= \frac{x}{z} \\ &= \frac{z}{y-x}\left(\frac{x(y-x)}{z^2}\right) \\ &= -r\left(\frac{(y-x)^2}{y(ay-bx)}\right), \end{aligned}$$

so x has a simple zero. Similarly, we can check y has simple poles at $(0 : 1 : 0)$ and $(a : b : 0)$ and a simple pole at $(1 : 0 : 0)$. These are the only zeroes and poles of x and y.

If we write the map in (5) as $\psi(x, y) = (X, Y)$, then

$$X = x\prod_{i=1}^{s}\frac{x^2-\alpha_i^2}{\alpha_i^2(1-b^2\alpha_i^2x^2)},$$

$$Y = y\prod_{i=1}^{s}\frac{y^2-\beta_i^2}{\beta_i^2(1-a^2\beta_i^2y^2)}.$$

For a fixed i, consider the function $x^2 - \alpha_i^2$. It has simple zeroes at $\pm(\alpha_i, \beta_i)$ and $\pm(-\alpha_i, 1/a\beta_i)$. As x has a simple pole at $(1 : 0 : 0)$ and $(a : b : 0)$ then $x^2 - \alpha_i^2$ has poles of order two at these same points. Similarly, if we examine the function $1 - b^2\alpha_i^2x^2$, then we have simple zeroes at $\pm(1/b\alpha_i)$ and $\pm(-1/b\alpha_i, -1/a\beta_i)$ and double poles at $(1 : 0 : 0)$ and $(a : b : 0)$. We are able to compute

$$\begin{aligned} \frac{x^2-\alpha_i^2}{\alpha_i^2(1-b^2\alpha_i^2x^2)} &= -1 + \frac{1-b^2\alpha_i^4}{\alpha_i^2}x^2 + O(x^4) \\ &= -1 + \frac{1-b^2\alpha_i^4}{\alpha_i^2(b-a)^2}t^2 + O(t^4). \end{aligned}$$

So then

$$\begin{aligned} \frac{X}{x} &= \prod_{i=1}^{s}\left(-1 + \frac{1-b^2\alpha_i^4}{\alpha_i^2(b-a)^2}t^2 + O(t^4)\right) \\ &= (-1)^s + (-1)^{s+1}\left(\sum_{i=1}^{s}\frac{1-b^2\alpha_i^4}{\alpha_i^2(b-a)^2}\right)t^2 + O(t^4). \end{aligned}$$

Therefore,

$$X = \frac{(-1)^s}{a-b}\left(t - \frac{1}{(a-b)^2}\left(-a + \sum_{i=1}^{s}\frac{1-a^2\beta_i^4}{\beta_i^2}\right)t^3 + O(t^5)\right),$$

and similarly,

$$Y = \frac{(-1)^s}{a-b}\left(t - \frac{1}{(a-b)^2}\left(-b + \sum_{i=1}^{s}\frac{1-b^2\alpha_i^4}{\alpha_i^2}\right)t^3 + O(t^5)\right).$$

Now we define

$$G_{c,d} = X(cY^2 - 1) - Y(dX^2 - 1) = (Y - X) + XY(cY - dX).$$

We first note that

$$Y - X = \frac{(-1)^s}{(a-b)^3}\left(b - a + \sum_{i=1}^{s} \frac{1 - b^2\alpha_i^4}{\alpha_i^2} - \frac{1 - a^2\beta_i^4}{\beta_i^2}\right) t^3 + O(t^5),$$

and so we can see that $G_{c,d}$ will have a zero of order 3 at $(0,0)$. A further computation shows

$$G_{c,d} = \frac{(-1)^s}{(a-b)^3}\left(b - a + c - d + \sum_{i=1}^{s} \frac{1 - a^2\beta_i^4}{\beta_i^2} - \frac{1 - b^2\alpha_i^4}{\alpha_i^2}\right) t^3 + O(t^5). \quad (6)$$

The only possible poles of $G_{c,d}$ are at the poles of X and Y. From above, the poles of X are at $(1 : 0 : 0), (a : b : 0), \pm(1/b\alpha_i, -\beta_i)$, and $\pm(-1/b\alpha_i, -1/a\beta_i)$, all of which are simple. The poles of Y are all simple, and are located at $(0 : 1 : 0), (a : b : 0), \pm(-\alpha_i, 1/a\beta_i)$, and $\pm((-1/b\alpha_i, -1/a\beta_i))$.

At $(1 : 0 : 0)$, X has a simple pole, while Y has a simple zero, so $G_{c,d}$ will have at worst a simple pole there. The same is true for $(0 : 1 : 0)$. At $(a : b : 0)$, we see that there will be at most a triple pole for $G_{c,d}$. Now, at the points $\pm(1/b\alpha_i, -\beta_i)$, we see there is at most a simple pole, and similarly for $\pm(-\alpha_i, 1/a\beta_i)$. Finally, we note that $\pm(-1/b\alpha_i, -1/a\beta_i)$ will cause $G_{c,d}$ to have at most a triple pole. So the total number of poles (counting multiplicity) is $10s + 5 = 5\ell$. Thus, the total number of zeroes is at most 5ℓ. By the definition of X and Y, we know that they are invariant under translation by points in the kernel F. As $G_{c,d}$ has at least a triple zero at $(0,0)$, then there is at least a triple zero at $\pm(\alpha_i, \beta_i)$. So (counting multiplicities), we see that $G_{c,d}$ has at least $3 + 6s = 3\ell$ zeroes.

We see from (6) that the coefficient of t^3 in $G_{c,d}$ is linear in c and d. A more detailed analysis also shows the coefficient of t^5 is linear in c and d as well. Thus, we may solve this system of equations to make these coefficients zero. With these values of c and d, then $G_{c,d}$ has a zero of order at least 7 at $(0,0)$, as well as at the $\pm(\alpha_i, \beta_i)$. Counting multiplicities, we obtain that there are at least $7 + 14s = 7\ell$ zeroes. This is more than the number of poles, which is a contradiction, unless $G_{c,d}$ is constant. We easily see $G_{c,d}(0,0) = 0$, and hence $G_{c,d}$ is identically zero. This shows the image of ψ is a Huff curve. We've found a rational map which sends $H_{a,b}$ to another Huff curve and maps $(0,0)$ to $(0,0)$. This is necessarily an isogeny. We do not give the detailed expressions for c and d, as we can come up with vastly simplified equations for the codomain curve. We now show how to do this.

Solving for the projective maps on the Huff curve gives us:

$$X = x \prod_{i}^{2} \left[\left(x^2 - \alpha_i^2 z^2\right) \beta_i^2 \left(z^2 - a^2 \beta_i^2 y^2\right)\right],$$

$$Y = y \prod_{i}^{s} \left[\left(y^2 - \beta_i^2 z^2 \right) \alpha_i^2 \left(z^2 - b^2 \alpha_i^2 x^2 \right) \right],$$

and

$$Z = z \prod_{i}^{s} \left[\alpha_i^2 \left(z^2 - b^2 \alpha_i^2 x^2 \right) \beta_i^2 \left(z^2 - a^2 \beta_i^2 y^2 \right) \right].$$

From this we see that the points at infinity $(1 : 0 : 0)$ and $(0 : 1 : 0)$ map to $(1 : 0 : 0)$ and $(0 : 1 : 0)$ respectively. The third point at infinity $(a : b : 0)$ maps to $(a^\ell B^4 (ab)^{2s} : b^\ell A^4 (ab)^{2s} : 0)$, which is equivalent to the point $(a^\ell B^4 : b^\ell A^4 : 0)$.

By plugging this into the curve:

$$X \left(\hat{a} Y^2 - Z^2 \right) = Y \left(\hat{b} X^2 - Z^2 \right)$$

we get that:

$$\frac{\hat{a}}{a^\ell B^4} = \frac{\hat{b}}{b^\ell A^4}.$$

Thus we can conclude that for some constant c we have that $\hat{a} = a^\ell B^4 c$ and $\hat{b} = b^\ell A^4 c$.

Now we observe the image of the point $P = \left(\frac{1}{\sqrt{b}}, \frac{1}{\sqrt{a}} \right)$ under this isogeny. We first calculate the term inside the product for the x-coordinate map:

$$\frac{(1/\sqrt{b})^2 - (\alpha_i)^2}{\alpha_i^2 \left(1 - b^2 \alpha_i^2 (1/\sqrt{b})^2 \right)} = \frac{1 - b\alpha_i^2}{b\alpha_i^2 (1 - b\alpha_i^2} = \frac{1}{b\alpha_i^2}.$$

And thus the whole product, and hence the x-coordinate map of the isogeny becomes:

$$\frac{1}{\sqrt{b^\ell A^4}}.$$

Similarly, the y-coordinate map of the isogeny becomes:

$$\frac{1}{\sqrt{a^\ell B^4}}.$$

Plugging these values into the codomain curve, and making the substitutions $\hat{a} = a^\ell B^4 c$ and $\hat{b} = b^\ell A^4 c$ we get:

$$\frac{1}{\sqrt{b^\ell A^4}}(c - 1) = \frac{1}{\sqrt{a^\ell B^4}}(c - 1).$$

If $c \neq 1$, we can conclude that $\sqrt{b^\ell A^4} = \sqrt{a^\ell B^4}$. However, if this were the case, then the image of the point $P = \left(\frac{1}{\sqrt{b}}, \frac{1}{\sqrt{a}} \right)$ is a singular point on the codomain. This is not the case as can be seen by mapping this point to the Weierstrass model, performing the isogeny and mapping back to the Huff model. Thus $c = 1$ so that $\hat{a} = a^\ell B^4$ and $\hat{b} = b^\ell A^4$. □

5.3 Kernel polynomials for Huff curves

We can use kernel polynomials to write the Huff isogeny. Denote the points in the kernel by $\{(0,0),(\alpha_i,\beta_i),(-\alpha_i,-\beta_i) : i = 1 \dots s\}$. The kernel polynomials are

$$g(x) = \prod_{i=1}^{s}(x^2 - \alpha_i^2)$$

$$h(y) = \prod_{i=1}^{s}(y^2 - \beta_i^2),$$

Then by Theorem 4,

$$\psi(x,y) = \left(\frac{xg(x)}{g(0)(-bx)^{2s}g(\frac{1}{bx})}, \frac{yh(y)}{h(0)(-ay)^{2s}h(\frac{1}{ay})}\right).$$

The codomain curve is $H_{\hat{a},\hat{b}}$, where $\hat{a} = a^\ell h(0)^2$ and $\hat{b} = b^\ell g(0)^2$. Note again that this can be efficiently computed if we have an efficient algorithm for computing g and h.

5.4 More isogenies

We include a formula for 2-isogenies on Huff curves.

Theorem 5 *There is a 2-isogeny from the curve $H_{a,b}$ to the curve $H_{-(\sqrt{a}+\sqrt{b})^2,-(\sqrt{a}-\sqrt{b})^2}$ given by*

$$(x,y) \to \left(\frac{(bx-ay)}{(b-a)^2}\frac{((bx-ay)+\sqrt{ab}(x-y))^2}{bx^2-ay^2}, \right.$$
$$\left. \frac{(bx-ay)}{(b-a)^2}\frac{((bx-ay)-\sqrt{ab}(x-y))^2}{bx^2-ay^2}\right).$$

Proof The proof is similar to the method used for 2-isogenies for Edwards curves. The map

$$\phi_1(x,y) = \Big(\frac{bx-ay}{y-x}, \frac{b-a}{y-x}\Big),$$

sends $H_{a,b}$ to the Weierstrass curve $E_1 : y^2 = x^3 + (a+b)x^2 + abx$. The point $(0,0)$ on this curve has order 2, and by Vélu's formula we have a 2-isogeny

$$\phi_2(x,y) = \Big(\frac{x^2+ab}{x}, y\frac{x^2-ab}{x^2}\Big),$$

to the curve $E_2 : y^2 = x^3 + (a+b)x^2 - 4abx - 4ab(a+b)$. In order to map E_2 back to a Huff curve, we first use a linear translation to get it in the right form:

$$\phi_3(x,y) = (x + a + b, y).$$

The image of this map is the curve $E_3 : y^2 = x^3 - 2(a+b)x^2 + (a-b)^2x$. The inverse map of ϕ_1 requires a curve in the form $y^2 = x^3 + (c+d)x^2 + cdx$. Equating this with E_3, we need $c + d = -2(a+b)$, and $cd = (a-b)^2$. Solving this system, we get $c = -(\sqrt{a} + \sqrt{b})^2$ and $d = -(\sqrt{a} - \sqrt{b})^2$. The map

$$\phi_4(x,y) = \Big(\frac{x+c}{y}, \frac{x+d}{y}\Big) = \Big(\frac{x - (\sqrt{a}+\sqrt{b})^2}{y}, \frac{x - (\sqrt{a}-\sqrt{b})^2}{y}\Big),$$

takes E_3 to the Huff curve $H_{c,d}$. Composing the maps $\phi_1, \phi_2, \phi_3, \phi_4$ leads to the formulas given in the statement of the theorem. We omit the algebraic details. □

We are also able to give another explicit formula for odd degree isogenies for Huff curves.

Theorem 6 *Let $H_{a,b}$ be an elliptic curve given by the Huff model $x(ay^2 - 1) = y(bx^2 - 1)$. Let the kernel of the isogeny be $\{(0,0), (\alpha_1, \beta_1), (-\alpha_1, -\beta_1), \ldots, (\alpha_s, \beta_s), (-\alpha_s, -\beta_s)\}$. Then there is a $(2s+1)$-isogeny Ψ given by*

$$\psi(x,y) = \left(\frac{1}{b^{2s}} x \prod_{i=1}^{s} \frac{(x - \alpha_i/\beta_i y)(x + a\alpha_i\beta_i y)}{\alpha_i^4 (x - a\beta_i/b\alpha_i y)(x + 1/b\alpha_i\beta_i y)}, \right.$$
$$\left. y \prod_{i=1}^{s} \frac{(x - \alpha_i/\beta_i y)(x + 1/b\alpha_i\beta_i y)}{(x - a\beta_i/b\alpha_i y)(x + a\alpha_i\beta_i y)}\right).$$

The proof is similar to that of Theorem 3. This isogeny returns the same values as the Huff isogeny formula given by Theorem 4 in section 5.2.

6 Computation

There has been much interest in the various computational aspects of isogenies, especially efficiency, see [5], [6], [10], or [29] for example. The models for isogenies of elliptic curves in the past have only used the Weierstrass equation. With the Edwards and Huff isogeny formulas presented in this paper, we now have an alternative to previous work. In this section, we briefly examine the computational cost of computing the Edwards and Huff isogenies on input points, and compare it to known results for Weierstrass isogenies. We emphasize that we are only doing a quick analysis – a serious study will be the focus of future work.

For Edwards curves, we can evaluate an isogeny with kernel $\{\pm\alpha_i, \beta_i\} \cup (0,1)$ by

$$\psi(x,y) = \left(x \prod_{i=1}^{s} \frac{x^2 - \alpha_i^2/\beta_i^2 y^2}{1 - d^2\alpha_i^2\beta_i^2 x^2 y^2}, y \prod_{i=1}^{s} \frac{y^2 - \alpha_i^2/\beta_i^2 x^2}{1 - d^2\alpha_i^2\beta_i^2 x^2 y^2}\right).$$

Let M and S denote the cost of a multiplication and squaring in K respectively. Let C denote multiplication by a constant in K. If constants are carefully

chosen, the cost of the multiplications denoted by C could be significantly less than those in M, however, in the general case, we should regard C and M as equal. We ignore addition, as the cost of addition is usually much less than squaring and multiplication. We first compute x^2 and y^2, from which we deduce $dx^2y^2 = x^2 + y^2 - 1$, at a cost of $2S$. For each i, we then compute $x^2 - \alpha_i^2/\beta_i^2 y^2$, $y^2 - \alpha_i^2/\beta_i^2 x^2$, and $1 - d\alpha_i^2\beta_i^2(dx^2y^2)$. This requires $(3s)C$. Computing $x\prod_{i=1}^{s}(x^2 - \alpha_i^2/\beta_i^2 y^2)$, $y\prod_{i=1}^{s}(y^2 - \alpha_i^2/\beta_i^2 x^2)$, and $\prod_{i=1}^{s}(1 - d^2\alpha_i^2/\beta_i^2 x^2y^2)$ costs $(2 + 3(s-1))M$. In affine coordinates, we must invert $\prod_{i=1}^{s}(1 - d^2\alpha_i^2/\beta_i^2 x^2y^2)$, and perform 2 more multiplications M. Thus, the total affine cost is $(3s+1)M + 2S + 3sC + 1I$, where I is the cost of an inversion.

To avoid inversions, which can be costly, we look at using projective coordinates. The isogeny is

$$\psi(x,y,z) = \left(xz\prod_{i=1}^{s}(x^2 - \alpha_i^2/\beta_i^2 y^2) : yz\prod_{i=1}^{s}(y^2 - \alpha_i^2/\beta_i^2 x^2) : \prod_{i=1}^{s}(z^4 - d^2\alpha_i^2/\beta_i^2 x^2y^2) \right).$$

We can see we must also compute z^4, and xz and yz at a cost of $2M + 2S$. The total cost in the projective case is $(3s + 3)M + 4S + 3sC$.

We do not claim these formulas are optimal. They only provide an upper bound for the cost to evaluate an Edwards isogeny. For specific values of s, it is possible to do better. For example, using projective coordinates we have found a way to compute an Edwards 3-isogeny in $5M + 4S + 3C$, and a 5-isogeny in $6M + 6S + 5C$. For comparison, an optimized 3-isogeny is given in [11] which costs $3M + 3S + 1C$, and an optimized 5-isogeny is given in [26] which costs $8M + 5S + 7C$. Both of these optimized formulas were given for Weierstrass curves. It is more complicated to determine the *exact* cost of evaluating a general $(2s + 1)$-isogeny on an input point for Weierstrass curves. From [25], it can be seen that the cost is bounded above by $(3 + o(1))(2s + 1)(M + C) + I$. Using our formulas, it appears that evaluating isogenies is more efficient on Edwards curves than on Weierstrass curves.

For Huff curves, we use the formula

$$\psi(x,y) = \left(x\prod_{i=1}^{s}\frac{x^2 - \alpha_i^2}{\alpha_i^2(1 - b^2\alpha_i^2 x^2)}, y\prod_{i=1}^{s}\frac{y^2 - \beta_i^2}{\beta_i^2(1 - a^2\beta_i^2 y^2)} \right).$$

A similar analysis shows we can evaluate ψ with $(4s-2)M + 2S + (2s)C + 2I$ in the affine case, and $(4s + 3)M + 3S + (4s)C$ in the projective case. A possible reason the Huff isogeny might not be as efficient as the Edwards isogeny lies in the denominators. In the Edwards case, the same denominator is used for both the x and y-coordinates, while for Huff isogenies, different denominators must be calculated.

7 Conclusion

In this paper we have found isogeny formulas for Edwards and Huff curves, similar to Vélu's formulas for Weierstrass curves. It is interesting that these

formulas are "multiplicative", compared to the "additive" Vélu formula. The new isogeny formulas also yield rational maps that are easier to express than Vélu's formula.

These new isogeny formulas have potential uses in many applications. As there are many uses for isogenies on isogenies of Weierstrass curves in the literature, it is likely that the faster evaluation of Edwards (or Huff) isogenies could improve performance of these results by switching models. This is similar to how the Edwards addition law can speed up point multiplication on elliptic curves. Such possibilities include the SEA algorithm [31], pairings [6], the Doche-Icart-Kohel technique [11], or in public key cryptosystems [20].

We also leave it as future work to optimize the computations in section 6. Our preliminary operation counts show the isogeny formulas are efficient, but this analysis needs more work. Another research topic is to find similar isogeny formulas for other models of curves, such as Hessian curves, Jacobi quartics, or Jacobi intersections. Yet another interesting direction would be to address some of the other computational problems associated with isogenies (mentioned in the introduction.) In particular the problem of computing an isogeny of known degrees from the domain and codomain.

References

[1] O. Ahmadi, and R. Granger, On isogeny classes of Edwards curves over finite fields, Cryptology ePrint Archive Report 2011/135, (2011). Available at `http://eprint.iacr.org/2011/135`.

[2] D. Bernstein, P. Birkner, M. Joye, T. Lange, C. Peters. Twisted Edwards curves, in: Progress in cryptology—AFRICACRYPT 2008, S. Vaudenay (ed.), Lecture Notes in Comput. Sci. 5023, Springer, pp. 389–405 (2008).

[3] D. Bernstein, and T. Lange, Faster addition and doubling on elliptic curves, in: Advances in cryptology—ASIACRYPT 2007, K. Kurosawa (ed.), Lecture Notes in Comput. Sci. 4833, Springer, pp. 29-50 (2007).

[4] G. Bisson, and A. Sutherland, Computing the Endomorphism Ring of an Ordinary Elliptic Curve over a Finite Field, J. Number Theory, 131 (5), pp. 815–831, (2011).

[5] A. Bostan, F. Morain, B. Salvy, and E. Schost, Fast algorithms for computing isogenies between elliptic curves, Math. Comp. 77, pp. 1755–1778, (2008).

[6] R. Broker, D. Charles, and K. Lauter. Evaluating large degree isogenies and applications to pairing based cryptography, in: Pairing 08: Proceedings of the 2nd international conference on Pairing-Based Cryptography, Lecture Notes in Comput. Sci. 5209, Springer-Verlag, pp. 100-112, (2008).

[7] R. Broker, K. Lauter, and A. Sutherland, Modular polynomials via isogeny volcanoes, to appear in Math. Comp., (2012).

[8] D. Charles, E. Goren, and K. Lauter, Cryptographic hash functions from expander graphs, J. Cryptology, 22 (1), pp. 93–113, (2009).

[9] H. Debiao, C. Jianhua, and H. Jin, A Random Number Generator Based on Isogenies Operations, Cryptology ePrint Archive Report 2010/94, (2010). Available at `http://eprint.iacr.org/2010/094`.

[10] L. De Feo. Algorithmes Rapides pour les Tours de Corps Finis et les Isogenies, PhD thesis. Ecole Polytechnique X, (2010).

[11] C. Doche, T. Icart, and D. Kohel, Efficient Scalar Multiplication by Isogeny Decompositions, in: Public Key Cryptography-PKC 2006, Lecture Notes in Comput. Sci. 3958, Springer-Verlag, pp. 285–352, (2006).

[12] H. Edwards, A normal form for elliptic curves, Bull. Amer. Math. Soc. 44, pp. 393–422 (2007).

[13] N. Elkies, Elliptic and modular curves over finite fields and related computational issues, In: Computational perspectives on number theory: proceedings of a conference in honor of AOL Atkin, D.A. Buell and J.T. Teitelbaum (Eds.), pp. 21–76 (1997).

[14] R. Farashahi, On the Number of Distinct Legendre, Jacobi, Hessian and Edwards Curves (Extended Abstract), in: Proceedings of the Workshop on Coding theory and Cryptology (WCC 2011), pp. 37–46, (2011). Available at `hal.inria.fr/docs/00/60/72/79/PDF/76.pdf`.

[15] R. Farashahi, I. Shparlinski. On the number of distinct elliptic curves in some families. Des. Codes Cryptogr. 54(1), pp. 83-99, (2010).

[16] R. Feng, and H. Wu, Elliptic curves in Huff's model, Cryptology ePrint Archive Report 2010/390, (2010). Available at `http://eprint.iacr.org/2010/390.pdf`.

[17] M. Fouquet, and F. Morain, Isogeny Volcanoes and the SEA Algorithm, In: Proceedings of the 5th International Symposium on Algorithmic Number Theory (ANTS-V), C. Fieker and D. Kohel (Eds.). Springer-Verlag, pp. 276–291, (2002).

[18] L. Hitt, G. Mcguire, and R. Moloney, Division polynomials for twisted Edwards curves, Preprint, (2008). Available at `http://arxiv.org/PS_cache/arxiv/pdf/0907/0907.4347v1.pdf`.

[19] G. Huff, Diophantine problems in geometry and elliptic ternary forms, Duke Math. J. 15, pp. 443–453, (1948).

[20] D. Jao, L. De Feo, Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies, Cryptology ePrint Archive, Report 2011/506, (2011). Available at `http://eprint.iacr.org/2011/506`.

[21] D. Jao, S. D. Miller, and R. Venkatesan, Do all elliptic curves of the same order have the same difficulty of discrete log?, In: Advances in Cryptology ASIACRYPT 2005, B. Roy (Ed.), Lecture Notes in Comput. Sci. 3788, pp. 21–40, (2005).

[22] M. Joye, M. Tibouchi, and D. Vergnaud, Huff's model for elliptic curves, In: 9th Algorithmic Number Theory Symposium (ANTS-IX), G. Hanrot, F. Morain, E. Thomé, (Eds.), Lecture Notes in Comput. Sci. 6197, Springer-Verlag, pp. 234–250, (2010).

[23] G. McGuire, and R. Moloney, Two Kinds of Division Polynomials For Twisted Edwards Curves, to appear in Appl. Algebra Engrg. Comm. Comput., (2011). Available at `http://arxiv.org/PS_cache/arxiv/pdf/0907/0907.4347v1.pdf`.

[24] D. Kohel, Endomorphism Rings of Elliptic Curves over Finite Fields, PhD thesis, University of California at Berkeley, (1996).

[25] R. Lercier and F. Morain, Algorithms for computing isogenies between elliptic curves, in: Computational Perspectives on Number Theory, AMS/IP Stud. Adv. Math. 7, Amer. Math. Soc., pp. 77–96, (1997).

[26] D. Moody, Using 5-isogenies to quintuple points on elliptic curves, Inf. Process. Lett. 111 (7), pp. 314–317, (2011).

[27] D. Moody, and H. Wu, $\mathbb{F}_q$-Isomorphism classes of Edwards and twisted Edwards curves, Cryptology ePrint Archive, Report 2011/206, (2011). Available at `http://eprint.iacr.org/2011/206`.

[28] A. Rostovtsev and A. Stolbunov, Public-key cryptosystem based on isogenies, Cryptology ePrint Archive, Report 2006/145, (2006). Available at `http://eprint.iacr.org/2006/145`.

[29] D. Shumow, Isogenies of Elliptic Curves: A Computational Approach, Masters Thesis, University of Washington, (2009).

[30] J. Silverman, The arithmetic of elliptic curves, Springer-Verlag, New York, (1986).

[31] R. Schoof, Elliptic curves over finite fields and the computation of square roots mod p, Math. Comp. 44, pp. 483–494, (1985).

[32] A. Stolbunov, Constructing public-key cryptographic schemes based on class group action on a set of isogenous elliptic curves, Adv. Math. Commun. 4(2), pp. 215–235, (2010).

[33] A. Sutherland, Computing Hilbert class polynomials with the Chinese Remainder Theorem, Math. Comp. 80, pp.501-538, (2011).

[34] E. Teske, An Elliptic curve trapdoor system, J. Cryptology, 19 (1), pp. 115–133, (2006).

[35] J. Vélu, Isogénies entre courbes elliptiques, C.R. Acad. Sc. Paris, Série A., 273, pp. 238–241 (1971).

[36] L. Washington, Elliptic curves (Number theory and cryptography), 2nd edition, Chapman & Hall, Boca Raton, Fl, (2008).