ANALOGUES OF VÉLU'S FORMULAS FOR ISOGENIES ON ALTERNATE MODELS OF ELLIPTIC CURVES

DUSTIN MOODY AND DANIEL SHUMOW

Abstract. Isogenies are the morphisms between elliptic curves, and are accordingly a topic of interest in the subject. As such, they have been well-studied, and have been used in several cryptographic applications. Vélu's formulas show how to explicitly evaluate an isogeny, given a specification of the kernel as a list of points. However, Vélu's formulas only work for elliptic curves specified by a Weierstrass equation. This paper presents formulas similar to Vélu's that can be used to evaluate isogenies on Edwards curves and Huff curves, which are normal forms of elliptic curves that provide an alternative to the traditional Weierstrass form. Our formulas are not simply compositions of Vélu's formulas with mappings to and from Weierstrass form. Our alternate derivation yields efficient formulas for isogenies with lower algebraic complexity than such compositions. In fact, these formulas have lower algebraic complexity than Vélu's formulas on Weierstrass curves.

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 [22], are used in the SEA point counting algorithm [13],[18],[32] 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],[25], computing modular and Hilbert class polynomials [7],[34], and in the construction of new public key cryptosystems [21],[28],[33],[35].

Traditionally, elliptic curves have been specified by Weierstrass equations. However, this is only one possible model for elliptic curves. There are alternate models, such as Edwards and to a lesser extent Huff curves, that have been proposed for use in cryptography. These models have different point addition formulas that are simpler and have fewer special cases. The simpler formulas yield more efficient arithmetic that requires less expensive operations like multiplication and division, whereas fewer special cases in the point addition formulas give improved security by reducing information leakage through side channels.

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.

2000 *Mathematics Subject Classification.* Primary: 14K02; Secondary: 14H52, 11G05, 11Y16.
Key words and phrases. Elliptic curve, isogeny, Edwards curve, Huff curve.

(3) Given the kernel of an isogeny, determine the rational function form of the isogeny (up to isomorphism).
(4) Given the rational function form of an isogeny, compute the image through the isogeny on given input points.
(5) Given a prime l and an elliptic curve E, enumerate all elliptic curves l-isogenous to E.

This paper primarily focuses on problem 3, and also partially on problem 4.

From a high level, isogenies of elliptic curves are an algebraic concept independent of the specific model chosen for the curve. However, for computational aspects the model chosen for the curve is important. Vélu [36] gives explicit formulas for isogenies between curves specified by Weierstrass equations. This paper presents explicit formulas for isogenies in Edwards and Huff form. This is convenient as it allows one to evaluate isogenies directly on these alternate models, without converting back to Weierstrass form.

This is 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. This is, in fact, the case. The main contribution of this paper is a solution to problem 3, as listed above. Specifically, given an elliptic curve in Edwards or Huff form, and a finite kernel of an isogeny on this curve, we give explicit formulas for the isogeny. These isogeny formulas are not simply compositions of Vélu's formulas with mappings to and from Weierstrass form. This allows for more efficient formulas with strictly better algebraic complexity.

For previous work on the aspects of efficient computation of isogenies on Weierstrass curves see [5], [6], or [10]. For isogenies of Edwards curves, the only paper in the literature is [1], which counts the number of isogeny classes of an Edwards curve over a finite field.

For solving problem 4, Vélu's formulas run in time linear in the degree of the isogeny (assuming the kernel points are in the base field). In [6], the authors present an approach to problem 4 that is logarithmic in the degree of the isogeny. However, this approach is exponential in the discriminant of the endomorphism ring of the curve and only applies to *horizontal* isogenies. As such, for some specific curves the approach of [6] may be more efficient, but for the general case Vélu's approach is better as it has no reliance on the discriminant and is valid for all isogenies. The formulas in this paper are of a Vélu like approach, and as such scale linearly in the degree of the isogeny. However, they provide a more efficient solution for the evaluation of isognies of elliptic curves (problem 4 above) than known results for computing Vélu's formulas on Weiestrass curves in [5] and [10].

This paper is organized as follows. Section 2 reviews basic facts about isogenies, including Vélu's formulas. Section 3 covers Edwards curves and Huff curves. Sections 4 and 5, give the analogue of Vélu's formula for Edwards and Huff curves respectively. Section 6 presents a brief look at the computational cost (problem 4) of computing the formulas from sections 4 and 5. We also include some timings to demonstrate the practicality of our results. Finally, section 7 concludes with directions for future study.

2. Preliminaries

2.1. **Weierstrass Form.** Let K be a perfect field, and $\overline{K}$ a fixed algebraic closure of K. Any elliptic curve over K can be written in Weierstrass form

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

with the $a_i \in K$. For a curve in Weierstrass form, there is a point at infinity, denoted ∞. It is well known that the set of K-rational points (x, y) on E, together with the point ∞, form an abelian group.

2.2. **Isogenies.** Recall a few basic facts about isogenies. For a more complete reference, see [31] or [37]. An isogeny is a nonzero homomorphism (defined over K) given by rational maps from the curve E to another elliptic curve. If the kernel of a (separable) cyclic isogeny ϕ has order l, then ϕ is known as an l-isogeny, and l is the degree of the isogeny.

Let $\phi : E \to E'$ denote an isogeny. If the pullback of the invariant differential ω' of E' along ϕ is equal to the invariant differential ω of E, then ϕ is said to be *normalized*. As the space of differentials is one dimensional, we know $\phi^*\omega' = c_\phi\omega$, for some $c_\phi \in \overline{K}^*$. If $c_\phi = 1$, then $\phi^*\omega' = \omega$ and ϕ is normalized.

The kernel of ϕ does not uniquely determine ϕ, which can be seen by composing ϕ with an isomorphism $\psi : E' \to E''$. However, a finite subgroup F of an elliptic curve does uniquely determine a normalized isogeny with kernel F.

2.3. **Vélu's formulas.** For simplicity, assume the characteristic of $K \neq 2, 3$. Let $E : y^2 = x^3 + ax + b$ be an elliptic curve in short Weierstrass form, with l odd. Let F be a subgroup of E of order l. In [36], Vélu showed how to explicitly find the rational function form of a normalized isogeny $\phi : E \to E'$ with kernel F. These formulas are presented here, for comparison with the new formulas for Edwards and Huff curves presented in sections 4 and 5.

Define ϕ as follows. For $P = (x_P, y_P) \notin F$, let

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

For any point $P \in F$, 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. Furthermore, since x_{P+Q} is a rational function of the coordinates of P and Q, so is $x_{\phi(P)}$. See [36] for more details, including the explicit rational functions as well as the equation for the codomain curve.

We present the rational functions given by Vélu, for purposes of comparison with the isogeny formulas that we derive. To express the rational functions for ϕ, consider points of F excluding the point at ∞. Notice that if a point $P \neq \infty$ 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 $P \in F^+$ if and only if $-P \in F^-$. 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 showed how the isogeny ϕ can be alternatively written in terms of its kernel polynomial [25]. The kernel polynomial is defined as

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

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

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

More generally, neither Vélu's paper nor Kohel's requires that l be odd, nor E be given by a simplified Weierstrass equation, although the equations are simpler 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

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

with $d \neq 0, 1$. Twisted Edwards curves are a generalization of Edwards curves, proposed in [2]. These twisted Edwards 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, 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:

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

The identity on $E_{a,d}$ is the point $(0, 1)$, and the inverse of the point (x, y) is $(-x, y)$. Note that the Edwards curve E_d always has a cyclic subgroup of order 4, namely $\{(0,1), (0,-1), (1,0), (-1,0)\}$. Twisted Edwards curves always have a point of order 2, but not necessarily of order 4.

There is a birational transformation from $E_{a,d}$ 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 $E : y^2 = x^3 + 2(a+d)x^2 + (a-d)^2 x$. 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 [23]. The model was used by Huff in 1948 to solve a certain diophantine equation [20]. In [17], 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 $-P = (-x, -y)$, and the identity is $(0, 0)$. 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. The addition formula (for points that are not these points at infinity) is

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

There is also a simple birational transformation from a curve in Huff form to a curve in Weierstrass form [20]. 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.** Before describing the results on isogenies, we first examine isomorphisms between Edwards curves. For any $u \neq 0$ in K, it is easy to see the map $I_u : E_{a,d} \to E_{u^2a,u^2d}$ given by $I_u(x, y) = (x/u, y)$ is an isomorphism. We also consider the map $J(x, y) = (x, 1/y)$, that takes a point on $E_{a,d}$ to a point on $E_{d,a}$.

However, these maps are not the only isomorphisms of Edwards curves. It suffices to consider only Edwards curves, and not the more general twisted Edwards curves, because for a suitable choice of u, then I_u maps a twisted Edwards curve to one with $a = 1$ (though this map may only be defined over a quadratic extension of K.) 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 (over an extension of K). From [31, III.3.1] it is easy to check that the only isomorphisms between curves of the form $y^2 = x^3 + Ax^2 + Bx$ have maps of the form

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

for some u, r with $u \neq 0$.

If $r = 0$, then comparing the coefficients of the image of I' with those of $E_{\hat{d}}$ we find that $(1 + d)u^2 = 1 + \hat{d}$, and $(1 - d)^2u^4 = (1 - \hat{d})^2$. Solving these equations simultaneously, we find $u = \pm 1$, or $u^2 = 1/d$. For $u = 1$ or -1, then $\hat{d} = d$ and the isomorphism is the identity map or negation map, respectively. If instead $u^2 = 1/d$, then $\hat{d} = 1/d$. Let $\sqrt{d}$ denote a fixed square root of d. Then the isomorphism is $J \circ I_{1/\sqrt{d}} : (x, y) \to (\sqrt{d}x, 1/y)$ mapping E_d to $E_{1/d}$.

In the case $r \neq 0$, then again comparing the coefficients of the image of I' with those of $E_{\hat{d}}$ we find that we must have $r^2 + 2(1+d)r + (1-d)^2 = 0$. Thus $r = -1 - d \pm 2\sqrt{d}$, and we are left with the equations

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

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

Our convention for the symbols $\pm$ and $\mp$ is that in each formula, take all the signs on top, or alternatively all the signs on the bottom of each symbol. This system can be solved for u and $\hat{d}$, although the details are more tedious and hence are omitted. The solution to this system of equations leads to non-trivial isomorphisms of the form

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

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

Isomorphisms of Edwards curves have been discussed in the literature. For example, [1] includes some explicit Edwards isomorphisms. Also, the question of the number of Edwards curve isomorphism classes over finite fields is discussed in [14], [15], [16].

4.2. **2-isogenies in Edwards Form.** As shown in in section 3.1 there are birational maps from Edwards curves to Weierstrass curves. The most intuitive approach to find explicit isogenies for Edwards curves is to combine these maps with Vélu's formula.

Let ϕ_1 be the transformation from the Edwards curve E_d to a Weierstrass curve E given in (1). Let ϕ_2 be an l-isogeny from E to another curve E', whose rational functions are as given by Vélu's formula. The Weierstrass equation for E' (as computed from Vélu's formula) is not likely to be in the form

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

for some $\hat{d}$, so it is not immediately obvious how to find such a birational transformation to map this image curve back to an Edwards curve. However, the birational transformation which does work is described in [3]. Let $P = (r_2, s_2)$ be a point of order 2 on the image curve E'. 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 $\hat{d} = 1 - 4r_1^3/s_1^2$. Thus $a = 2\frac{1+\hat{d}}{1-\hat{d}}r_1$ and $b = r_1^2$. The map

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

maps to the Edwards curve

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

Composing the three maps ϕ_1, ϕ_2, and ϕ_3 gives an explicit l-isogeny ψ from E_d to $E_{d'}$. Applying this observation yields simple explicit formulas for 2-isogenies of Edwards curves.

Theorem 1. *Let E_d be an Edwards curve, and γ,δ, and i be elements (possibly in an extension) of K such that $\gamma^2 = 1 - d$, $\delta^2 = d$, and $i^2 = -1$. 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

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

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

Finally

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

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

Proof. For $l = 2$, the kernel of one 2-isogeny is the set $\{(0, 1), (0, -1)\}$. For this kernel, it suffices to explicitly find the maps ϕ_1, ϕ_2, and ϕ_3 as described above. The map $\phi_1 : E_d \to E$ was already given in equation (1). Formulas for 2-isogenies are well-known, see Example 4.5 of [31, III] for the 2-isogeny $\phi_2 : E \to E'$

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

The equation for E' is the curve

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

The points $(\pm 2(1 - d), 0)$, and $(-2(1 + d), 0)$ each have order 2. The first map is the linear transformation $(x, y) \to (x - 2(1 - d), y)$ that maps the curve E' to the curve

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

As $a = -4(d - 2) = 2\frac{1+\hat{d}}{1-\hat{d}}r_1$ and $b = 16(1 - d) = r_1^2$, it is easy to see 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 given in equation (2) with these values of r_1 and $\hat{d}$. Composing the maps and simplifying the equations leads to the stated formula for ψ_1. The algebraic details are straightforward and omitted for brevity. The other stated 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].

The 2-isogenies in Theorem 1 may not be defined over the same field as E_d. This is the case when any of the elements $-1, d, d - 1$, or $1 - d$ are not a square in K. Hence, each of these isogenies is defined over a quadratic extension of K. Furthermore, a simple argument based on observing the effect that any 2-isogeny must have on the point at the identiy and the points of order 2, as well as preserving

negation, shows that the rational functions of the coordinate maps of any 2-isogeny cannot have lower degree.

4.3. **Edwards curve isogenies.** This section presents a formula for isogenies on Edwards curves analogous to Vélu's formulas, stated in section 2. For l larger than 2, the approach in the last subsection of mapping to and from a Weierstrass curve, while theoretically possible, leads to far more complex formulas. The following formulas are simpler to express, manipulate and immediately lend themselves to a more efficient implementation. As opposed to the previous section, the approach in this section is to directly derive the isogeny formulas from the point addition formulas.

To show that the approach of mapping to Weierstrass from Edwards to apply Vélu's formulas leads to more complicated formulas, consider the example of $l = 3$. The Weierstrass equation for the image of the 3-isogeny is $E' : y^2 = x^3 + 2(1 + d)x^2 + a_4x + a_6$, with

$$a_4 = \frac{(1-d)}{(1-\beta)^2}(79d\beta^2 + 42d\beta + \beta^2 - 42\beta - d - 79),$$

$$a_6 = -8\frac{(1-d)}{(1-\beta)^3}(44d^2\beta^3+27d^2\beta^2-12d\beta^3-d^2\beta-58d\beta^2-\beta^2-58d\beta+27\beta-12d+44).$$

Here (α, β) is a point of order 3 on the Edwards curve E_d. The point

$$(x_4, y_4) = \left(\frac{5d\beta^3 - d\beta^2 - \beta^3 - 3\beta^2 - 4\beta + 4}{\beta^2(1-\beta)}, -2\frac{d\beta^3 + 2d\beta^2 - \beta^3 + 2\beta^2 - 4}{\beta^3}\right)$$

can be shown to have order 4 on E'. Accordingly, the Weierstrass curve E' can be mapped to the Edwards curve $E_{\hat{d}}$, with $\hat{d} = 1 - 4x_4^3/y_4^2$. By attempting to compose the birational transformations to and from the Weierstrass form with Velu's formulas, it quickly becomes apparent that the formulas become unwieldy and this approach is not ammenable to formulating simple explicit formula. For larger values of l, the situation grows even more complex. In contrast, the results presented below are much simpler. They also show a striking similarity in appearance to Vélu's formulas.

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 $l = 2s + 1$, 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 $\hat{d} = B^8d^l$ and $B = \prod_{i=1}^s \beta_i$. The coordinate maps are given by:

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

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 (4) from the Edwards curve addition law.

It remains to derive the formula for $\hat{d}$ on the image curve:

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

where $X(P)$ and $Y(P)$ are the coordinate maps of ϕ. To accomplish this, consider the function

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

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, to 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 gives

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

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

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

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

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

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

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

Substituting these into the equation of the image of ψ yields

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

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, as argued above G has a zero of order 2 at $x = 0$. So G must be 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, thus the codomain of this map is another Edwards curve. Hence, the transformation in (4) is a rational map from an Edwards curve to another that preserves the identity point. This is necessarily an isogeny [31, III.4.8].

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

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

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

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

Note that the formula for isogenies given in Theorem 1 also works for twisted Edwards curves $E_{a,d}$. This is easiest to see by observing that the map $(x, y) \to (x/\sqrt{a}, y)$ maps $E_{a,d}$ to $E_{1,d/a}$. Then applying Theorem 2, which maps to the curve $E_{1,B^8(d/a)^l}$. Mapping back to the twisted Edwards form by sending $(X, Y) \to (\sqrt{a^l}X, Y)$ 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 $l = 2s + 1$, 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 $\hat{a} = a^l$, $\hat{d} = B^8 d^l$ and $B = \prod_{i=1}^{s} \beta_i$.

Now, using Corollary 1 it is possible to give the formula for the unique normalized isogeny of twisted Edwards curves, given the kernel. This is comparable with Vélu's formulas, which are normalized and hence unique.

Theorem 3. *Suppose F is a subgroup of the twisted Edwards curve $E_{a,d}$ with odd order $l = 2s + 1$, and points*

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

Define

$$\Psi(P) = \left(x_P \prod_{Q \in F - (0,1)} \frac{x_{P+Q}}{x_Q}, y_P \prod_{Q \in F-(0,1)} \frac{y_{P+Q}}{y_Q} \right).$$

Then Ψ is a normalized l-isogeny, with kernel F, from the curve $E_{a,d}$ to the curve $E_{\hat{a},\hat{d}}$ where $\hat{a} = A^4/B^4 a^l$ and $\hat{d} = A^4 B^4 d^l$, with $A = \prod_{i=1}^{s} \alpha_i, B = \prod_{i=1}^{s} \beta_i$. The coordinate maps are given by:

$$\Psi(x,y) = \left((-1)^s \frac{x}{A^2} \prod_{i=1}^{s} \frac{\beta_i^2 x^2 - \alpha_i^2 y^2}{1 - d^2 \alpha_i^2 \beta_i^2 x^2 y^2}, \frac{y}{B^2} \prod_{i=1}^{s} \frac{\beta_i^2 y^2 - \alpha_i^2 x^2}{1 - d^2 \alpha_i^2 \beta_i^2 x^2 y^2} \right). \tag{4}$$

Proof. Let Ψ be the composition of the isogeny ψ from Corollary 1 and the isomorphism $\phi(x,y) \to ((-1)^s \frac{B^2}{A^2} x, y)$. Thus Ψ is also an isogeny with kernel F. From section 2.2, we know that the image is $E_{\hat{a},\hat{d}}$ with $\hat{a} = \frac{A^4}{B^4} a^l$ and $\hat{d} = A^4 B^4 d^l$. Thus it only remains to check that Ψ is normalized.

The twisted Edwards curve equation is $ax^2 + y^2 = 1 + dx^2 y^2$. The invariant differential can thus be written:

$$\omega = \frac{\partial x}{2y(1 - dx^2)}.$$

As seen in Section 2.2, for Ψ to be normalized, the pullback of the invariant differential must be equal to the invariant differential on the domain curve $E_{\hat{a},\hat{d}}$. That is, if $\Psi(x,y) = (\Psi_x(x,y), \Psi_y(x,y))$, then

$$\frac{\partial \Psi_x}{2\Psi_y(1 - \hat{d}\Psi_x^2)} = \frac{c\partial x}{2y(1 - dx^2)},$$

for some constant c. It remains to to show that $c = 1$. As $\partial \Psi_x = \Psi'_x \partial x$, this simplifies to

$$c\frac{\Psi_y}{y} = \Psi'_x \frac{(1 - dx^2)}{1 - \hat{d}\Psi_x^2}.$$

Expanding the coordinate map Ψ_y as a power series (as done in Theorem 2), gives that the left hand side is

$$\begin{aligned} c\frac{\Psi_y}{y} &= c \prod_{i=1}^{s} \left(1 + (d\beta_i^2 - 1/\beta_i^2)x^2 + O(x^4)\right) \\ &= c\left(1 + \left(\sum_{i=1}^{s} (d\beta_i^2 - 1/\beta_i^2)\right) x^2 + O(x^4)\right). \end{aligned}$$

For the right hand side, note

$$\begin{aligned}\Psi_x &= (-1)^s \frac{x}{A^2} \prod_{i=1}^{s} (-\alpha_i^2 + O(x^2)) \\ &= x + O(x^3).\end{aligned}$$

Consequently,

$$\begin{aligned}\frac{1 - dx^2}{1 - \hat{d}\Psi_x^2} &= (1 - dx^2)(1 + \hat{d}\Psi_x^2 + O(\Psi_x^4)) \\ &= (1 - dx^2)(1 + \hat{d}x^2 + O(x^4)) \\ &= 1 + O(x^2).\end{aligned}$$

So the complete right hand side is

$$\begin{aligned}\Psi'_x \frac{1 - dx^2}{1 - \hat{d}\Psi_x^2} &= (1 + O(x^2))(1 + O(x^2)) \\ &= 1 + O(x^2).\end{aligned}$$

Equating the constant coefficients of the two equal power series gives $c = 1$. Thus Ψ is normalized.

□

4.4. **Uniform Variable Formulas For Edwards Isogenies.** This section presents formulas for isogenies on Edwards curves that are written (almost) entirely in terms of one variable. Let $l = 2s + 1$ be the degree of the isogeny. We can assume the isogeny ψ satisfies $\psi(1, 0) = (1, 0)$. If not, simply compose ϕ with the negation map.

Theorem 4. *Let E_d be an Edwards curve with subgroup $F = \{(0, 1), (\pm\alpha_i, \beta_i) : i = 1 \dots s\}$. Then the map*

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

is an isogeny with kernel F. The polynomials $f(y)$ and $g(y)$ are the unique even polynomials of degree $2s$ satisfying:

$$\begin{aligned} f(0) &= (-1)^s \prod_{i=1}^{s} \beta_i^2 & f(\alpha_j) &= \beta_j \prod_{i=1}^{s} (\alpha_j^2 - \beta_i^2), \\ g(1) &= \prod_{i=1}^{s} (1 - \alpha_i^2), & g(\beta_j) &= \beta_j \prod_{i=1}^{s} (\beta_j^2 - \alpha_i^2). \end{aligned} \tag{5}$$

This isogeny is the same as the isogeny given by Theorem 2. The image is the curve $E_{B^s d^l}$.

Proof. Let $\psi : E_d \to E_{\hat{d}}$ be the isogeny described above. 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 [19],[24]) that over E_d, the coordinate maps can be uniquely expressed as $X = p(y) + xq(y)$ 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 $r(y) - xs(y) = r(y) + xs(y)$, and hence $p(y) = 0$ and $s(y) = 0$.

Next, $(\pm\alpha_i, \beta_i)$ 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 $(\pm\alpha_i, \beta_i) + (0, -1) = (\mp\alpha_i, -\beta_i)$, so $\psi(\mp\alpha_i, -\beta_i) = \psi(0, -1) = (0, -1)$. 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 implies

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

for some polynomial $f(y)$.

Similarly, using the identities$(x, y) + (1, 0) = (y, -x)$, and $(x, y) + (-1, 0) = (-y, x)$, gives that $\psi(\pm\beta_i, \alpha_i) = (\pm 1, 0)$ and $\psi(\pm\beta_i, -\alpha_i) = (\mp 1, 0)$. Trivially $\psi(\pm 1, 0) = (1, 0)$. Thus

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

for some polynomial $g(y)$.

Evaluating at the points in the kernel, gives the equations in (5). 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 shows $f(-y) = f(y)$ 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 $\tilde{x}$ be a square root of $\frac{1-\tilde{y}^2}{1-d\tilde{y}^2}$ 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, given that all points in the kernel were already determined. 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. **Edwards Isogenies From Kernel Polynomials.** In the previous sections, the kernel of an isogeny was assumed to be expressed as a list of points in the kernel. However, this is merely one way of expressing the kernel. An alternate method is by a kernel polynomial. That is, a polynomial with roots at the coordinates of the kernel points (each kernel polynomial is uniform in either the x or y coordinate). This approach was originally used for computing the rational maps of isogenies by D. Kohel in his thesis, where he showed how the kernel polynomial of an isogeny can also be used to explicitly write down an isogeny [25] for Weierstrass curves. This was summarized in the section 2.3.

We present a similar approach to determine the rational maps of an isogeny from kernel polynomials for Edwards curves. For Weierstrass form, kernel polynomials are usually expressed in terms of the x coordinates, but the symmetry of coordinates in Edwards form admits equally sufficient kernel polynomials in the x and y coordinates. If the kernel is $\{(0,1),(\pm\alpha_1,\beta_1),\ldots,(\pm\alpha_s,\beta_s)\}$, then the x-coordinate kernel polynomial is

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

which has as roots the $\pm\alpha_i$. Alternatively the y-coordinate kernel polynomial is

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

Applying Theorem 2, the isogeny $\psi(x,y)=(X,Y)$ can be written

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

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

Note that it is possible to compute X solely in terms of x (and not y), and likewise it is possible to solely express Y in terms of y (and not x). Writing these in terms of the kernel polynomials, gives

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

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

The codomain of this isogeny is the curve $E_{\hat{d}}$, where $\hat{d} = d^{2s+1}\prod_{i=1}^{s}\beta_i^8 = d^{2s+1}h(0)^4 = dg(1)^2/g(1/\sqrt{d})^2$.

5. Isogenies on Huff curves

5.1. **Isomorphisms.** Let $H_{a,b}$ be the Huff curve $x(ay^2-1)=y(bx^2-1)$, with $ab(a-b)\neq 0$. Suppose Ψ is an isomorphism (over K) 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 over K. 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 $u, r \in K$, with $u \neq 0$. When $r = 0$, composing the maps $I' \circ \phi$ gives a map from $H_{a,b}$ to $y^2 = x^3 + (a + b)u^2x^2 + abu^4x$. It follows 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 $r \neq 0$, it is easy to check that $r = -a$ or $r = -b$. When $r = -a$, the codomain curve is $y^2 = x^3 + (b - 2a)u^2x^2 + a(a - b)u^4x$, this shows 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 the composition map is $H_{a,b}$ to $H_{(a-b)u^2,-bu^2}$ given by $(x, y) \to \left(\frac{x}{u}, \frac{bx-ay}{u(b-a)}\right)$.

There is also the isomorphism $(x, y) \to (y, x)$ which sends $H_{a,b}$ to $H_{b,a}$.

5.2. **Huff isogenies.** This section presents explicit formulas for isogenies of Huff curves that are similar to Vélu's as presented in Section 2. The derivation of these forumlae proceeds in a similar fashion to the derivation in the Edwards case. Let F be the desired kernel of an isogeny. 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 5. *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 with kernel F from the curve $H_{a,b}$ to the curve $H_{\hat{a},\hat{b}}$, where $\hat{a} = a^l B^4$ and $\hat{b} = b^l A^4$. Using the addition law, we can write

$$\psi(x, y) = \left(\frac{x}{A^2} \prod_{i=1}^{s} \frac{\alpha_i^2 - x^2}{1 - b^2\alpha_i^2 x^2}, \frac{y}{B^2} \prod_{i=1}^{s} \frac{\beta_i^2 - y^2}{1 - a^2\beta_i^2 y^2} \right). \tag{6}$$

The equation (6) *is valid for points which are not points at infinity. The points at infinity are mapped to the points at infinity on the codmain curve.*

Proof. First it is straightforward to see that ψ maps F and only F to $(0, 0)$. It remains to show that the image of ψ is the Huff curve $H_{\hat{a},\hat{b}}$. As was done in the Edwards case, this is accomplished by counting the zeros of the rational coordinate maps by evaluating them as power series. Due to the similarilities, we omit much of the details in the calculations.

First we parameterize the Huff curve $H_{a,b}$ by $t = ay - bx$, which has a simple zero at the identity point $(0, 0)$ as well as $(a : b : 0)$ and simple poles at $(1 : 0 : 0)$ and $(0 : 1 : 0)$. Now consider the function x over the Huff curve. Thus reparameterizing the coordinates by t gives:

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

and

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

where both x and y have simple zeros at $(0,0)$.

For the points at infinity, affine coordinate are not sufficient, so the formulas must be evaluted in projective coordinates. Doing so shows x has simple poles at $(1:0:0)$ and $(a:b:0)$, as well as a simple zero at $(0:1:0)$. In addition, y has simple poles at $(0:1:0)$ and $(a:b:0)$ and a simple zero at $(1:0:0)$. These are the only zeroes and poles of x and y.

Write the map in (6) as $\psi(x,y) = (X,Y)$. A straightforward calculation leads to

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

and similarly,

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

Define

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

A computation shows

$$G_{c,d} = \frac{1}{(a-b)^3}\left(b-a+c-d + \sum_{i=1}^{s} \frac{1-a^2\beta_i^4}{\beta_i^2} - \frac{1-b^2\alpha_i^4}{\alpha_i^2}\right)t^3 + O(t^5). \tag{7}$$

The only possible poles of $G_{c,d}$ are at the poles of X and Y. We leave it to the reader to verify that 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. Also, 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 most a simple pole there. The same is true for $(0:1:0)$. At $(a:b:0)$, there will be at most a triple pole for $G_{c,d}$. Now, at the points $\pm(1/b\alpha_i, -\beta_i)$ there is at most a simple pole, and similarly at $\pm(-\alpha_i, 1/a\beta_i)$. Finally, note that $G_{c,d}$ has at most a triple pole at the points $\pm(-1/b\alpha_i, -1/a\beta_i)$. So the total number of poles (counting multiplicity) is is at most $10s+5 = 5l$.

Equation (7) shows 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, it is possible to 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 $7+14s = 7l$ zeroes. This is more than the number of possible 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. Thus there is a rational map which sends $H_{a,b}$ to another Huff curve and maps $(0,0)$ to $(0,0)$. This is necessarily an isogeny [31, III.4.8]. However, while this proof shows that it is possible to find the codomain of this isogeny, we do not present explicit expressions for c and d. This is because there is a significantly easier way to derive this codomain formula, presented as follows.

Using projective coordinates, we find the point $(a:b:0)$ maps to the projective point $(a^lB^4(-ab)^{2s} : b^lA^4(-ab)^{2s} : 0)$, which is equivalent to the point $Q = (a^lB^4 : b^lA^4 : 0)$.

As Q is a point on the curve $H_{\hat{a},\hat{b}} : X\left(\hat{a}Y^2 - Z^2\right) = Y\left(\hat{b}X^2 - Z^2\right)$, then we must have that

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

Thus there exists a constant c such that $\hat{a} = a^l B^4 c$ and $\hat{b} = b^l A^4 c$.

Next observe the image of the point $P = (\gamma, \delta)$ under this isogeny, where $\gamma^2 = 1/b$ and $\delta^2 = 1/a$. Calculating, we find $\psi(P) = \left((-1)^s \gamma^l / A^2, (-1)^s \delta^l / B^2\right)$. Plugging the coordinates of $\psi(P)$ into the equation for $H_{\hat{a},\hat{b}}$ and substituting in $\hat{a} = a^l B^4 c$, $\hat{b} = b^l A^4 c$ leads to

$$\frac{\gamma^l}{A^2}(c-1) = \frac{\delta^l}{B^2}(c-1).$$

If $c \neq 1$ then $\gamma^l A^2 = \delta^l B^2$. However, if this were the case, then the image of the point $P = (\gamma, \delta)$ 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 $\hat{a} = a^l B^4$ and $\hat{b} = b^l A^4$. □

Theorem 6. *The Huff isogeny given by Theorem 5 is normalized.*

Proof. This is a similar approach to the one used to derive the formulas for Edwards curves. First observe the effect of the isogeny on the invariant differential of the Huff curve:

$$\frac{\phi'_x dx}{2\hat{a}\phi_x\phi_y - \hat{b}\phi_x^2 + 1} = \frac{c dx}{2axy - bx^2 + 1},$$

or

$$\phi'_x(2axy - bx^2 + 1) = c(2\hat{a}\phi_x\phi_y - \hat{b}\phi_x^2 + 1). \tag{8}$$

The expansions of x, y, ϕ_x, and ϕ_y in powers of t are given in the proof of Theorem 5 above. Substituting these into equation (8), and comparing the constant term on both the left and right sides leads to $c = 1$, as desired. □

5.3. **Huff isogenies from kernel polynomials.** As for Edwards curves, it is useful to have formulas for Huff isogenies where the kernel is specified by the kernel polynomial. We note that for both the Edwards and Huff cases, the derivation of isogeny formulas from the kernel polynomial is quite straightforward, in contrast to the Weierstrass case where it is not obvious. Denote the points in the kernel by $\{(0,0), (\alpha_i, \beta_i), (-\alpha_i, -\beta_i) : i = 1 \ldots s\}$. 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 5,

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

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

5.4. **Huff 2-isogenies.** The Huff curve isogenies presented in the previous subsections only work for odd degree isogenies. So, for completeness this section presents formulas for 2-isogenies on Huff curves.

Theorem 7. *Let $\eta \in \overline{K}$ be such that $\eta^2 = ab$. There is a 2-isogeny from the Huff curve $H_{a,b}$ to the Huff curve $H_{-(a+2\eta+b),-(a-2\eta+b)}$ given by*

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

Proof. This proof is similar to the method used for 2-isogenies for Edwards curves. It consists of composing the maps to and from Huff curves to Weierstrass curves (given in Section 3), along with a known 2-isogeny between the relevant Weierstass curves. As the maps to and from Huff curves were already given, we only include the equations for the 2-isogeny. In this regard, the map

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

is a 2-isogeny from $y^2 = x^3 + (a+b)x^2 + abx$ to $y^2 = x^3 - 2(a+b)x^2 + (a-b)^2x$. For brevity the algebraic details are omitted. □

6. Computation

As isogenies are a useful tool in computational mathematics and cryptography, there has been much interest and work in the literature on the various computational aspects of isogenies, especially efficiency, see [5], [6], [10], or [30] for example. However, until now the assessment of efficiency of the evaluation of isogenies has only used Weierstrass curves. With the Edwards and Huff isogeny formulas presented in this paper, we now have an alternative to this previous work. This section briefly examines the computational cost, in terms of algebraic complexity, of evaluating the formulas for Edwards and Huff isogenies on input points, and compares it to known results for Weierstrass isogenies. This initial assessment shows that for both Edwards curves and Huff curves the isogeny formulas, have strictly less multiplication operations than Vélu's formulas for Weierstrass curves. Both the Edwards and Huff curve formulas require approximately half the operations that the Weierstrass curves do. This is not intended to be an in depth analysis of the complexity of these formulas, but rather a quick analysis to show that the formulas presented in this paper do, in fact, have better finite size scaling than Vélu's formulas, without further optimization.

First for the case of Edwards curves, the isogeny with kernel $\{\pm\alpha_i, \beta_i\} \cup \{(0,1)\}$ has coordinate maps

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

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 can be significantly less than those in M, however, in the general case, C and M should be regarded as equal. It is standard

to ignore additions and subtraction, as the cost of these operations is much less than squaring and multiplication. First computing x^2 and y^2, gives $dx^2y^2 = x^2 + y^2 - 1$, at a cost of $2S$. For each i, one must 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, the formulas require inversions of $\prod_{i=1}^{s}(1 - d^2\alpha_i^2/\beta_i^2 x^2y^2)$ and 2 more multiplications M. Thus, the total affine cost is $(3s+1)M + 2S + 3sC + I$, where I is the cost of an inversion.

Projective coordinates are used to avoid inversions, which are costly. The isogeny is

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

However, there are trade offs as it is also necesssary to 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 [27] 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 [26], it can be seen that the cost is bounded above by $(3+o(1))(2s+1)M + S + (3+o(1))(2s+1)C + I$. So using these formulas it appears that evaluating isogenies is more efficient on Edwards curves than on Weierstrass curves, by approximately a factor of two.

For Huff curves, The formula derived for an isogeny with kernel $\{\pm\alpha_i, \beta_i\} \cup \{(0,1)\}$ is

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

A similar analysis shows that it is possible to 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. In this naive analysis, Huff isogenies are not as efficient as the Edwards isogeny, and this has to do with 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. However, when one equates multiplications with constant multiplications, the Huff curves also require approximately half as many expensive algebraic operations (although the analysis may be more complicated if the two operations have drastically different timings).

Figure 1 shows the performance of SAGE [29] implementations of isogeny computation for curves represented in in Edwards, Huff and Weierstrass form. The implementations were written in SAGE, and are straightforward implementations of the affine formulas presented herein for Edwards and Huff curves. They match the exact algebraic complexity analysis presented above. The Weierstrass implementation used for comparison is the EllipticCurveIsogeny class included in SAGE. To perform these measurements, it was necessary to generate elliptic curves for testing the isogeny formulas. These experiments represent 511 curves defined over

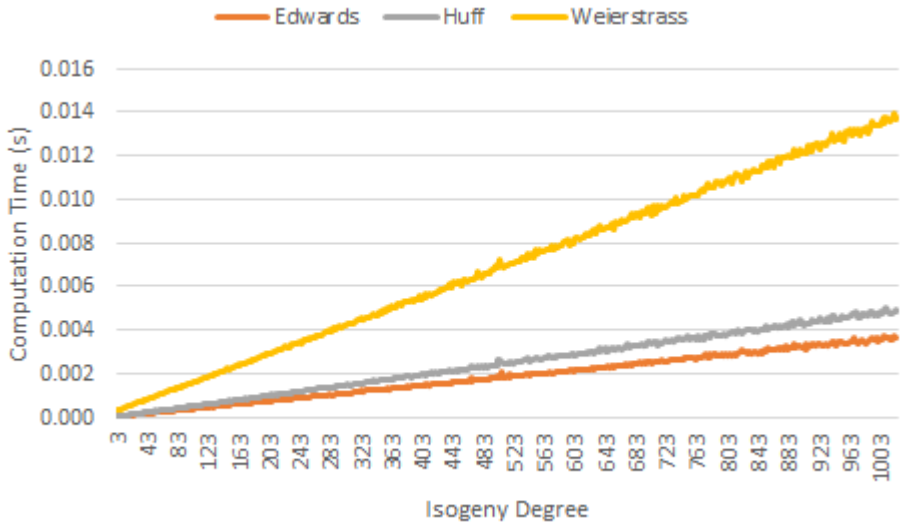

FIGURE 1. Isogeny computation time by model.

256 bit prime order fields. For each odd integer k between 3 and 1023, there is an elliptic curve with a subgroup of order k. Note that the prime moduli varied for each curve, but were always 256 bits. None of the formulas are dependant on special forms for the moduli and the performance of the underlying field arithmetic was the same across fields. The curves were selected such that each curve admits a representation in Weierstrass, Edwards and Huff forms over the given prime modulus. To perform the the timing, each odd order subgroup was used as a kernel for an isogeny and evaluated with the formulas for the respective models. As such, the timings compare the same isogeny calcuation, varying only the representation of the curve and corresponding isogeny formulae. The computation time was calculated by using the timing functionality built in to SAGE and provided by the sage_timeit class. These performance experiments confirm the algebraic complexity analyses of the isogeny formulas presented here; specifically, these experiments show that straight forward implementations of isogenies on curves in Edwards and Huff form are considerably faster than Vélu's formula's on curves in Weierstrass form.

7. Conclusion

This paper presents isogeny formulas for Edwards and Huff curves, similar to Vélu's formulas for Weierstrass curves. It is interesting to note that these formulas are "multiplicative", compared to the "additive" form of Vélu's formulas. Furthermore, because the addition law on these alternate forms of curves is simpler than Weierstrass form, these new isogeny formulas also yield rational maps that are simpler to express than Vélu's formulas. In addition to being simpler to express, these isogeny formulas also yield strictly better algebraic complexity in the general case, indicating that they will improve the performance of evaluating isogenies.

These new isogeny formulas have potential uses in many applications. As there are many uses for 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 [32], pairings [6], the Doche-Icart-Kohel technique [11], or in public key cryptosystems [21].

This paper leaves many directions for future work. The preliminary operation counts show the isogeny formulas are efficient, however this analysis is incomplete and it remains to do a deep optimization of the computations in section 6. Another similar research topic is derivations of 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, J. Number Theory, 132 (6), pp. 1337-1358, (2011).

[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, Math. Comp. 81, pp. 1201-1231, (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, D. Moody, and H. Wu, Isomorphism classes of Edwards curves over finite fields, Finite Fields Appl. (18), pp. 597–612, (2012).

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

[17] 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`.
[18] 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).
[19] 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`.
[20] G. Huff, Diophantine problems in geometry and elliptic ternary forms, Duke Math. J. 15, pp. 443–453, (1948).
[21] D. Jao, and L. de Feo, Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies, Post-Quantum Cryptography pp. 19-34 (2011).
[22] 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).
[23] 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).
[24] G. McGuire, and R. Moloney, Two Kinds of Division Polynomials For Twisted Edwards Curves, Appl. Algebra Engrg. Comm. Comput. 22 (5), pp. 321–345, (2011).
[25] D. Kohel, Endomorphism Rings of Elliptic Curves over Finite Fields, PhD thesis, University of California at Berkeley, (1996).
[26] 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).
[27] D. Moody, Using 5-isogenies to quintuple points on elliptic curves, Inf. Process. Lett. 111 (7), pp. 314–317, (2011).
[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] SAGE software, *Version 4.3.5*, `http://sagemath.org`.
[30] D. Shumow, Isogenies of Elliptic Curves: A Computational Approach, Masters Thesis, University of Washington, (2009).
[31] J. Silverman, The arithmetic of elliptic curves, Springer-Verlag, New York, (1986).
[32] R. Schoof, Elliptic curves over finite fields and the computation of square roots mod p, Math. Comp. 44, pp. 483–494, (1985).
[33] 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).
[34] A. Sutherland, Computing Hilbert class polynomials with the Chinese Remainder Theorem, Math. Comp. 80, pp.501-538, (2011).
[35] E. Teske, An Elliptic curve trapdoor system, J. Cryptology, 19 (1), pp. 115–133, (2006).
[36] J. Vélu, Isogénies entre courbes elliptiques, C.R. Acad. Sc. Paris, Série A., 273, pp. 238–241 (1971).
[37] L. Washington, Elliptic curves (Number theory and cryptography), 2nd edition, Chapman & Hall, Boca Raton, Fl, (2008).

Computer Security Division, National Institute of Standards and Technology (NIST), Gaithersburg MD, USA
E-mail address: `dustin.moody@nist.gov`

eXtreme Computing Group, Microsoft Research, Redmond WA, USA
E-mail address: `danshu@microsoft.com`