2-1-2019

Connecting legendre with kummer and edwards

Sabyasachi Karati
University of Calgary

Palash Sarkar
Indian Statistical Institute, Kolkata

Connecting Legendre with Kummer and Edwards

Sabyasachi Karati
iCIS Lab
Department of Computer Science
University of Calgary
Canada
e-mail: sabyasachi.karati@ucalgary.ca

Palash Sarkar
Applied Statistics Unit
Indian Statistical Institute
203, B.T. Road, Kolkata
India 700108.
e-mail: palash@isical.ac.in

December 14, 2017

Abstract

Scalar multiplication on Legendre form elliptic curves can be speeded up in two ways. One can perform the bulk of the computation either on the associated Kummer line or on an appropriate twisted Edwards form elliptic curve. This paper provides details of moving to and from between Legendre form elliptic curves and associated Kummer line and moving to and from between Legendre form elliptic curves and related twisted Edwards form elliptic curves. Further, concrete twisted Edwards form elliptic curves are identified which correspond to known Kummer lines at the 128-bit security level which provide very fast scalar multiplication on modern architectures supporting SIMD operations.
Keywords: Elliptic curve, Legendre form, Edwards form, Kummer line

1 Introduction

Scalar multiplication over an elliptic curve is a basic operation for implementation of basic public key functionalities including Diffie-Hellman key exchange and digital signature schemes. Consequently, secure and efficient algorithms for scalar multiplication are of paramount importance in practical deployment of such schemes. Depending on the target functionality, it is required to consider various cases of scalar multiplication, namely fixed base scalar multiplication, variable base scalar multiplication and multi-scalar multiplication. Diffie-Hellman key exchange has two phases, the first phase consists of computation of the public key and requires a fixed base scalar multiplication whereas the second phase consists of shared secret computation and requires a variable base scalar multiplication. On the other hand, signature generation requires a fixed base scalar multiplication while signature verification requires multi-scalar multiplication.

Our Contributions:

Gaudry and Lubicz [12] had proposed the use of Kummer line for scalar multiplication. This idea has been developed in [15] where all the relevant details were worked out. The work [15] also proposed several concrete Kummer lines targeted at the 128-bit security level and provided implementations of these on modern Intel platforms supporting single instruction multiple data (SIMD) operations. For such platforms, the obtained timing results indicate that for genus one curve over large characteristic fields, Kummer lines provide the fastest scalar multiplication algorithm. In particular, the obtained timings are better than the best known implementation of the widely deployed Curve25519. This result is relevant mainly for variable base scalar multiplication. For fixed base scalar multiplication, it is possible to improve the timings by working over suitable twisted Edwards curves. The present work makes the following contributions.

Connecting Legendre to Kummer: A Kummer line is not a group. In fact, a Kummer line is associated with a Legendre form elliptic curve. A scalar multiplication on the Kummer line does not require the y-coordinate of the Legendre curve point. For shared secret computation in Diffie-Hellman computation, it is sufficient to consider only variable base scalar multiplication on the Kummer line. More generally, one may be interested in performing a full scalar multiplication on the Legendre form curve. This requires a method for recovering the y-coordinate of the result from the Kummer line computation. The first contribution of the present paper is to provide a detailed explicit formula for doing this. The earlier work [15] had briefly sketched the method, but, the details provided in the present work were not given in [15].

Connecting Legendre to Edwards: As mentioned above, fixed base scalar multiplication can benefit from the use of suitable twisted Edwards form curve. The fastest known scalar multiplication formula is for special types of twisted Edwards form curves [13]. Our second and main contribution is to provide three conversion methods from Legendre form curves to appropriate twisted Edwards form curves. Two of the conversion methods are birational equivalences while the third one is a 2-isogeny. Each method is built by composing several individual mappings. All of the individual mappings have appeared earlier in the literature. Our contribution is to put together these mappings in an appropriate manner and to supply details which have not been provided in earlier works. We go beyond the task of just providing the mappings and propose concrete twisted Edwards form curves corresponding to the concrete Kummer lines introduced in [15].

The net effect of the present work is to obtain a set of concrete Legendre form curves and associated Kummer lines and twisted Edwards form curves. Scalar multiplication on the Legendre form curves can be done by moving to either the associated Kummer line or to the associated twisted Edwards form curve. The complete details for moving to and from between the Legendre form curves and the associated Kummer lines and for moving to and from between the Legendre form curves and the corresponding twisted Edwards form curves are provided. Depending on the requirement, one may choose to perform scalar multiplication on the Legendre form curve via the Kummer line or via the twisted Edwards form curve. For certain applications, it may also be sufficient to work only on the Kummer line or only on the twisted Edwards form curve.

Previous and Related Works:

Elliptic curve cryptography (ECC) was introduced independently by Koblitz [16] and Miller [17]. Over the years, ECC has become the method of choice for compact and efficient implementation of various public key operations. Montgomery [18] introduced the so-called Montgomery form of elliptic curves which provided a method for very fast x-coordinate only scalar multiplication. The famous Curve25519 proposed by Bernstein [2] is based on the Montgomery form elliptic curve. Bernstein and Lange [4] proposed the use of Edwards form curve [9] to cryptography. A later work [5] introduced the twisted Edwards form curve. The fastest known scalar multiplication algorithm for certain types of twisted Edwards form curves was proposed by Hisil et al [13]. Gaudry [11] proposed the use of Kummer surfaces for speeding up scalar multiplication and a later work by Gaudry and Lubicz [12] suggested the use of Kummer lines. As mentioned earlier, this idea was fully developed in [15] where concrete Kummer lines were suggested and implementation and timing results were reported.

2 Kummer Line and Elliptic Curves

A brief background on Kummer lines and the relevant forms of elliptic curves are provided in this section.

2.1 Kummer Line

Let $\mathbb{C}$ be the field of complex numbers. Kummer lines are defined using theta functions over $\mathbb{C}$. On the other hand, for cryptographic purposes, we will work over a prime field of large characteristic. The derivations that

are used have a good reduction [12] which makes it possible to use the Lefschetz principle [1, 10] to carry over the identities which hold over the complex to those over a large characteristic field.

Let $\vartheta_1, \vartheta_2, \Theta_1$ and Θ_2 be functions from $\mathbb{C}$ to $\mathbb{C}$ satisfying the following identities.

$$\begin{aligned} 2\Theta_1(\mathsf{w}_1+\mathsf{w}_2)\Theta_1(\mathsf{w}_1-\mathsf{w}_2) &= \vartheta_1(\mathsf{w}_1)\vartheta_1(\mathsf{w}_2)+\vartheta_2(\mathsf{w}_1)\vartheta_2(\mathsf{w}_2); \\ 2\Theta_2(\mathsf{w}_1+\mathsf{w}_2)\Theta_2(\mathsf{w}_1-\mathsf{w}_2) &= \vartheta_1(\mathsf{w}_1)\vartheta_1(\mathsf{w}_2)-\vartheta_2(\mathsf{w}_1)\vartheta_2(\mathsf{w}_2); \end{aligned} \tag{1}$$

$$\begin{aligned} \vartheta_1(\mathsf{w}_1+\mathsf{w}_2)\vartheta_1(\mathsf{w}_1-\mathsf{w}_2) &= \Theta_1(2\mathsf{w}_1)\Theta_1(2\mathsf{w}_2)+\Theta_2(2\mathsf{w}_1)\Theta_2(2\mathsf{w}_2); \\ \vartheta_2(\mathsf{w}_1+\mathsf{w}_2)\vartheta_2(\mathsf{w}_1-\mathsf{w}_2) &= \Theta_1(2\mathsf{w}_1)\Theta_1(2\mathsf{w}_2)-\Theta_2(2\mathsf{w}_1)\Theta_2(2\mathsf{w}_2). \end{aligned} \tag{2}$$

For the concrete definition of the theta functions in genus one and the proofs of the above identities, we refer to [15]. For the general theory covering higher genus we refer to [19, 14] and to [11, 12] for proposing cryptographic applications of theta functions.

Putting $w_1 = w_2 = w$ in (1) and (2), we obtain

$$\begin{aligned} 2\Theta_1(2\mathsf{w})\Theta_1(0) &= \vartheta_1(\mathsf{w})^2+\vartheta_2(\mathsf{w})^2; \\ 2\Theta_2(2\mathsf{w})\Theta_2(0) &= \vartheta_1(\mathsf{w})^2-\vartheta_2(\mathsf{w})^2; \end{aligned} \tag{3}$$

$$\begin{aligned} \vartheta_1(2\mathsf{w})\vartheta_1(0) &= \Theta_1(2\mathsf{w})^2+\Theta_2(2\mathsf{w})^2; \\ \vartheta_2(2\mathsf{w})\vartheta_2(0) &= \Theta_1(2\mathsf{w})^2-\Theta_2(2\mathsf{w})^2. \end{aligned} \tag{4}$$

Putting $\mathsf{w} = 0$ in (3), we obtain

$$\begin{aligned} 2\Theta_1(0)^2 &= \vartheta_1(0)^2+\vartheta_2(0)^2; \\ 2\Theta_2(0)^2 &= \vartheta_1(0)^2-\vartheta_2(0)^2. \end{aligned} \tag{5}$$

Denote by $\mathbb{P}^1(\mathbb{C})$ the projective line over $\mathbb{C}$. Given $\mathsf{a}^2 = \vartheta_1(0)^2$ and $\mathsf{b}^2 = \vartheta_2(0)^2$, the Kummer line $\mathcal{K}_{\mathsf{a}^2,\mathsf{b}^2}$ is the image of the map φ from $\mathbb{C}$ to $\mathbb{P}^1(\mathbb{C})$ defined by

$$\varphi : \mathsf{w} \longmapsto [\vartheta_1(\mathsf{w}) : \vartheta_2(\mathsf{w})]. \tag{6}$$

Let A and B be such that $\mathsf{A}^2 = \mathsf{a}^2 + \mathsf{b}^2$ and $\mathsf{B}^2 = \mathsf{a}^2 - \mathsf{b}^2$.

Suppose that $\mathsf{P} = [\mathsf{x}_1^2 : \mathsf{z}_1^2]$ is known where $\mathsf{x}_1 = \vartheta_1(\mathsf{w})$, $\mathsf{z}_1 = \vartheta_2(\mathsf{w})$ and $\varphi(\mathsf{w}) = [\vartheta_1(\mathsf{w}) : \vartheta_2(\mathsf{w})]$ for some $\mathsf{w} \in \mathbb{C}$. Using (3) and (4) it is possible to compute $2\mathsf{P} = [\mathsf{x}_3^2 : \mathsf{z}_3^2]$ where $\mathsf{x}_3 = \vartheta_1(2\mathsf{w})$ and $\mathsf{z}_3 = \vartheta_2(2\mathsf{w})$ without knowing the value of w. This procedure is called doubling and Algorithm dbl in Table 1 shows how to obtain x_3^2 and z_3^2 from x_1^2 and z_1^2.

Suppose that $\mathsf{P}_1 = [\mathsf{x}_1^2 : \mathsf{z}_1^2]$, $\mathsf{P}_2 = [\mathsf{x}_2^2 : \mathsf{z}_2^2]$ and $\mathsf{P}_1 - \mathsf{P}_2 = [\mathsf{x}^2 : \mathsf{z}^2]$ are known, where $\mathsf{x}_i = \vartheta_1(\mathsf{w}_i)$, $\mathsf{z}_i = \vartheta_2(\mathsf{w}_i)$, $i = 1, 2$; $\mathsf{x} = \vartheta_1(\mathsf{w}_1 - \mathsf{w}_2)$ and $\mathsf{z} = \vartheta_2(\mathsf{w}_1 - \mathsf{w}_2)$. Using (1) and (2) it is possible to compute $\mathsf{P}_1 + \mathsf{P}_2 = [\mathsf{x}_3^2 : \mathsf{z}_3^2]$ where $\mathsf{x}_3 = \vartheta_1(\mathsf{w}_1 + \mathsf{w}_2)$ and $\mathsf{z}_3 = \vartheta_2(\mathsf{w}_1 + \mathsf{w}_2)$. This procedure is called differential (or pseudo) addition and Algorithm $\mathsf{diffAdd}$ in Table 1 shows how to obtain x_3^2 and z_3^2 from $\mathsf{x}_1^2, \mathsf{z}_1^2, \mathsf{x}_2^2, \mathsf{z}_2^2, \mathsf{x}^2$ and z^2.

With respect to the above defined doubling and differential addition, the point $[\mathsf{a}^2 : \mathsf{b}^2]$ acts as the identity element while the point $[\mathsf{b}^2 : \mathsf{a}^2]$ has order two. Given $\mathsf{P} = [\mathsf{x}_1^2 : \mathsf{z}_1^2]$ on $\mathcal{K}_{\mathsf{a}^2,\mathsf{b}^2}$ and a positive integer n, Algorithm $\mathsf{scalarMult}$ in Table 2 returns (R, S), where $\mathsf{R} = n\mathsf{P} = [\mathsf{x}_n^2 : \mathsf{z}_n^2]$ and $\mathsf{S} = (n+1)\mathsf{P} = [\mathsf{x}_{n+1}^2 : \mathsf{z}_{n+1}^2]$.

Since both doubling and differential addition work with only squared quantities, this is referred to as the square only setting.

Let p be a prime not equal to 2 and $\mathbb{F}_p$ be the finite field of q elements. As mentioned earlier, using the Lefschetz principle, we consider Kummer lines over $\mathbb{F}_p$. Also, $\mathbb{F}_p$ will be the underlying field for all the elliptic curves defined in the rest of the work.

$\mathsf{dbl}(\mathsf{x}^2, \mathsf{z}^2)$	$\mathsf{diffAdd}(\mathsf{x}_1^2, \mathsf{z}_1^2, \mathsf{x}_2^2, \mathsf{z}_2^2, \mathsf{x}^2, \mathsf{z}^2)$
$\mathsf{s}_0 = \mathsf{B}^2(\mathsf{x}^2 + \mathsf{z}^2)^2;$	$\mathsf{s}_0 = \mathsf{B}^2(\mathsf{x}_1^2 + \mathsf{z}_1^2)(\mathsf{x}_2^2 + \mathsf{z}_2^2);$
$\mathsf{t}_0 = \mathsf{A}^2(\mathsf{x}^2 - \mathsf{z}^2)^2;$	$\mathsf{t}_0 = \mathsf{A}^2(\mathsf{x}_1^2 - \mathsf{z}_1^2)(\mathsf{x}_2^2 - \mathsf{z}_2^2);$
$\mathsf{x}_3^2 = \mathsf{b}^2(\mathsf{s}_0 + \mathsf{t}_0)^2;$	$\mathsf{x}_3^2 = \mathsf{z}^2(\mathsf{s}_0 + \mathsf{t}_0)^2;$
$\mathsf{z}_3^2 = \mathsf{a}^2(\mathsf{s}_0 - \mathsf{t}_0)^2;$	$\mathsf{z}_3^2 = \mathsf{x}^2(\mathsf{s}_0 - \mathsf{t}_0)^2;$
return $(\mathsf{x}_3^2, \mathsf{z}_3^2)$.	return $(\mathsf{x}_3^2, \mathsf{z}_3^2)$.

Table 1: Double and differential addition in the square-only setting.

$\mathsf{scalarMult}(\mathsf{P}, n)$	$\mathsf{ladder}(\mathsf{R}, \mathsf{S}, \mathfrak{b})$
input: $\mathsf{P} \in \mathcal{K}_{\mathsf{a}^2,\mathsf{b}^2}$;	if $(\mathfrak{b} = 0)$
ℓ-bit scalar $n = (1, n_{\ell-2}, \ldots, n_0)$;	$\mathsf{S} = \mathsf{diffAdd}(\mathsf{R}, \mathsf{S}, \mathsf{P});$
output: $n\mathsf{P}$;	$\mathsf{R} = \mathsf{dbl}(\mathsf{R});$
set $\mathsf{R} = \mathsf{P}$ and $\mathsf{S} = \mathsf{dbl}(\mathsf{P})$;	else
for $i = \ell - 2, \ell - 3, \ldots, 0$ do	$\mathsf{R} = \mathsf{diffAdd}(\mathsf{R}, \mathsf{S}, \mathsf{P});$
$(\mathsf{R}, \mathsf{S}) = \mathsf{ladder}(\mathsf{R}, \mathsf{S}, n_i);$	$\mathsf{S} = \mathsf{dbl}(\mathsf{S});$
return (R, S).	return (R, S).

Table 2: Scalar multiplication on Kummer line using a ladder.

2.2 Legendre Form Elliptic Curve

The Legendre form elliptic curve $E_{L,\mu}$ in affine coordinates (x, y) is given by an equation

$$E_{L,\mu} : y^2 = x(x-1)(x-\mu) \tag{7}$$

with $\mu \in \mathbb{F}_p \backslash \{0\}$. The projective coordinates $(X : Y : Z)$ correspond to the affine point $(X/Z, Y/Z)$. In projective coordinates, the curve has the form $E_{L,\mu} : Y^2Z = X(X-Z)(X-\mu Z)$. To avoid introducing additional notation, we will use $E_{L,\mu}$ to denote both the affine and the projective forms of the curve. The intended form will be clear from the context. The curve $E_{L,\mu}$ has three points of order two, namely, $(0:0:1)$, $(1:0:1)$ and $(\mu:0:1)$. Let $\mathbf{T} = (\mu : 0 : 1)$.

Let $\mathcal{K}_{\mathsf{a}^2,\mathsf{b}^2}$ be a Kummer line such that

$$\mu = \frac{\mathsf{a}^4}{\mathsf{a}^4 - \mathsf{b}^4}. \tag{8}$$

Let $\sigma : E_{L,\mu} \to E_{L,\mu}$ be the automorphism which maps a point of $E_{L,\mu}$ to its inverse, i.e., for $(X : Y : Z) \in E_{L,\mu}$, $\sigma(X : Y : Z) = (X : -Y : Z)$. An explicit map $\psi : \mathcal{K}_{\mathsf{a}^2,\mathsf{b}^2} \setminus \{[\mathsf{b}^2 : \mathsf{a}^2]\} \to E_{L,\mu}/\sigma$ has been given in [12].

$$\psi([\mathsf{x}^2 : \mathsf{z}^2]) = \begin{cases} (1:0:0) & \text{if } [\mathsf{x}^2 : \mathsf{z}^2] = [\mathsf{a}^2 : \mathsf{b}^2]; \\ (\mathsf{a}^2\mathsf{x}^2 : \cdot : \mathsf{a}^2\mathsf{x}^2 - \mathsf{b}^2\mathsf{z}^2) & \text{otherwise;} \end{cases} \tag{9}$$

$$\psi^{-1}((X : \cdot : Z)) = \begin{cases} [\mathsf{a}^2 : \mathsf{b}^2] & \text{if } (X : \cdot : Z) = (1 : \cdot : 0); \\ [\mathsf{b}^2 X : \mathsf{a}^2(X - Z)] & \text{otherwise.} \end{cases} \tag{10}$$

The map ψ by itself does not preserve the consistency of doubling and differential addition between $E_{L,\mu}$ and $\mathcal{K}_{\mathsf{a}^2,\mathsf{b}^2}$. Instead, the map ψ needs to be extended to obtain a map $\widehat{\psi} : \mathcal{K}_{\mathsf{a}^2,\mathsf{b}^2} \setminus \{[\mathsf{b}^2 : \mathsf{a}^2]\} \to E_{L,\mu}/\sigma$ where

$$\widehat{\psi}(\mathsf{P}) = \psi(\mathsf{P}) + \mathbf{T}, \tag{11}$$

$$\widehat{\psi}^{-1}(\mathbf{P}) = \psi^{-1}(\mathbf{P} + \mathbf{T}). \tag{12}$$

The map $\widehat{\psi}$ preserves the consistency of doubling and addition between $E_{L,\mu}$ and $\mathcal{K}_{a^2,b^2}$. We refer to [15] for details. Further, it can be argued [12, 15] that the discrete logarithm problem in $E_{L,\mu}$ and $\mathcal{K}_{\mathsf{a}^2,\mathsf{b}^2}$ are equally hard.

2.3 Concrete Choices of Kummer Lines

For cryptographic purposes, we work over a large characteristic field. As mentioned earlier, since all the identities have good reductions, using the Lefschetz principle, the identities also hold over such finite fields. Further, since the characteristic p of the field will be large and we will choose small values of a^2 and b^2, $\mathsf{a}^4 - \mathsf{b}^4$ will not be zero modulo p so that μ is also defined over $\mathbb{F}_p$.

We consider the following concrete Kummer lines.

$\mathsf{KL}_{1a} := \mathsf{KL2519}(81, 20)$: The Kummer line $\mathcal{K}_{81,20}$ over the field $\mathbb{F}_{2^{251}-9}$.
$\mathsf{KL}_{1b} := \mathsf{KL2519}(186, 175)$: The Kummer line $\mathcal{K}_{186,175}$ over the field $\mathbb{F}_{2^{251}-9}$.
$\mathsf{KL}_2 := \mathsf{KL25519}(82, 77)$: The Kummer line $\mathcal{K}_{82,77}$ over the field $\mathbb{F}_{2^{255}-19}$.
$\mathsf{KL}_3 := \mathsf{KL2663}(260, 139)$: The Kummer line $\mathcal{K}_{260,139}$ over the field $\mathbb{F}_{2^{266}-3}$.

The work [15] proposed KL_{1a}, KL_2 and KL_3. We additionally consider KL_{1b}. The efficiency of scalar multiplication on KL_{1b} is the same as that of KL_{1a}. On the other hand, for conversion to twisted Edwards form, KL_{1b} provides a few more options which are not obtained from either KL_{1a}, KL_2 or KL_3.

By E_{1a}, E_{1b}, E_2 and E_3 we will denote the group of $\mathbb{F}_p$-rational points of the Legendre form elliptic curves corresponding to KL_{1a}, KL_{1b}, KL_2 and KL_3 respectively.

All of the proposals provide security at about the 128-bit level. The relevant properties of these proposals are shown in Table 3. Comparison to other well known proposals are given in [15]. In Table 3, ℓ and ℓ_T are the orders of the largest prime subgroups of the curves and their quadratic twists; h and h_t are the co-factors of the curves and their quadratic twists; and D is the complex multiplication field discriminant [3].

Table 3: Some properties of the group of $\mathbb{F}_p$-rational points of the Legendre form elliptic curves E_{1a}, E_{1b}, E_2 and E_3.

	E_{1a}	E_{1b}	E_2	E_3
p	$2^{251}-9$	$2^{251}-9$	$2^{255}-19$	$2^{266}-3$
$(\lg \ell, \lg \ell_T)$	$(248, 248)$	$(248, 248)$	$(251.4, 252)$	$(262.4, 263)$
(h, h_T)	$(8, 8)$	$(8, 8)$	$(12, 8)$	$(12, 8)$
(k, k_T)	$\left(\ell - 1, \frac{\ell_T - 1}{7}\right)$	$(\ell - 1, \ell_T - 1)$	$(\ell - 1, \ell_T - 1)$	$\left(\frac{\ell-1}{2}, \ell_T - 1\right)$
$\lg(-D)$	246.3	249.8	255	266
KL base pt	$[64 : 1]$	$[19 : 1]$	$[31 : 1]$	$[2 : 1]$

2.4 Twisted Edwards Form Elliptic Curve

The twisted Edwards form elliptic curve $E_{E,a,d}$ in affine coordinates (u, v) is given by the equation

$$E_{E,a,d} : au^2 + v^2 \quad = \quad 1 + du^2v^2 \tag{13}$$

with $a, d \in \mathbb{F}_p \setminus \{0\}$ and $a \neq d$.

The extended affine coordinates [13] (u, v, t) is obtained by introducing an auxilliary coordinate $t = uv$. The extended twisted Edwards coordinates [13] is a projective coordinate system $(U : V : T : W)$ with $W \neq 0$,

which corresponds to the extended affine coordinates $(U/W, V/W, T/W)$. The identity element is represented as $(0:1:0:1)$ and the inverse of (U,V,T,W) is $(-U:V:-T:W)$.

If $a=-1$, i.e., the curve $E_{E,-1,d}$ has the currently fastest addition algorithm in the extented twisted Edwards coordinates. So, it is of interest to be able to move from $E_{E,a,d}$ to $E_{E,-1,d'}$. Based on the discussion in Section 2 of [5], we have the following two options.

Suppose the Legendre symbols $\left(\frac{a}{p}\right)$ and $\left(\frac{-1}{p}\right)$ are equal. Then a can be written as $a=-b^2$ for some $b \in \mathbb{F}_p$. The map

$$(\overline{u}, \overline{v}) \quad \mapsto \quad (u,v) = (b\overline{u}, \overline{v}) \tag{14}$$

is an isomorphism over $\mathbb{F}_p$ from $E_{E,a,d} : a\overline{u}^2 + \overline{v}^2 = 1 + d\overline{u}^2\overline{v}^2$ to $E_{E,-1,-d/a} : -u^2 + v^2 = 1 + (-d/a)u^2v^2$.

Suppose $\left(\frac{a}{p}\right) \neq \left(\frac{-1}{p}\right)$ but, $\left(\frac{d}{p}\right) = \left(\frac{-1}{p}\right)$. The map

$$(\hat{u}, \hat{v}) \quad \mapsto \quad (\overline{u}, \overline{v}) = (\hat{u}, 1/\hat{v}) \tag{15}$$

is a birational equivalence over $\mathbb{F}_p$ from $E_{E,a,d} : a\hat{u}^2 + \hat{v}^2 = 1 + d\hat{u}^2\hat{v}^2$ to $E_{E,d,a} : d\overline{u}^2 + \overline{v}^2 = 1 + a\overline{u}^2\overline{v}^2$ having the exceptional point $\hat{v}=0$. One can then apply the map in (14) to $E_{E,d,a}$ to move to $E_{E,-1,-a/d}$.

Remark: The equation $-u^2 + v^2 = 1 + du^2v^2$ can be rewritten as $u^2(1+dv^2) = v^2 - 1$. If $1+dv^2 = 0$, then $v^2 = 1$ and then $d=-1$. So, if $d \neq -1$, then $1+dv^2 \neq 0$ and $u = \pm\sqrt{(v^2-1)/(1+dv^2)}$. On the other hand, if $d=-1$, then $v^2=1$ corresponds to the two points $(0,1)$ (the identity) and $(0,-1)$ (having order 2). In our applications, $d \neq -1$. So, given the value of v and the sign of u, it is possible to uniquely determine u. Following [6], this allows compressing the point (u,v) to $(\mathsf{sgn}(u), v)$ which is useful for applications to Edwards curve based signature verification.

2.5 Montgomery form Elliptic Curve

The Montgomery form elliptic curve $E_{M,A,B}$ in affine coordinates (r,s) is given by an equation

$$E_{M,A,B} : Bs^2 \quad = \quad r^3 + Ar^2 + r \tag{16}$$

with $A \in \mathbb{F}_p \setminus \{-2, 2\}$ and $B \in \mathbb{F}_p \setminus \{0\}$. We will encounter Montgomery form elliptic curves while transiting from Legendre form curves to Edwards form curves. There will be no occasion to use projective coordinates of the Montgomery form and hence we do not introduce it here.

The connection between Montgomery and twisted Edwards form that we will use is given by Theorem 3.2 of [5]. The Montgomery curve $E_{M,A,B} : Bs^2 = r^3 + Ar^2 + r$ is birationally equivalent to the twisted Edwards curve $E_{E,a,d} : au^2 + v^2 = 1 + du^2v^2$ with $a = (A+2)/B$ and $d = (A-2)/B$ and is given by the map

$$(r,s) \quad \mapsto \quad (u,v) = (r/s, (r-1)/(r+1)). \tag{17}$$

The exceptional points are given by $s=0$ and $r=-1$.

2.6 Weierstrass form Elliptic Curve

The Weierstrass form elliptic curve $E_{W,\mathtt{a},\mathtt{b}}$ in affine coordinates $(\mathtt{x}, \mathtt{y})$ is given by an equation

$$E_{W,\mathtt{a},\mathtt{b}} : \mathtt{y}^2 \quad = \quad \mathtt{x}^3 + \mathtt{a}\mathtt{x} + \mathtt{b} \tag{18}$$

where $4\mathtt{a}^3 + 27^2 \neq 0$.

Proposition 1 in [20] shows that $E_{W,\mathtt{a},\mathtt{b}}$ can be converted into a Montgomery form if and only if the following two conditions hold.

$$\left.\begin{array}{l} 1.\ \text{There is an } \alpha \in \mathbb{F}_p \text{ such that } \alpha^3 + \mathtt{a}\alpha + \mathtt{b} = 0. \\ 2.\ \text{For this } \alpha, \text{ there is a } \mathtt{c} \in \mathbb{F}_p \text{ such that } \mathtt{c}^2 = (3\alpha^2 + \mathtt{a})^{-1}. \end{array}\right\} \tag{19}$$

Suppose that (19) holds. Then the map

$$(\mathtt{x}, \mathtt{y}) \quad \mapsto \quad (r, s) = (\mathtt{c}(\mathtt{x} - \alpha), \mathtt{cy}) \tag{20}$$

is an isomorphism from $E_{W,\mathtt{a},\mathtt{b}} : \mathtt{y}^2 = \mathtt{x}^3 + \mathtt{ax} + \mathtt{b}$ to $E_{M,A,B} : Bs^2 = r^3 + Ar^2 + r$ where $A = 3\alpha\mathtt{c}$ and $B = \mathtt{c}$.

2.7 Notation

1. Upper-case bold face letters $\mathbf{P}, \mathbf{Q}, \mathbf{R}$ and $\mathbf{S}$ denote points of elliptic curves and upper case letters $\mathsf{P}, \mathsf{Q}, \mathsf{R}$ and S in sans serif font denote points of Kummer lines.
2. $[\mathsf{x}^2 : \mathsf{z}^2]$ denote points on the Kummer line.
3. (x, y) denotes affine Legendre coordinates; (X, Y, Z) denotes projective Legendre coordinates.
4. (u, v, t) denotes extended affine Edwards coordinates; (U, V, T, W) denotes extended twisted Edwards coordinates.
5. (r, s) denotes affine Montgomery coordinates.
6. $(\mathtt{x}, \mathtt{y})$ denotes affine Weierstrass coordinates.

$\mathcal{M}$, $\mathcal{S}$, $\mathcal{A}$ denote multiplication, squaring and addition respectively over $\mathbb{F}_p$; $\mathcal{C}$ denotes multiplication by a small constant over $\mathbb{F}_p$.

3 Moving Between E_μ and $\mathcal{K}_{a^2,b^2}$

Suppose $P = [\mathsf{x}^2 : \mathsf{z}^2]$ is a point of $\mathcal{K}_{\mathsf{a}^2,\mathsf{b}^2}$ which is not of order two and let $\widehat{\psi}(\mathsf{P}) = \mathbf{P} = (X : \cdot : Z)$ be the corresponding point of $E_{L,\mu}$. We wish to obtain formulas for X and Z in terms of x^2 and z^2. Note that the y-coordinate of $\mathbf{P}$ is not uniquely obtained from P. Conversely, suppose we are given $\mathbf{P} = (X : \cdot : Z) \in E_{L,\mu}(\mathbb{F}_p)$ which is not of order two and we wish to obtain the coordinates x^2 and z^2 of the corresponding point $\widehat{\psi}^{-1}(\mathbf{P}) =$

Table 4: Conversions from Kummer line to Legendre form elliptic curves and vice versa. Here $\alpha_0 = \mathsf{a}^4\mathsf{b}^2$ and $\alpha_1 = \mathsf{a}^2\mathsf{b}^4$ are precomputed quantities.

KL to Legendre	Legendre to KL
$\widehat{\psi}([\mathsf{x}^2 : \mathsf{z}^2])$	
$X = \alpha_0\mathsf{z}^2;$	$\widehat{\psi}^{-1}(X : \cdot : Z)$
$t_1 = \alpha_1\mathsf{x}^2;$	$\mathsf{x}^2 = \alpha_0(X - Z);$
$t_2 = \alpha_0\mathsf{z}^2;$	$\mathsf{z}^2 = \alpha_1 X;$
$Z = t_2 - t_1;$	return $[\mathsf{x}^2 : \mathsf{z}^2]$.
return $(X : \cdot : Z)$.	

$\mathsf{P} = [\mathsf{x}^2 : \mathsf{z}^2]$. These tasks are done as follows.

$$\begin{aligned}
\widehat{\psi}(\mathsf{P}) &= \widehat{\psi}([\mathsf{x}^2 : \mathsf{z}^2]) \\
&= \psi([\mathsf{x}^2 : \mathsf{z}^2]) + \mathbf{T} \\
&= \left(\mathsf{a}^2\mathsf{x}^2 : \cdot : \mathsf{a}^2\mathsf{x}^2 - \mathsf{b}^2\mathsf{z}^2\right) + (\mu : 0 : 1) \\
&= \left(\mu\mathsf{b}^2\mathsf{z}^2 : \cdot : (1-\mu)\mathsf{a}^2\mathsf{x}^2 + \mu\mathsf{b}^2\mathsf{z}^2\right) \\
&= \left(\mathsf{a}^4\mathsf{b}^2\mathsf{z}^2 : \cdot : -\mathsf{a}^2\mathsf{b}^4\mathsf{x}^2 + \mathsf{a}^4\mathsf{b}^2\mathsf{z}^2\right) \\
&= (X : \cdot : Z). \qquad (21) \\
\widehat{\psi}^{-1}(\mathbf{P}) &= \widehat{\psi}^{-1}(X : \cdot : Z) \\
&= \psi^{-1}((X : \cdot : Z) + \mathbf{T}) \\
&= \psi^{-1}((X : \cdot : Z) + (\mu : 0 : 1)) \\
&= \psi^{-1}(\mu(X-1) : 0 : X - \mu) \\
&= [\mathsf{b}^2\mu(X - Z) : \mathsf{a}^2 X(\mu - 1)) \\
&= [\mathsf{b}^2\mathsf{a}^4(X - Z) : \mathsf{a}^2\mathsf{b}^4 X] \\
&= [\mathsf{x}^2 : \mathsf{z}^2]. \qquad (22)
\end{aligned}$$

Explicit formulas to compute the expressions given by (21) and (22) are shown in Table 4. We note that the expressions given by (21) and (22) and the formulas appearing in Table 4 do not appear in [15]. Since a^2 and b^2 are small constants, the pre-computed constants α_0 and α_1 are also not too large. The conversion from Kummer line to Legendre form elliptic curve requires three multiplications by small constants while the conversion from Legendre form elliptic curve to Kummer line requires two such multiplications.

Using $\widehat{\Psi}$, it is possible to map the KL base points provided in Table 3 to base points on the corresponding Legendre form curves. These are shown in affine coordinates in Table 5. For the Legendre form curves, the y-coordinate is the positive square root of $x(x-1)(x-\mu)$ where $x = \mathsf{a}^4\mathsf{b}^2\mathsf{z}^2/(-\mathsf{a}^2\mathsf{b}^4\mathsf{x}^2 + \mathsf{a}^4\mathsf{b}^2\mathsf{z}^2)$ for the values of $\mathsf{a}^2, \mathsf{b}^2, \mathsf{x}^2$ and z^2 shown in Table 5. These values are as follows.

$$\begin{aligned}
\mathfrak{y}_1 &= 660779751606431880601449706469571005138317100501546769210310679914171628271, \\
\mathfrak{y}_2 &= 101362230726483345709451684337581328099144030152437758469769413717077964179 1, \\
\mathfrak{y}_3 &= 425557773815612033904467816145303465807318937689947195035416526424296504856 45, \\
\mathfrak{y}_4 &= 813434244188840759342018993082302069527012389780799905356481715722502287370105 12.
\end{aligned}$$

Table 5: Base points for E_{1a}, E_{1b}, E_2 and E_3 corresponding to KL_{1a}, KL_{1b}, KL_2 and KL_3.

p	a^2	b^2	$[\mathsf{x}^2 : \mathsf{z}^2]$	(x, y)
$2^{251} - 9$	81	20	$[64 : 1]$	$(-131220/1942380, \mathfrak{y}_1)$
$2^{251} - 9$	186	175	$[19 : 1]$	$(-6054300/102174450, \mathfrak{y}_2)$
$2^{255} - 19$	82	77	$[31 : 1]$	$(-504300/13794450, \mathfrak{y}_3)$
$2^{266} - 3$	260	139	$[2 : 1]$	$(-9396400/650520, \mathfrak{y}_4)$

3.1 Scalar Multiplication on E_μ via $\mathcal{K}_{a^2,b^2}$

The main purpose of using Kummer lines is to be able to perform fast scalar multiplication. Suppose $\mathbf{P} = (X_P : Y_P : Z_P)$ is a point on $E_{L,\mu}$ and n is a positive integer. The requirement is to obtain $\mathbf{Q} = n\mathbf{P}$. Using the associated Kummer line $\mathcal{K}_{\mathsf{a}^2,\mathsf{b}^2}$, this is achieved in the following manner.

Set $\mathsf{P} = \widehat{\psi}^{-1}(\mathbf{P})$ and compute $(\mathsf{Q}, \mathsf{R}) = \mathsf{scalarMult}(\mathsf{P}, n)$. Then $\mathsf{Q} = n\mathsf{P}$ and $\mathsf{R} = (n+1)\mathsf{P}$. Set $\mathbf{Q} = \widehat{\psi}(\mathsf{Q})$ and $\mathbf{R} = \widehat{\psi}(\mathsf{R})$. By the consistency of scalar multiplication between $\mathcal{K}_{\mathsf{a}^2,\mathsf{b}^2}$ and $E_{L,\mu}$, it follows that $\mathbf{Q} = n\mathbf{P}$ and $\mathbf{R} = (n+1)\mathbf{P}$. Let $\mathbf{Q} = (X_Q : Y_Q : Z_Q)$ and $\mathbf{R} = (X_R : Y_R : Z_R)$.

The problem with the above approach is that $\mathbf{Q} = \widehat{\psi}(\mathsf{Q})$ does not recover Y_Q. On the other hand, since $\mathbf{Q} - \mathbf{R} = -\mathbf{P}$, the value of Y_Q can be recovered from X_P ,Y_P, Z_P, X_Q, Z_Q, X_R and Z_R. The method for doing this has been mentioned in [15] in the context of affine coordinates. Here we solve a more general problem in projective coordinates.

Given $\mathsf{Q} = (\mathsf{x}_\mathsf{Q}^2 : \mathsf{z}_\mathsf{Q}^2)$, $\mathsf{R} = (\mathsf{x}_\mathsf{R}^2 : \mathsf{z}_\mathsf{R}^2)$ and $\mathbf{P} = (X_P : Y_P : Z_P)$, we provide formulas for determining X_Q, Y_Q and Z_Q. We assume that $\mathbf{P}$ is not the identity nor a point of order two, so that $Z_P \neq 0$ and $Y_P \neq 0$. Let

$$\begin{aligned} \gamma_\mathsf{Q} &= \mu\mathsf{b}^2\mathsf{z}_\mathsf{Q}^2, \qquad \delta_\mathsf{Q} = (1-\mu)\mathsf{a}^2\mathsf{x}_\mathsf{Q}^2 + \mu\mathsf{b}^2\mathsf{z}_\mathsf{Q}^2; \\ \gamma_\mathsf{R} &= \mu\mathsf{b}^2\mathsf{z}_\mathsf{R}^2, \qquad \delta_\mathsf{R} = (1-\mu)\mathsf{a}^2\mathsf{x}_\mathsf{R}^2 + \mu\mathsf{b}^2\mathsf{z}_\mathsf{R}^2. \end{aligned}$$

Then

$$\widehat{\psi}(Q) = \widehat{\psi}([\mathsf{x}_\mathsf{Q}^2 : \mathsf{z}_\mathsf{Q}^2]) = (\gamma_\mathsf{Q} : \cdot : \delta_\mathsf{Q}) = \mathbf{Q} \quad \text{and} \quad \widehat{\psi}(R) = \widehat{\psi}([\mathsf{x}_\mathsf{R}^2 : \mathsf{z}_\mathsf{R}^2]) = (\gamma_\mathsf{R} : \cdot : \delta_\mathsf{R}) = \mathbf{R}.$$

For simplicity of the ensuing calculation, we shift to affine coordinates. $\mathbf{P}$ in affine coordinates is (x_P, y_P) where $x_P = X_P/Z_P$ and $y_P = Y_P/Z_P$. Let $x_Q = \gamma_\mathsf{Q}/\delta_\mathsf{Q}$ and $x_R = \gamma_\mathsf{R}/\delta_\mathsf{R}$ and so $\mathbf{Q}$ and $\mathbf{R}$ in affine coordinates are (x_Q, y_Q) (with y_Q unknown) and $(x_R, \cdot)$ respectively.

Since $\mathsf{Q} = n\mathsf{P}$ and $\mathsf{R} = (n+1)\mathsf{P}$, $\mathsf{Q} \neq \mathsf{R}$ and so $\mathbf{Q} \neq \mathbf{R}$ implying that $x_Q \neq x_R$. Further, $\mathbf{Q} = n\mathbf{P}$ and $\mathbf{R} = (n+1)\mathbf{P}$ and so $\mathbf{Q} - \mathbf{R} = -\mathbf{P}$. Let $y = mx + c$ be the line passing through $\mathbf{Q}$ and $-\mathbf{R}$. This line also passes through $\mathbf{P}$ and so we have $m = (y_Q - y_P)/(x_Q - x_P)$. Plugging the equation $y = mx + c$ into the affine form of the curve $y^2 = x^3 - (\mu+1)x^2 + \mu x$ and simplifying we have $x^3 - (\mu + 1 + m^2)x^2 + (\mu - 2mc)x - c^2 = 0$. Since x_P, x_Q and x_R are the three roots of this equation, we have $x_P + x_Q + x_R = \mu + 1 + m^2$. Substituting the expression for m and using $y_Q^2 = x_Q(x_Q - 1)(x_Q - \mu)$ we obtain

$$y_Q = -\frac{1}{2y_P}\left((x_Q - x_P)^2 (x_P + x_Q + x_R - \mu - 1) - x_Q(x_Q - 1)(x_Q - \mu) - y_P^2\right).$$

Substituting $x_Q = \gamma_{\mathsf{Q}}/\delta_{\mathsf{Q}}$, $x_R = \gamma_{\mathsf{R}}/\delta_{\mathsf{R}}$, $x_P = X_P/Z_P$ and $y_P = Y_P/Z_P$, yields

$$\begin{aligned} & y_Q \\ = & -\frac{Z_P}{2Y_P}\left(\left(\frac{\gamma_{\mathsf{Q}}}{\delta_{\mathsf{Q}}} - \frac{X_P}{Z_P}\right)^2\left(\frac{X_P}{Z_P} + \frac{\gamma_{\mathsf{Q}}}{\delta_{\mathsf{Q}}} + \frac{\gamma_{\mathsf{R}}}{\delta_{\mathsf{R}}} - \mu - 1\right) - \frac{\gamma_{\mathsf{Q}}}{\delta_{\mathsf{Q}}}\left(\frac{\gamma_{\mathsf{Q}}}{\delta_{\mathsf{Q}}} - 1\right)\left(\frac{\gamma_{\mathsf{Q}}}{\delta_{\mathsf{Q}}} - \mu\right) - \frac{Y_P^2}{Z_P^2}\right) \\ = & \cdots \\ = & \frac{-1}{2Y_P\delta_{\mathsf{Q}}^3\delta_{\mathsf{R}}Z_P^2}\left((Z_P\gamma_{\mathsf{Q}} - X_P\delta_{\mathsf{Q}})^2(X_P\delta_{\mathsf{Q}}\delta_{\mathsf{R}} + Z_P\gamma_{\mathsf{Q}}\delta_{\mathsf{R}} + Z_P\delta_{\mathsf{Q}}\gamma_{\mathsf{R}} - (\mu+1)Z_P\delta_{\mathsf{Q}}\delta_{\mathsf{R}})\right. \\ & \left. -Z_P^3\delta_{\mathsf{R}}\gamma_{\mathsf{Q}}(\gamma_{\mathsf{Q}} - \delta_{\mathsf{Q}})(\gamma_{\mathsf{Q}} - \mu\delta_{\mathsf{Q}}) - Y_P^2\delta_{\mathsf{Q}}^3\delta_{\mathsf{R}}Z_P\right). \end{aligned}$$

Converting back to projective coordinates, using $\mu = \mathsf{a}^4/(\mathsf{a}^4 - \mathsf{b}^4)$ and defining pre-computed constants $\beta_0 = 2\mathsf{a}^4 - \mathsf{b}^4$ and $\beta_1 = \mathsf{a}^4 - \mathsf{b}^4$ we have

$$\mathbf{Q} = [x_Q : y_Q : 1] = (X_Q : Y_Q : Z_Q)$$

where

$$\left.\begin{aligned} X_Q &= 2\gamma_{\mathsf{Q}}Y_P\delta_{\mathsf{Q}}^2\delta_{\mathsf{R}}Z_P^2\beta_1, \\ Y_Q &= -\left((Z_P\gamma_{\mathsf{Q}} - X_P\delta_{\mathsf{Q}})^2(\beta_1(X_P\delta_{\mathsf{Q}}\delta_{\mathsf{R}} + Z_P\gamma_{\mathsf{Q}}\delta_{\mathsf{R}} + Z_P\delta_{\mathsf{Q}}\gamma_{\mathsf{R}}) - \beta_0 Z_P\delta_{\mathsf{Q}}\delta_{\mathsf{R}})\right. \\ &\qquad \left. -Z_P^3\delta_R\gamma_{\mathsf{Q}}(\gamma_{\mathsf{Q}} - \delta_{\mathsf{Q}})(\beta_1\gamma_{\mathsf{Q}} - a^4\delta_{\mathsf{Q}}) - Y_P^2\delta_{\mathsf{Q}}^3\delta_{\mathsf{R}}Z_P\beta_1\right), \\ Z_Q &= 2Y_P\delta_{\mathsf{Q}}^3\delta_{\mathsf{R}}Z_P^2\beta_1. \end{aligned}\right\} \tag{23}$$

The computations of X_Q, Y_Q and Z_Q are shown in Algorithm 1. The total cost is $4\mathcal{C} + 26\mathcal{M} + 4\mathcal{S} + 10\mathcal{A}$.

4 Moving From Legendre to Twisted Edwards Form Elliptic Curves

The general idea is to move from the Legendre form to the Montgomery form and then use (17) to move to the twisted Edwards form. Further, we wish to move to $E_{E,-1,d}$ for some d. For this, we use either (14) directly or (15) followed by (14) whenever these are feasible to be applied. For moving from the Legendre to the Montgomery form we identify three approaches.

1. If the curve has a point of order 4, then the method given in [4] can be simplified to move from the Legendre form to the Montgomery form. This provides a birational equivalence between the two forms.

2. It is possible to move from the Legendre form to the Weierstrass form. Then using (20) it is possible to move to the Montgomery form, if feasible. This also provides a birational equivalence between the two forms.

3. Based on the method provided in [5], it is possible to obtain a 2-isogeny for moving from the Legendre form to the Montgomery form.

For the first two methods, a birational equivalence is obtained between the Legendre form curve and the twisted Edwards curve. Since birational equivalence preserves the difficulty of discrete log computation, one can simply work over the obtained twisted Edwards curve without referring to the Legendre curve in the background. On the other hand, in the case of the third method, an isogeny is obtained. In this case, it is required to start from the Legendre form curve, move to the twisted Edwards form curve using the isogeny, perform the scalar multiplication and then move back to the Legendre form curve using the dual isogeny. This idea was introduced in [7] and we provide more details later.

Algorithm 1 Compute $\mathbf{Q} = (X_Q : Y_Q : Z_Q)$ from $\mathbf{P} = (X_P, Y_P, Z_P)$, $\mathsf{Q} = [\mathsf{x}_\mathsf{Q}^2 : \mathsf{z}_\mathsf{Q}^2]$ and $\mathsf{R} = [\mathsf{x}_\mathsf{R}^2 : \mathsf{z}_\mathsf{R}^2]$ where $\mathbf{Q} = n\mathbf{P}$, $\mathsf{Q} = n\mathsf{P}$, $\mathsf{R} = (n+1)\mathsf{P}$ and $\mathsf{P} = \widehat{\psi}^{-1}(\mathbf{P})$. Here $\beta_0 = 2\mathsf{a}^4 - \mathsf{b}^4$, $\beta_1 = \mathsf{a}^4 - \mathsf{b}^4$, $\beta_2 = \mu\mathsf{b}^2$ and $\beta_3 = (1-\mu)\mathsf{a}^2$. A multiplication by μ is counted as a general multiplication over $\mathbb{F}_p$.

Input: $\mathbf{P} = (X_P : Y_P : Z_P), \mathsf{Q} = [\mathsf{x}_\mathsf{Q}^2 : \mathsf{z}_\mathsf{Q}^2], \mathsf{R} = [\mathsf{x}_\mathsf{R}^2 : \mathsf{z}_\mathsf{R}^2]$.
Output: $\mathbf{Q} = (X_Q : Y_Q : Z_Q)$.
$\gamma_\mathsf{Q} = \beta_2\mathsf{z}_\mathsf{Q}^2$; $\delta_\mathsf{Q} = \gamma_\mathsf{Q} + \beta_3\mathsf{x}_\mathsf{Q}^2$; $/* 2\mathcal{M} + 1\mathcal{A} */$
$\gamma_\mathsf{R} = \beta_2\mathsf{z}_\mathsf{R}^2$; $\delta_\mathsf{R} = \gamma_\mathsf{R} + \beta_3\mathsf{x}_\mathsf{R}^2$; $/* 2\mathcal{M} + 1\mathcal{A} */$
$t_1 \leftarrow \gamma_\mathsf{Q} \cdot Z_P$; $t_2 \leftarrow X_P \cdot \delta_\mathsf{Q}$; $/* 2\mathcal{M} */$
$t_3 \leftarrow t_1 - t_2$; $t_3 \leftarrow t_3^2$; $/* 1\mathcal{A} + 1\mathcal{S} */$
$t_4 \leftarrow t_1 + t_2$; $t_4 \leftarrow t_4 \cdot \delta_\mathsf{R}$; $/* 1\mathcal{A} + 1\mathcal{M} */$
$t_5 \leftarrow Z_P \cdot \delta_\mathsf{Q}$; $t_6 \leftarrow t_5 \cdot \gamma_\mathsf{R}$; $/* 2\mathcal{M} */$
$t_6 \leftarrow t_4 + t_6$; $t_7 \leftarrow t_5 \cdot \delta_\mathsf{R}$; $/* 1\mathcal{A} + 1\mathcal{M} */$
$t_8 \leftarrow \beta_0 \cdot t_7$; $t_6 \leftarrow \beta_1 \cdot t_6$; $/* 2\mathcal{C} */$
$t_6 \leftarrow t_6 - t_8$; $t_3 \leftarrow t_3 \cdot t_6$; $/* 1\mathcal{A} + 1\mathcal{M} */$
$t_9 \leftarrow Z_P^2$; $t_{10} \leftarrow Z_P \cdot \delta_\mathsf{R}$; $/* 1\mathcal{S} + 1\mathcal{M} */$
$t_{11} \leftarrow t_9 \cdot t_{10}$; $t_{12} \leftarrow t_{11} \cdot \gamma_\mathsf{Q}$; $/* 2\mathcal{M} */$
$t_{13} \leftarrow \gamma_\mathsf{Q} - \delta_\mathsf{Q}$; $t_{14} \leftarrow \delta_\mathsf{Q} \cdot a^4$; $/* 1\mathcal{A} + 1\mathcal{C} */$
$t_6 \leftarrow \beta_1 \cdot \gamma_\mathsf{Q}$; $t_{14} \leftarrow t_6 - t_{14}$; $/* 1\mathcal{A} + 1\mathcal{M} */$
$t_{12} \leftarrow t_{12} \cdot t_{13}$; $t_{12} \leftarrow t_{12} \cdot t_{14}$; $/* 2\mathcal{M} */$
$t_3 \leftarrow t_3 - t_{12}$; $t_{15} \leftarrow Y_P^2$; $/* 1\mathcal{A} + 1\mathcal{S} */$
$t_{16} \leftarrow t_{15} \cdot \delta_\mathsf{Q}^2$; $t_{17} \leftarrow t_{16} \cdot \delta_\mathsf{Q}$; $/* 2\mathcal{M} + 1\mathcal{S} */$
$t_{18} \leftarrow t_{10} \cdot t_{17}$; $t_{18} \leftarrow t_{18} \cdot \beta_1$; $/* 2\mathcal{M} */$
$t_3 \leftarrow t_{18} - t_3$; $t_{19} \leftarrow t_{10} \cdot t_{16}$; $/* 1\mathcal{A} + 1\mathcal{M} */$
$t_{19} \leftarrow t_{19} \cdot Y_P$; $t_{19} \leftarrow 2\beta_1 \cdot t_{19}$; $/* 1\mathcal{M} + 1\mathcal{C} */$
$t_{20} \leftarrow t_1 \cdot t_{19}$; $t_5 \leftarrow t_5 \cdot t_{19}$; $/* 2\mathcal{M} */$
$t_5 \leftarrow t_5 \cdot Z_P$; $/* 1\mathcal{M} */$
$X_Q \leftarrow t_{20}$; $Y_Q \leftarrow t_3$; $Z_Q \leftarrow t_5$;
return $(X_Q : Y_Q : Z_Q)$.

4.1 Method 1: via a Point of Order 4

Proposition 1. *Let G be a finite cyclic group of order $2^i q$ with q odd and having three points of order two. Then G has a point of order four if and only if $i > 2$.*

Proof. If $i = 0$ or 1, then clearly G cannot have any point of order 4 as that would violate Lagrange's theorem. So, suppose $i \geq 2$. If $i = 2$, then by Sylow's theorem G has a unique subgroup of order 4. This subgroup consists of the three points of order 2 along with the identity. So, G does not have any point of order 4. If $i > 2$, then by Sylow's theorem consider the (unique) subgroup H of G of order 2^i. The order of any element of H is a power of 2. Since G has three elements of order 2 and the order of H is at least 8, H must have an element h whose order is 2^j for $j \geq 2$. The element $h^{2^{j-2}}$ is an element of order 4. □

From Table 3, the co-factors of E_{1a}, E_{1b}, E_2 and E_3 are 8, 8, 12 and 12 respectively. Using Proposition 1, E_{1a} and E_{1b} have points of order 4 while E_2 and E_3 do not. The next proposition shows how to find a point of order 4 in E_{1a} or E_{1b}.

Proposition 2. *Consider $E_{L,\mu} : y^2 = x(x-1)(x-\mu)$. The point (x_1, y_1) is of order 4 if and only if x_1 and y_1 are solutions of the equations*

$$\left.\begin{array}{rcl} x_1^3 - 3x_2x_1^2 + (2(\mu+1)x_2 - \mu)x_1 - \mu x_2 & = & 0 \\ 2y_1^2 - (3x_1^2 - 2(\mu+1)x_1 + \mu)(x_1 - x_2) & = & 0 \end{array}\right\} \tag{24}$$

for some $x_2 \in \{0, 1, \mu\}$ and $x_1 \neq x_2$.

Proof. The three points of order 2 on $E_{L,\mu}$ are $(0,0)$, $(1,0)$ and $(\mu,0)$. Since (x_1, y_1) is a point of order 4, $2(x_1, y_1)$ is a point of order 2 and so is equal to $(x_2, 0)$ for some $x_2 \in \{0, 1, \mu\}$.

Let m be the slope of the tangent to the curve passing through the point (x_1, y_1). This tangent also passes through the point $(x_2, 0)$. This gives two ways of obtaining m.

$$m = \frac{3x_1^2 - 2(\mu+1)x_1 + \mu}{2y_1} = \frac{y_1 - 0}{x_1 - x_2}.$$

This shows

$$\begin{aligned} 2y_1^2 &= (x_1 - x_2)(3x_1^2 - 2(\mu+1)x_1 + \mu) && (25) \\ &= 3x_1^3 - 2(\mu+1)x_1^2 + \mu x_1 - x_2(3x_1^2 - 2(\mu+1)x_1 + \mu). && (26) \end{aligned}$$

Since (x_1, y_1) is also on the curve, $y_1^2 = x_1^3 - (\mu+1)x_1^2 + \mu x_1$. Substituting in (26) and simplifying we obtain

$$x_1^3 - 3x_2x_1^2 + (2(\mu+1)x_2 - \mu)x_1 - \mu x_2 = 0. \tag{27}$$

Equations (25) and (27) show the desired result.

Conversely, suppose (24) holds and suppose that $2(x_1, y_1) = (x_2, y_2)$. We need to argue that $y_2 = 0$ which would imply that (x_2, y_2) is a point of order 2 and so (x_1, y_1) is a point of order 4. The slope of the tangent to the curve at the point (x_1, y_1) is $(3x_1^2 - 2(\mu+1)x_1 + \mu)/(2y_1)$ and this tangent also passes through the point (x_2, y_2). The line passing through (x_1, y_1) and (x_2, y_2) has slope $(y_1 - y_2)/(x_1 - x_2)$. So, $(3x_1^2 - 2(\mu+1)x_1 + \mu)/(2y_1) = (y_1 - y_2)/(x_1 - x_2)$. On the other hand, the second equation of (24) shows that $(3x_1^2 - 2(\mu+1)x_1 + \mu)/(2y_1) = y_1/(x_1 - x_2)$. Comparing the two expressions, we obtain $y_2 = 0$ as required. □

Proposition 2 shows a method to find a point of order 4 over $\mathbb{F}_p$. For each value of $x_2 = 0, 1, \mu$ try to solve (24) for x_1 and y_1 over $\mathbb{F}_p$. If a solution is found, then we have an $\mathbb{F}_p$ rational point of order 4 and if no solution is found, then there is no $\mathbb{F}_p$ rational point of order 4. Note that for Legendre form curves, this provides

Table 6: Values of x_1, y_1 and x_2 which are solutions to (24).

$x_2 = 0$	$x_1 = \sqrt{\mu}$	$y_1 = \pm\sqrt{-\mu^2 + 2\mu^{3/2} - \mu}$
	$x_1 = -\sqrt{\mu}$	$y_1 = \pm\sqrt{-\mu^2 - 2\mu^{3/2} - \mu}$
$x_2 = 1$	$x_1 = 1 + \sqrt{1-\mu}$	$y_1 = \pm(-1 + \mu - \sqrt{1-\mu})$
	$x_1 = 1 - \sqrt{1-\mu}$	$y_1 = \pm(-1 + \mu + \sqrt{1-\mu})$
$x_2 = \mu$	$x_1 = \mu + \sqrt{\mu^2 - \mu}$	$y_1 = \pm\left(2\mu^3 + 2\mu^2\sqrt{\mu^2-\mu} - 3\mu^2 - 2\mu\sqrt{\mu^2-\mu} + \mu\right)^{1/2}$
	$x_1 = \mu - \sqrt{\mu^2 - \mu}$	$y_1 = \pm\left(2\mu^3 - 2\mu^2\sqrt{\mu^2-\mu} - 3\mu^2 + 2\mu\sqrt{\mu^2-\mu} + \mu\right)^{1/2}$

a method different from Proposition 1 of determining whether there is an $\mathbb{F}_p$ rational point of order 4. The possible solutions for (x_1, y_1) arising from solving (24) are given in Table 6. These 12 solutions along with the 3 points of order 2 and the identity provide the 16 elements of the 4-torsion subgroup of $E_{L,\mu}$ in the algebraic closure of $\mathbb{F}_p$. Not all of the solutions in Table 6 are in $\mathbb{F}_p$.

For E_{1a}, there are no $\mathbb{F}_p$ rational points of order 4 corresponding to $x_2 = 0$ and $x_2 = 1$. For $x_2 = \mu$, the point

$$(\mu - \sqrt{\mu^2 - \mu}, \left(2\mu^3 - 2\mu^2\sqrt{\mu^2-\mu} - 3\mu^2 + 2\mu\sqrt{\mu^2-\mu} + \mu\right)^{1/2})$$

is an $\mathbb{F}_p$ rational point of order 4 such that $2(x_1, y_1) = (\mu, 0)$. The actual values of x_1 and y_1 are as follows.

$$\begin{aligned} x_1 &= 322440842554407722404745935977163109739922605813974342931657876259659086249 1; \\ y_1 &= 313869923061754536882167092899891687342788246781360046334350333184335107154 0. \end{aligned}$$

For E_{1b}, there are no $\mathbb{F}_p$ rational points of order 4 corresponding to $x_2 = 0$. For $x_2 = 1$, the point

$$(1 + \sqrt{1-\mu}, -1 + \mu - \sqrt{1-\mu})$$

is an $\mathbb{F}_p$ rational point of order 4 such that $2(x_1, y_1) = (1, 0)$. The actual values of x_1 and y_1 are as follows.

$$\begin{aligned} x_1 &= 292714878655320361755150718408976090298214976818868567324303337830906191617 3; \\ y_1 &= 149050458021924755511809851442855137094643312701266044913869011129024282833 5. \end{aligned}$$

The work [4] proposed the use of Edwards form elliptic curve in cryptography. This work showed birational equivalence between (long) Weierstrass form curves satisfying certain properties and Edwards form curves. From the proof it is possible to pick out a birational equivalence between curves of the form $y^2 = x^3 + a_2x^2 + a_4x$ (satisfying certain properties) and Montgomery form curves. Since Legendre form curves can be written in this form, this should directly provide a birational equivalence between Legendre form curves and Montgomery form curves. However, the result as stated in [4] does not permit obtaining such a birational equivalence. This is because the result and the proof in [4] requires that there should be an element of order 4 and a unique element of order 2 for the birational equivalence to be possible. Since Legendre form curves have 3 elements of order 2, the result does not directly apply to Legendre form curves. A closer examination of the proof, on the other hand, reveals that the condition of having a unique element of order 2 is not really required; the condition of having an element of order 4 is sufficient. This was already observed in [8], but, the details of the resulting proof were not provided. Below we provide these details as well as certain details which were skipped in the proof provided in [4].

Lemma 1. *[4] Suppose the curve given by $E : y^2 = x^3 + a_2x^2 + a_4x$ has a point (x_1, y_1) of order 4 and let $2(x_1, y_1) = (x_2, 0)$. Let $\overline{E} : \overline{y}^2 = \overline{x}^3 + A_2\overline{x}^2 + A_4\overline{x}$ where $A_2 = a_2 + 3x_2$ and $A_4 = a_4 + 3x_2^2 + 2a_2x_2$. The map*

$$(x, y) \quad \mapsto \quad (\overline{x}, \overline{y}) = (x - x_2, y) \tag{28}$$

from E to $\overline{E}$ is an isomorphism. Further, the point $(\overline{x}_1, \overline{y}_1) = (x_1 - x_2, y_1)$ has order 4 in $\overline{E}$ and $2(\overline{x}_1, \overline{y}_1) = (0, 0)$.

Proof.

$$\begin{aligned}
\overline{y}^2 = y^2 &= x^3 + a_2x^2 + a_4x. \\
&= (\overline{x} + x_2)^3 + a_2(\overline{x} + x_2)^2 + a_4(\overline{x} + x_2) \\
&= \overline{x}^3 + (a_2 + 3x_2)\overline{x}^2 + (a_4 + 3x_2^2 + 2a_2x_2)\overline{x} + x_2^3 + a_2x_2^2 + a_2r_2 \\
&= \overline{x}^3 + A_2\overline{x}^2 + A_4\overline{x}.
\end{aligned}$$

The last equation follows from the definition of A_2 and A_4 and from the fact that $(x_2, 0)$ is on E. Using [21] we have that the map given by (28) is an isomorphism. So, it preserves the orders of points. Since (x_1, y_1) is mapped to $(x_1 - x_2, y_1)$ and $(x_2, 0)$ is mapped to $(0, 0)$, it follows that on $\overline{E}$, $(x_1 - x_2, y_1)$ is a point of order 4 and $2(x_1 - x_2, y_1) = (0, 0)$. □

Lemma 2. *Suppose the curve given by $\overline{E} : \overline{y}^2 = \overline{x}^3 + A_2\overline{x}^2 + A_4\overline{x}$ has a point $(\overline{x}_1, \overline{y}_1)$ of order 4 and $2(\overline{x}_1, \overline{y}_1) = (0, 0)$. Then $A_4 = \overline{x}_1^2$ and $A_2 = \overline{y}_1^2/\overline{x}_1^2 - 2\overline{x}_1$. Further, the map*

$$(\overline{x}, \overline{y}) \quad \mapsto \quad (r, s) = (\overline{x}/\overline{x}_1, 2\overline{y}/\overline{y}_1) \tag{29}$$

is a birational equivalence from $\overline{E}$ to $Bs^2 = r^3 + Ar^2 + r$ where $B = 1/(1 - \theta)$ and $A = 2(1 + \theta)/(1 - \theta)$ with $\theta = 1 - 4\overline{x_1}^3/\overline{y}_1^2$.

Proof. The proof is essentially similar to the proof of Theorem 2.1 of [4] with a small difference which we point out later. Since $(\overline{x}_1, \overline{y}_1)$ has order 4, $\overline{y}_1 \neq 0$ and so $\overline{x}_1 \neq 0$. The point $(\overline{x}_1, \overline{y}_1)$ is on $\overline{E}$ and so

$$\overline{y}^2 \quad = \quad \overline{x}^3 + A_2\overline{x}^2 + A_4\overline{x}. \tag{30}$$

Since $2(\overline{x}_1, \overline{y}_1) = (0, 0)$, the tangent to $\overline{E}$ at the point $(\overline{x}_1, \overline{y}_1)$ passes through the point $(0, 0)$. Following the proof of Proposition 2, the slope of the tangent can be expressed in two different ways. This yields

$$\begin{aligned}
&\frac{\overline{y}_1 - 0}{\overline{x}_1 - 0} = \frac{3\overline{x}_1^2 + 2A_2\overline{x}_1 + A_4}{2\overline{y}_1} \\
&\Rightarrow 2\overline{y}_1^2 = 3\overline{x}_1^3 + 2A_2\overline{x}_1^2 + A_4\overline{x}_1 \\
&\Rightarrow 2(\overline{x}_1^3 + A_2\overline{x}_1^2 + A_4\overline{x}_1) = 3\overline{x}_1^3 + 2A_2\overline{x}_1^2 + A_4\overline{x}_1 \quad \text{using (30)} \\
&\Rightarrow A_4 = \overline{x}_1^2 \quad \text{since } \overline{x}_1 \neq 0 \\
&\Rightarrow A_2 = \frac{\overline{y}_1^2}{\overline{x}_1^2} - 2\overline{x}_1 \quad \text{from (30).}
\end{aligned}$$

From (29), $\overline{x} = r\overline{x}_1$ and $\overline{y} = s\overline{y}_1/2$. Using $\overline{y}^2 = \overline{x}^3 + A_2\overline{x}^2 + A_4\overline{x}$; the expressions for A_2, A_4 and θ; and $\overline{y}_1^2 = 4\overline{x}_1^3/(1 - d)$ we compute as follows.

$$\begin{aligned}
\frac{s^2\overline{y}_1^2}{4} = \overline{y}^2 &= \overline{x}^3 + A_2\overline{x}^2 + A_4\overline{x} = r^3\overline{x}_1^3 + A_2r^2\overline{x}_1^2 + A_4r\overline{x}_1 \\
\frac{s^2\overline{x}_1^3}{1 - \theta} &= r^3\overline{x}_1^3 + \left(\frac{4}{1 - \theta} - 2\right)\overline{x}_1^3r^2 + \overline{x}_1^3r \\
Bs^2 &= r^3 + Ar^2 + r.
\end{aligned}$$

This shows the result. □

Remarks:

1. Note that $\overline{x}_1/(1-\theta) = \overline{y}_1^2/(4\overline{x}_1^2)$ which is a square. This was overlooked in the proof of Theorem 2.1 in [4] leading to some unnecessary complications.

2. We note that Theorem 3.3 of [5] shows that every elliptic curve having a point of order 4 is birationally equivalent to an Edwards curve and Theorem 3.4 of [5] shows that if $p \equiv 3 \bmod 4$, then every Montgomery curve is birationally equivalent to an Edwards curve. These results are not directly useful for us since we wish to move to a twisted Edwards curve of the form $E_{E,-1,d}$ while these result show how to move to an Edwards curve of the form $E_{E,1,d}$.

By putting together the different maps, we obtain the following result.

Theorem 3. *Let $E_{L,\mu} : y^2 = x(x-1)(x-\mu)$ have a point (x_1, y_1) of order 4 with $2(x_1, y_1) = (x_2, 0)$. Let $\theta = 1 - 4(x_1 - x_2)^3/y_1^2$ and suppose that both -1 and θ are non-squares in $\mathbb{F}_p$. Let $4\theta = -b^2$ for some $b \in \mathbb{F}_p$. Then $E_{L,\mu}$ is birationally equivalent to $E_{E,-1,d} : -u^2 + v^2 = 1 + du^2v^2$ where $d = -1/\theta$ and the birational equivalence is given by*

$$(x, y) \quad \mapsto \quad (u, v) = \left(\frac{b(x - x_2)y_1}{(x_1 - x_2)y}, \frac{x + x_1 - 2x_2}{x - x_1} \right) \tag{31}$$

with exceptional points given by $y(x - x_1) = 0$, corresponding to points of order 2 (for $y = 0$) or to a point of order 4 (for $x = x_1$). Further, the birational equivalence from $E_{E,-1,d} : -u^2 + v^2 = 1 + du^2v^2$ to $E_{L,\mu}$ is given by

$$(u, v) \quad \mapsto \quad (x, y) = \left(x_2 + (x_1 - x_2)\frac{v+1}{v-1}, \frac{by_1(v+1)}{2u(v-1)} \right) \tag{32}$$

with exceptional points given by $u(v - 1) = 0$, corresponding to the identity $(0, 1)$ or to the point of order 2 $(0, -1)$.

Proof. $E_{L,\mu}$ can be written as $y^2 = x^3 + a_2x^2 + a_4x$ where $a_2 = -(\mu + 1)$ and $a_4 = \mu$. The composition of (28) and (29) gives the map

$$(x, y) \quad \mapsto \quad (r, s) = \left(\frac{x - x_2}{x_1 - x_2}, \frac{y}{y_1} \right) \tag{33}$$

which is a birational equivalence from $E_{L,\mu}$ to $E_{M,A,B} : Bs^2 = r^3 + Ar^2 + r$ where $B = 1/(1 - \theta)$ and $A = 2(1 + \theta)/(1 - \theta)$. Composing (33) with (17) and (15) gives the map

$$(x, y) \quad \mapsto \quad (\overline{u}, \overline{v}) = \left(\frac{(x - x_2)y_1}{(x_1 - x_2)y}, \frac{x + x_1 - 2x_2}{x - x_1} \right) \tag{34}$$

which is a birational equivalence from $E_{L,\mu}$ to $E_{E,\overline{a},4} : \overline{a}\overline{u}^2 + \overline{v}^2 = 1 + 4\overline{u}^2\overline{v}^2$ where $\overline{a} = 4\theta$. Since both θ and -1 are non-squares in $\mathbb{F}_p$, $-a$ is a square and we can write $a = 4\theta = -b^2$ for some $b \in \mathbb{F}_p$. Composing (34) with (14) we obtain the map given by (31) which is a birational equivalence from $E_{L,\mu}$ to $E_{E,-1,d} : -u^2 + v^2 = 1 + du^2v^2$ where $d = -1/\theta$.

The converse birational equivalence is similarly obtained. □

4.2 Method 2: via short Weierstrass

This method moves from the Legendre form to the short Weierstrass form and then to the Montgomery form. The first step of the reduction is given by the following result.

Proposition 3. *Let $\mu \in \mathbb{F}_p \setminus \{0\}$ and $E_{L,\mu} : y^2 = x(x-1)(x-\mu)$ be in the Legendre form. Let $\omega = (\mu+1)/3$. Then the map*

$$(x, y) \quad \mapsto \quad (\mathtt{x}, \mathtt{y}) = (x - \omega, y) \tag{35}$$

is a birational equivalence from $E_{L,\mu}$ to $E_{W,\mathtt{a},\mathtt{b}} : \mathtt{y}^2 = \mathtt{x}^3 + \mathtt{a}\mathtt{x} + \mathtt{b}$ where $\mathtt{a} = \mu - 3\omega^2$ and $\mathtt{b} = \omega^3 + \omega(\mu - 2\omega^2)$.

Proof. The following computation shows the result.

$$\begin{aligned}
\mathtt{y}^2 = y^2 &= x^3 - (\mu+1)x^2 + \mu x \\
&= (\mathtt{x}+\omega)^3 - 3\omega(\mathtt{x}+\omega)^2 + \mu(\mathtt{x}+\omega) \\
&= \mathtt{x}^3 + 3\mathtt{x}^2\omega + 3\mathtt{x}\omega^2 + \omega^3 - 3\omega\mathtt{x}^2 - 6\mathtt{x}\omega^2 - 3\omega^3 + \mu\mathtt{x} + \mu\omega \\
&= \mathtt{x}^3 + \omega^3 + (\mu - 3\omega^2)\mathtt{x} + \omega(\mu - 2\omega^2) \\
&= \mathtt{x}^3 + \mathtt{a}\mathtt{x} + \mathtt{b}.
\end{aligned}$$

□

Theorem 4. *Let $\mu \in \mathbb{F}_p \setminus \{0\}$, $\omega = (\mu+1)/3$, $\mathtt{a} = \mu - 3\omega^2$ and $\mathtt{b} = \omega^3 + \omega(\mu - 2\omega^2)$. Suppose that $\alpha \in \{-\omega, 1-\omega, \mu-\omega\}$ is such that $\mathtt{c}^2 = (3\alpha^2 + \mathtt{a})^{-1}$ for some $\mathtt{c} \in \mathbb{F}_p$. Let $\mathfrak{a} = (3\alpha\mathtt{c} + 2)/\mathtt{c}$ and $\mathfrak{d} = (3\alpha\mathtt{c} - 2)/\mathtt{c}$.*

1. *Suppose that $\left(\frac{\mathfrak{a}}{p}\right) = \left(\frac{-1}{p}\right)$. Then the map*

$$(x, y) \quad \mapsto \quad (u, v) = \left(\frac{\mathfrak{b}(x - \omega - \alpha)}{y}, \frac{\mathtt{c}(x - \omega - \alpha) - 1}{\mathtt{c}(x - \omega - \alpha) + 1}\right) \tag{36}$$

is a birational equivalence from $E_{L,\mu} : y^2 = x(x-1)(x-\mu)$ to $E_{E,-1,d} : -u^2 + v^2 = 1 + du^2v^2$ where $\mathfrak{b}$ is such that $\mathfrak{a} = -\mathfrak{b}^2$ and $d = (2-3\alpha\mathtt{c})/(2+3\alpha\mathtt{c})$. The exceptional points of (36) are given by $y(\mathtt{c}(x-\omega-\alpha)+1) = 0$. The converse birational equivalence from $E_{E,-1,d} : -u^2 + v^2 = 1 + du^2v^2$ to $E_{L,\mu} : y^2 = x(x-1)(x-\mu)$ is given by

$$(u, v) \quad \mapsto \quad (x, y) = \left(\alpha + \omega + \frac{1+v}{\mathtt{c}(1-v)}, \frac{\mathfrak{b}}{\mathtt{c}u}\frac{1+v}{1-v}\right) \tag{37}$$

with the exceptional points given by $u(v-1) = 0$.

2. *Suppose that $\left(\frac{\mathfrak{a}}{p}\right) \neq \left(\frac{-1}{p}\right)$ and $\left(\frac{\mathfrak{d}}{p}\right) = \left(\frac{-1}{p}\right)$. Then the map*

$$(x, y) \quad \mapsto \quad (u, v) = \left(\frac{\mathfrak{b}(x - \omega - \alpha)}{y}, \frac{\mathtt{c}(x - \omega - \alpha) + 1}{\mathtt{c}(x - \omega - \alpha) - 1}\right) \tag{38}$$

is a birational equivalence from $E_{L,\mu} : y^2 = x(x-1)(x-\mu)$ to $E_{E,-1,d} : -u^2 + v^2 = 1 + du^2v^2$ where $\mathfrak{b}$ is such that $\mathfrak{d} = -\mathfrak{b}^2$ and $d = (2+3\alpha\mathtt{c})/(2-3\alpha\mathtt{c})$. The exceptional points of (38) are given by $y(\mathtt{c}(x-\omega-\alpha)+1) = 0$. The converse birational equivalence from $E_{E,-1,d} : -u^2 + v^2 = 1 + du^2v^2$ to $E_{L,\mu} : y^2 = x(x-1)(x-\mu)$ is given by

$$(u, v) \quad \mapsto \quad (x, y) = \left(\alpha + \omega + \frac{v+1}{\mathtt{c}(v-1)}, \frac{\mathfrak{b}}{\mathtt{c}u}\frac{v+1}{v-1}\right) \tag{39}$$

with the exceptional points given by $u(v-1) = 0$.

Proof. From Proposition 3, the map $(x, y) \mapsto (\mathtt{x}, \mathtt{y}) = (x - \omega, y)$ moves from $E_{L,\mu} : y^2 = x(x-1)(x-\mu)$ to $E_{W,\mathtt{a},\mathtt{b}} : \mathtt{y}^2 = \mathtt{x}^3 + \mathtt{a}\mathtt{x} + \mathtt{b}$. The conditions on α and $\mathtt{c}$ satisfy (19) for $\mathtt{a} = \mu - 3\omega^2$ and $\mathtt{b} = \omega(\mu - 2\omega^2)$. So, from (20) the map $(\mathtt{x}, \mathtt{y}) = (r, s) = (\mathtt{c}(\mathtt{x} - \alpha), \mathtt{c}\mathtt{y})$ is a birational equivalence from $E_{W,\mathtt{a},\mathtt{b}}$ to $E_{M,A,B} : Bs^2 = r^3 + Ar^2 + r$ where $A = 3\alpha\mathtt{c}$ and $B = \mathtt{c}$.

Suppose that $\left(\frac{\mathfrak{a}}{p}\right) = \left(\frac{-1}{p}\right)$. The map (17) given by $(r, s) \mapsto (\overline{u}, \overline{v}) = (r/s, (r-1)/(r+1))$ is a birational equivalence from $E_{M,A,B}$ to $E_{E,\overline{a},\overline{d}} : \overline{a}\,\overline{u}^2 + \overline{v}^2 = 1 + \overline{d}\overline{u}^2\overline{v}^2$ where $\overline{a} = (A+2)/B = \mathfrak{a}$ and $\overline{d} = (A-2)/B = \mathfrak{d}$. Using (14), the map $(\overline{u}, \overline{v}) \mapsto (u, v) = (\mathfrak{b}\overline{u}, \overline{v})$ is a birational equivalence from $E_{E,\overline{a},\overline{d}} : \overline{a}\,\overline{u}^2 + \overline{v}^2 = 1 + \overline{d}\overline{u}^2\overline{v}^2$ to $E_{E,-1,d}$. Composing all the above maps gives the map defined in the first point of the theorem statement.

Suppose that $\left(\frac{\mathfrak{a}}{p}\right) \neq \left(\frac{-1}{p}\right)$ and $\left(\frac{\mathfrak{d}}{p}\right) = \left(\frac{-1}{p}\right)$. As above, The map (17) given by $(r, s) \mapsto (\hat{u}, \hat{v}) = (r/s, (r-1)/(r+1))$ is a birational equivalence from $E_{M,A,B}$ to $E_{E,\hat{a},\hat{d}} : \hat{a}\hat{u}^2 + \hat{v}^2 = 1 + \hat{d}\hat{u}^2\hat{v}^2$ where $\hat{a} = (A+2)/B = \mathfrak{a}$ and $\hat{d} = (A-2)/B = \mathfrak{d}$. Using (15), the map $(\hat{u}, \hat{v}) \mapsto (\overline{u}, \overline{v}) = (\hat{u}, 1/\hat{v})$ is a birational equivalence from $E_{E,\hat{a},\hat{d}} : \hat{a}\hat{u}^2 + \hat{v}^2 = 1 + \hat{d}\hat{u}^2\hat{v}^2$ to $E_{E,\overline{a},\overline{d}} : \overline{a}\,\overline{u}^2 + \overline{v}^2 = 1 + \overline{d}\overline{u}^2\overline{v}^2$, where $\overline{a} = \hat{d} = \mathfrak{d}$ and $\overline{d} = \hat{a} = \mathfrak{a}$. Using (14), the map $(\overline{u}, \overline{v}) \mapsto (u, v) = (\mathfrak{b}\overline{u}, \overline{v})$ is a birational equivalence from $E_{E,\overline{a},\overline{d}} : \overline{a}\,\overline{u}^2 + \overline{v}^2 = 1 + \overline{d}\overline{u}^2\overline{v}^2$ to $E_{E,-1,d}$. Composing all the maps gives the map defined in the second point of the theorem statement.

□

4.3 Method 3: via a 2-Isogeny

The statement and proof of the following result is similar to Theorem 5.1 of [5]. We provide more details and more importantly, the final form of the twisted Edwards curve is also different.

Theorem 5. *Let $\mu \in \mathbb{F}_p \setminus \{0\}$ and $E_{L,\mu} : y^2 = x(x-1)(x-\mu)$ be a Legendre form curve.*

1. *If $p \equiv 3 \bmod 4$ and μ is a non-square in $\mathbb{F}_p$, then the map*

$$(x, y) \quad \mapsto \quad (u, v) = \left(\frac{\mathfrak{b}y}{\mu - x^2}, \frac{y^2 + x^2(1-\mu)}{y^2 - x^2(1-\mu)}\right) \tag{40}$$

is a 2-isogeny from $E_{L,\mu}$ to $E_{E,-1,d} : -u^2 + v^2 = 1 + du^2v^2$, where $\mathfrak{b}$ is such that $\mathfrak{b}^2 = -4\mu$ and $d = -1/\mu$. The dual 2-isogeny is given by the map

$$(u, v) \quad \mapsto \quad (x, y) = \left(\frac{-\mu}{u^2}, \frac{\mathfrak{b}(1-\mu)v}{2u(1-v^2)}\right). \tag{41}$$

2. *If $p \equiv 1 \bmod 4$ then the map*

$$(x, y) \quad \mapsto \quad (u, v) = \left(\frac{\mathfrak{b}y}{\mu - x^2}, \frac{y^2 - (1-\mu)x^2}{y^2 + (1-\mu)x^2}\right) \tag{42}$$

is a 2-isogeny from $E_{L,\mu}$ to $E_{E,-1,d} : -u^2 + v^2 = 1 + du^2v^2$, where $\mathfrak{b}$ is such that $\mathfrak{b}^2 = -4$ and $d = -\mu$. The dual 2-isogeny is given by the map

$$(u, v) \quad \mapsto \quad (x, y) = \left(\frac{-1}{u^2}, \frac{(1-\mu)\mathfrak{b}v}{2u(v^2-1)}\right). \tag{43}$$

Proof. Since $E_{L,\mu} : y^2 = x^3 - (\mu+1)x^2 + \mu x$, by Example 4.5 in Chapter III of [21], $E_{L,\mu}$ is 2-isogenous to the curve $\overline{E} : \overline{y}^2 = \overline{x}^3 + 2(\mu+1)\overline{x}^2 + (\mu-1)^2\overline{x}$ where the 2-isogeny is given by

$$(x, y) \quad \mapsto \quad (\overline{x}, \overline{y}) = \left(\frac{y^2}{x^2}, \frac{y(\mu - x^2)}{x^2}\right) \tag{44}$$

and the dual 2-isogeny from $\overline{E}$ to $E_{L,\mu}$ is given by

$$(\overline{x},\overline{y}) \quad \mapsto \quad (x,y) = \left(\frac{\overline{y}^2}{4\overline{x}^2}, \frac{\overline{y}((\mu-1)^2-\overline{x}^2)}{8\overline{x}^2}\right). \tag{45}$$

The map

$$(\overline{x},\overline{y}) \quad \mapsto \quad (r,s) = (\overline{x}/(1-\mu), \overline{y}/(1-\mu)) \tag{46}$$

is an isomorphism from $\overline{E}$ to $E_{M,A,B} : Bs^2 = r^3 + Ar^2 + r$, where $B = 1/(1-\mu)$ and $A = 2(1+\mu)/(1-\mu)$.

Suppose $p \equiv 3 \bmod 4$ and μ is a non-square in $\mathbb{F}_p$. In this case, -1 is a non-square in $\mathbb{F}_p$. Using (17), we obtain a birational equivalence from $E_{M,A,B}$ to $E_{E,4,4\mu} : 4\hat{u}^2 + \hat{v}^2 = 1 + 4\mu\hat{u}^2\hat{v}^2$. Using (15), there is a birational equivalence from $E_{E,4,4\mu}$ to $E_{E,4\mu,4} : 4\mu\overline{u}^2 + \overline{v}^2 = 1 + 4\overline{u}^2\overline{v}^2$. Since both -1 and μ are non-squares, using (14), there is a birational equivalence from $E_{E,4\mu,4}$ to $E_{E,-1,d} : -u^2+v^2 = 1+du^2v^2$ where $d = -1/\mu$. The intermediate maps for moving from $E_{L,\mu}$ to $E_{-1,d}$ are as follows:

$$\begin{aligned}
(x,y) &\mapsto (\overline{x},\overline{y}) = \left(\frac{y^2}{x^2}, \frac{y(\mu-x^2)}{x^2}\right)\\
(\overline{x},\overline{y}) &\mapsto (r,s) = \left(\frac{\overline{x}}{1-\mu}, \frac{\overline{y}}{1-\mu}\right)\\
(r,s) &\mapsto (\hat{u},\hat{v}) = \left(\frac{r}{s}, \frac{r-1}{r+1}\right)\\
(\hat{u},\hat{v}) &\mapsto (\overline{u},\overline{v}) = \left(\hat{u}, \frac{1}{\hat{v}}\right)\\
(\overline{u},\overline{v}) &\mapsto (u,v) = (\mathfrak{b}\overline{u},\overline{v}).
\end{aligned}$$

Composing these intermediate maps shows that the 2-isogeny from $E_{L,\mu}$ to $_{E,-1,d}$ is given by (40) and composing the maps in the opposite directions shows that the dual 2-isogeny is given by (41).

Suppose $p \equiv 1 \bmod 4$. In this case, -1 is a square in $\mathbb{F}_p$. Using (17), we obtain a birational equivalence from $E_{M,A,B}$ to $E_{E,4,4\mu} : 4\overline{u}^2 + \overline{v}^2 = 1 + 4\mu\overline{u}^2\overline{v}^2$. Since 4 and -1 are both square, using (14), there is a birational equivalence from $E_{E,4,4\mu}$ to $E_{E,-1,d} : -u^2 + v^2 = 1 + du^2v^2$ where $d = -\mu$. The intermediate maps for moving from $E_{L,\mu}$ to $E_{-1,d}$ are as follows:

$$\begin{aligned}
(x,y) &\mapsto (\overline{x},\overline{y}) = \left(\frac{y^2}{x^2}, \frac{y(\mu-x^2)}{x^2}\right)\\
(\overline{x},\overline{y}) &\mapsto (r,s) = \left(\frac{\overline{x}}{1-\mu}, \frac{\overline{y}}{1-\mu}\right)\\
(r,s) &\mapsto (\overline{u},\overline{v}) = \left(\frac{r}{s}, \frac{r-1}{r+1}\right)\\
(\overline{u},\overline{v}) &\mapsto (u,v) = (\mathfrak{b}\overline{u},\overline{v}).
\end{aligned}$$

Composing these intermediate maps shows that the 2-isogeny from $E_{L,\mu}$ to $_{E,-1,d}$ is given by (42) and composing the maps in the opposite directions shows that the dual 2-isogeny is given by (43). □

Corollary 1. *Suppose $E_{L,\mu}$ is given by projective coordinates $(X : Y : Z)$ and $E_{E,-1,d}$ is given by extended twisted Edwards coordinates $(U : V : T : W)$.*

1. *If $p \equiv 3 \bmod 4$ and μ is a non-square in $\mathbb{F}_p$, then the maps (40) and (41) are respectively*

$$\begin{aligned}(X:Y:Z) &\mapsto (U:V:T:W)\\ &= \big(\mathfrak{b}YZ(Y^2-X^2(1-\mu)) : (\mu Z^2-X^2)(Y^2+X^2(1-\mu))\\ &\qquad : UV : (\mu Z^2-X^2)(Y^2-X^2(1-\mu))\big) \qquad (47)\\ (U:V:T:W) &\mapsto (X:Y:Z)\\ &= \big(-2\mu W^2(W^2-V^2) : \mathfrak{b}(1-\mu)UVW^2\\ &\qquad : 2U^2(W^2-V^2)\big)\,. \qquad (48)\end{aligned}$$

2. *If $p \equiv 1 \bmod 4$, then the maps (42) and (43) are respectively*

$$\begin{aligned}(X:Y:Z) &\mapsto (U:V:T:W)\\ &= \big(\mathfrak{b}YZ(Y^2+X^2(1-\mu)) : (\mu Z^2-X^2)(Y^2-X^2(1-\mu))\\ &\qquad : UV : (\mu Z^2-X^2)(Y^2+X^2(1-\mu))\big) \qquad (49)\\ (U:V:T:W) &\mapsto (X:Y:Z)\\ &= \big(-2W^2(V^2-W^2) : \mathfrak{b}(1-\mu)UVW^2\\ &\qquad : 2U^2(V^2-W^2)\big)\,. \qquad (50)\end{aligned}$$

Remarks: In the extended twisted Edwards coordinates, the point $(0:1:0:1)$ is the identity and $(0:-1:0:1)$ is a point of order 2. In the projective coordinates for Legendre form, the identity is given by $(X:Y:0)$. The kernels of the isogenies given by (47), (48), (49) and (48) are as follows.

1. For the map (47), the kernel is obtained by setting the right hand side to $(0:1:0:1)$. This leads to the equations $YZ(Y^2-X^2(1-\mu))=0$, $(\mu Z^2-X^2)(Y^2+X^2(1-\mu))=1$ and $(\mu Z^2-X^2)(Y^2-X^2(1-\mu))=1$. From the first equation we have either $Z=0$ or $Y=0$ or $Y^2-X^2(1-\mu)=0$. The last condition contradicts the third equation. So, we have either $Z=0$ or $Y=0$. The point corresponding to $Z=0$ is the identity of the Legendre form curve. If $Z\neq 0$, then $Y=0$ which corresponds to a point of order 2. The points of order 2 are $(0:0:1)$, $(1:0:1)$ and $(\mu:0:1)$ and so $\mu Z^2-X^2\neq 0$. So, the last two equations lead to $Y^2+X^2(1-\mu)=Y^2-X^2(1-\mu)$ which combined with $Y=0$ leads to $X=0$. So, the two points in the kernel of (47) are the identity and the point $(0:0:1)$ of order 2.

2. For the map (41), the kernel is obtained by setting the last component of the right hand side to 0, i.e., $U^2(W^2-V^2)=0$. Suppose $U=0$, then from the projective form of the twisted Edwards curve, we have $W^2(V^2-W^2)=0$ which using $W\neq 0$ leads to $V=\pm W$. On the other hand, if $W^2-V^2=0$, then from the projective form of the twisted Edwards curve, we have $(1+d)U^2=0$ (using $W\neq 0$) and so $U=0$. So, the points in the kernel are given by $U=0$ and $V=\pm W$, i.e., the kernel consists of $\{(0:1:0:1),(0:-1:0:1)\}$. The first point is the identity of the twisted Edwards curve while the second point has order two.

3. A reasoning similar to the above shows that the kernel of (49) is the same as the kernel of (47) and the kernel of (50) is the same as the kernel of (48).

5 Concrete Twisted Edwards Curves

Theorems 3, 4 and 5 provide three ways of obtaining twisted Edwards curves from Legendre curves. In this section, we apply these methods to the Legendre curves arising from the Kummer lines mentioned in Section 2.3. In each case, the Edwards curve is of the form

$$E_{E,-1,d}: -u^2+v^2 \;=\; 1+du^2v^2. \qquad (51)$$

So, only the parameter d needs to be determined.

Case 1a: $E_{E,-1,d}$ arising from $E_{1a} = E_{L,\mu}$ arising from $\mathsf{KL2519}(81, 20)$. In this case $p = 2^{251} - 9$ and -1 is a non-square modulo p.

1. Consider the applicability of Theorem 3. This requires a point (x_1, y_1) of order 4 such that $2(x_1, y_1) = (x_2, y_2)$ where the possible values of x_1, y_1 and x_2 are given in Table 6. For the solutions of x_1, y_1 and x_2, it is required to determine whether the θ defined in Theorem 3 is a non-square. It turns out that for E_{1a} none of the solutions for x_1, y_1 and x_2 lead to a non-square θ. So, Theorem 3 does not lead to a desired twisted Edwards curve corresponding to E_{1a}.

2. Consider the applicability of Theorem 4. Recall that $\omega = (\mu+1)/3$, $\mathsf{a} = \mu - 3\omega^2$. The choices of $\alpha = 1-\omega$ and $\alpha = \mu-\omega$ do not lead to any solution. For $\alpha = -\omega$, $3\alpha^2+\mathsf{a}$ is a square; for both values of $\mathsf{c} = \pm\sqrt{3\alpha^2 + \mathsf{a}}$ the corresponding values of $\mathfrak{a}$ are non-squares. So, the first point of Theorem 4 applies giving the value of d to be $(2 - 3\alpha\mathsf{c})/(2 + 3\alpha\mathsf{c})$. This leads to two curves

$$\mathsf{Ed}_{1a,1} = E_{E,-1,d_1} \quad \text{and} \quad \mathsf{Ed}_{1a,2} = E_{E,-1,d_2} \tag{52}$$

where

$$\begin{aligned} d_1 &= 3004883614027606552641601849381600400091177755395884111215835704890098740623, \\ d_2 &= 2798833008714001129854195114850728831341938757267269034499352388556522149990. \end{aligned}$$

In the case of both $\mathsf{Ed}_{1a,1}$ and $\mathsf{Ed}_{1a,2}$, the exceptional points of (36) are given by $y = 0$ (corresponding to points of order two) and $x = \omega + \alpha - 1/\mathsf{c}$. For $\mathsf{Ed}_{1a,1}$, the value of $\omega + \alpha - 1/\mathsf{c}$ turns out to be $-\sqrt{\mu}$, while for $\mathsf{Ed}_{1a,2}$ the value of $\omega + \alpha - 1/\mathsf{c}$ turns out to be $\sqrt{\mu}$. From Table 6, these correspond to points of order 4. Further, the value of y corresponding to $x = \pm\sqrt{\mu}$ is not in $\mathbb{F}_p$. So, these order 4 points are not $\mathbb{F}_p$ rational.

The base point on $\mathsf{Ed}_{1a,1}$ corresponding to the point (x, y) on E_{1a} given in Table 5 is obtained by applying the map in (36) to (x, y). Denoting this point by $(u_{1a,1}, v_{1a,1})$, we have

$$\begin{aligned} u_{1a,1} &= 1026186610340456335262042546425133890128511340615658182636627624447632685128, \\ v_{1a,1} &= 2573882201554647992450201823427996983816049720177813746127591622922737044734. \end{aligned} \tag{53}$$

The base point on $\mathsf{Ed}_{1a,2}$ corresponding to the point (x, y) on E_{1a} given in Table 5 is obtained by applying the map in (36) to (x, y). Denoting this point by $(u_{1a,2}, v_{1a,2})$, we have

$$\begin{aligned} u_{1a,2} &= 3125143484386555645888388262718991870990762888878900211242226932085406844324, \\ v_{1a,2} &= 3574659419552526316819005233288272389020277530794054549274165519298432508101. \end{aligned} \tag{54}$$

3. In this case, $p \equiv 3 \bmod 4$ and μ is a square. So, Theorem 5 does not apply.

Case 1b: $E_{E,-1,d}$ arising from $E_{1b} = E_{L,\mu}$ arising from $\mathsf{KL2519}(186, 175)$. In this case $p = 2^{251} - 9$ and -1 is a non-square modulo p.

1. Consider the applicability of Theorem 3. This requires a point (x_1, y_1) of order 4 such that $2(x_1, y_1) = (x_2, y_2)$ where the possible values of x_1, y_1 and x_2 are given in Table 6. For the solutions of x_1, y_1 and x_2, it is required to determine whether the θ defined in Theorem 3 is a non-square. It turns out that for E_{1a} none of the solutions for x_1, y_1 and x_2 lead to a non-square θ. So, Theorem 3 does not lead to a desired twisted Edwards curve corresponding to E_{1b}.

2. Consider the applicability of Theorem 4. Recall that $\omega = (\mu+1)/3$, $\mathsf{a} = \mu - 3\omega^2$.
The choices $\alpha = -\omega$ and $\alpha = 1-\omega$ do not lead to any solution. For $\alpha = \mu - \omega$, $3\alpha^2 + \mathsf{a}$ is a square; for both values of $\mathsf{c} = \pm\sqrt{3\alpha^2+\mathsf{a}}$ the corresponding values of $\mathfrak{a}$ are non-squares. So, the first point of Theorem 4 applies giving the value of d to be $(2-3\alpha\mathsf{c})/(2+3\alpha\mathsf{c})$. This leads to two curves

$$\mathsf{Ed}_{1b,1} = E_{E,-1,d_1} \quad \text{and} \quad \mathsf{Ed}_{1b,2} = E_{E,-1,d_2} \tag{55}$$

where

$$\begin{aligned} d_1 &= 2007542825992269943426958567234500079037320930456129494954013128865487694617, \\ d_2 &= 3588597806941617626763563584979997144212912747902083596264181322559291197 07. \end{aligned}$$

In the case of both $\mathsf{Ed}_{1b,1}$ and $\mathsf{Ed}_{1b,2}$, the exceptional points of (36) are given by $y = 0$ (corresponding to points of order two) and $x = \omega + \alpha - 1/\mathsf{c}$. For $\mathsf{Ed}_{1b,1}$, the value of $\omega+\alpha-1/\mathsf{c}$ turns out to be $\mu - \sqrt{\mu^2-\mu}$, while for $\mathsf{Ed}_{1b,2}$ the value of $\omega+\alpha-1/\mathsf{c}$ turns out to be $\mu + \sqrt{\mu^2-\mu}$. From Table 6, these correspond to points of order 4. Further, the value of y corresponding to $x = \mu \pm \sqrt{\mu^2-\mu}$ is not in $\mathbb{F}_p$. So, these order 4 points are not $\mathbb{F}_p$ rational.

The base point on $\mathsf{Ed}_{1b,1}$ corresponding to the point (x,y) on E_{1b} given in Table 5 is obtained by applying the map in (36) to (x,y). Denoting this point by $(u_{1b,1}, v_{1a,1})$, we have

$$\begin{aligned} u_{1b,1} &= 359517623373432742494344986407396355702513837587773586343691543075013832 7631, \\ v_{1b,1} &= 358560730876916627874126061532584714659273532061216519326729450479049179 8530. \end{aligned} \tag{56}$$

The base point on $\mathsf{Ed}_{1b,2}$ corresponding to the point (x,y) on E_{1b} given in Table 5 is obtained by applying the map in (36) to (x,y). Denoting this point by $(u_{1b,2}, v_{1b,2})$, we have

$$\begin{aligned} u_{1b,2} &= 347888382208143305990809541905784590022487931111412386618732867410048924 1661, \\ v_{1b,2} &= 135874835400821174223565521805362464970942387361574222961044025555607512 0810. \end{aligned} \tag{57}$$

3. Consider the applicability of Theorem 5. In this case, $p \equiv 3 \bmod 4$, but, μ is a non-square in $\mathbb{F}_p$. So, the first point of Theorem 5 applies. This leads to the curve

$$\mathsf{Ed}_{1b,3} = E_{E,-1,d} \tag{58}$$

where $d = -1/\mu = (\mathsf{b}^4 - \mathsf{a}^4)/\mathsf{a}^4 = -3971/34596$.

The base point on $\mathsf{Ed}_{1b,3}$ corresponding to the point (x,y) on E_{1b} given in Table 5 is obtained by applying the map in (40) to (x,y). Denoting this point by $(u_{1b,3}, v_{1b,3})$, we have

$$\begin{aligned} u_{1b,3} &= 279384427863066756171296927756419730694510922171215401414283574039118576 4299, \\ v_{1b,3} &= 160787892939576083795501963091107162510895522278246234919330191365920373 1958. \end{aligned} \tag{59}$$

Case 2: $E_{E,-1,d}$ arising from $E_2 = E_{L,\mu}$ arising from $\mathsf{KL25519}(82,77)$.

1. The co-factor of $E_2(\mathbb{F}_p)$ is 12 and so by Proposition 1, there is no point of order 4. So, Theorem 3 does not apply.

2. Consider the applicability of Theorem 4. None of the choices of $\alpha \in \{-\omega, 1-\omega, \mu-\omega\}$ lead to any solution. So, Theorem 4 does not apply.

Table 7: Summary of the different twisted Edwards form curve. Here b.r. denotes birational equivalence and 2-iso denotes 2-isogeny.

Kummer	Legendre	twisted Edwards	Legendre to twisted Edwards
$\mathsf{KL2519}(81,20)$	E_{1a}	$\mathsf{Ed}_{1a,1}$	b.r. (Thm 4)
		$\mathsf{Ed}_{1a,2}$	b.r. (Thm 4)
$\mathsf{KL2519}(186,175)$	E_{1b}	$\mathsf{Ed}_{1b,1}$	b.r. (Thm 4)
		$\mathsf{Ed}_{1b,2}$	b.r. (Thm 4)
		$\mathsf{Ed}_{1b,3}$	2-iso (Thm 5)
$\mathsf{KL25519}(82,77)$	E_2	Ed_2	2-iso (Thm 5)
$\mathsf{KL2663}(260,139)$	E_3	Ed_3	2-iso (Thm 5)

3. Consider the applicability of Theorem 5. In this case, $p \equiv 1 \bmod 4$. So, the second case of Theorem 5 applies. This leads to the curve

$$\mathsf{Ed}_2 \quad = \quad E_{E,-1,d} \tag{60}$$

where $d = -\mu = a^4/(\mathsf{b}^4 - \mathsf{a}^4) = -6724/795$.

The base point on Ed_2 corresponding to the point (x, y) on E_2 given in Table 5 is obtained by applying the map in (40) to (x, y). Denoting this point by (u_2, v_2), we have

$$\begin{aligned} u_2 &= 363712947258755944640384273391126119777909476066306568950887863076854463512 35, \\ v_2 &= 542039950253442810131934806601899060517403319985880943197918187333790501426 7. \end{aligned} \tag{61}$$

Case 3: $E_{E,-1,d}$ arising from $E_3 = E_{L,\mu}$ arising from $\mathsf{KL2663}(260, 139)$.

1. The co-factor of $E_2(\mathbb{F}_p)$ is 12 and so by Proposition 1, there is no point of order 4. So, Theorem 3 does not apply.

2. Consider the applicability of Theorem 4. None of the choices of $\alpha \in \{-\omega, 1-\omega, \mu-\omega\}$ lead to any solution. So, Theorem 4 does not apply.

3. Consider the applicability of Theorem 5. In this case, $p \equiv 1 \bmod 4$. So, the second case of Theorem 5 applies. This leads to the curve

$$\mathsf{Ed}_3 \quad = \quad E_{E,-1,d} \tag{62}$$

where $d = -\mu = a^4/(\mathsf{b}^4 - \mathsf{a}^4) = -67600/48279$.

The base point on Ed_3 corresponding to the point (x, y) on E_3 given in Table 5 is obtained by applying the map in (40) to (x, y). Denoting this point by (u_3, v_3), we have

$$\begin{aligned} u_3 &= 8919004806221241600184220908322818790429055707808811414857735739566409385856 2357, \\ v_3 &= 5472512270313131129416933222567577373114675829668894266032876626509097577520 53. \end{aligned} \tag{63}$$

A summary of the twisted Edwards form curve that are obtained from the Legendre form curves is provided in Table 7.

6 Scalar Multiplication on Legendre/twisted Edwards Form Curves

For the twisted Edwards curves which are obtained from Legendre curves using a birational equivalence, the hardness of the discrete logarithm problem is preserved. For these twisted Edwards curves, it is sufficient to work only on these curves without reference to the underlying Legendre curves. So, the scalar multiplication algorithms for twisted Edwards curve using extended twisted Edwards coordinates can be applied. From Table 7, the relevant curves are $\mathsf{Ed}_{1a,1}$, $\mathsf{Ed}_{1b,1}$, $\mathsf{Ed}_{1b,2}$, $\mathsf{Ed}_{1b,3}$, $\mathsf{Ed}_{2,1}$, $\mathsf{Ed}_{3,1}$. For the twisted Edwards curves which are obtained from Legendre curves using a 2-isogeny, it is required to work over the Legendre curves.

Following [7] scalar multiplication on the corresponding Legendre curves can be performed in the following manner. Let Φ (resp. $\widehat{\Phi}$) be the 2-isogeny (resp. the dual 2-isogeny) from the Legendre form curve to the twisted Edwards form curve (resp. from the twisted Edwards form curve to the Legendre form curve). Let q be the largest prime dividing the order of the group of $\mathbb{F}_p$ rational points of the Legendre form curve. Let $\mathbf{P}$ be a point on the Legendre form curve of order q and n be a scalar. Since q is a prime, 2 has a multiplicative inverse modulo q. Following [7], the scalar multiplication $n\mathbf{P}$ can be done in the following manner: $\overline{\mathbf{P}} = \Phi(\mathbf{P})$; $\overline{n} = n/2 \bmod q$; $\overline{\mathbf{Q}} = \overline{n}\overline{\mathbf{P}}$; $\mathbf{Q} = \widehat{\Phi}(\overline{\mathbf{Q}})$; return $\mathbf{Q}$.

The above requires an application of Φ and $\widehat{\Phi}$ each and a scalar multiplication in the twisted Edwards form curve. The times required for computing Φ and $\widehat{\Phi}$ are negligible in comparison to the scalar multiplication. Instead of directly computing the scalar multiplication on the Legendre form curve, this procedure benefits from the fast scalar multiplication possible on the twisted Edwards form curve.

A unified addition algorithm using extended twisted Edwards coordinates for twisted Edwards curves of the form $-u^2 + v^2 = 1 + du^2v^2$ has been given in [13]. Suppose, it is required to add $(U_1 : V_1 : T_1 : W_1)$, $(U_2 : V_2 : T_2 : W_2)$ and the result is $(U_3 : V_3 : T_3 : W_3)$. The algorithm for performing this operation is shown in Table 8. This requires a total of $8\mathcal{M} + 1\mathcal{C} + 8\mathcal{A}$ where the $\mathcal{C}$ is the multiplication by $2d$. For the cases, where d is a general element of $\mathbb{F}_p$, essentially $9\mathcal{M} + 8\mathcal{A}$ is required. On the other hand, suppose that $d = d_1/d_2$ where d_1 and d_2 are small integers. The values of d arising in the cases of $\mathsf{Ed}_{1b,4}$, $\mathsf{Ed}_{2,2}$ and $\mathsf{Ed}_{3,2}$ can be written in this form. In this case, the above computation for obtaining $(U_3 : V_3 : T_3 : W_3)$ can be rewritten as shown in Table 9. This requires $8\mathcal{M} + 4\mathcal{C} + 8\mathcal{A}$. In this case, the multiplications counted by $\mathcal{C}$ are indeed multiplications by small constants. In other words, instead of $9\mathcal{M} + 8\mathcal{A}$, the cost becomes $8\mathcal{M} + 4\mathcal{C} + 8\mathcal{A}$. This is advantageous only if the time required for four multiplications by small constants is lesser than a general field multiplication.

For fixed base scalar multiplication, the efficiency can be further improved as suggested in [6]. Suppose $(U_1 : V_1 : T_1 : W_1)$ is the fixed base where $W_1 = 1$ and $T_1 = U_1V_1$. If the fixed base point is represented as $(U_1 - V_1, U_1 + V_1, 2dT_1)$ then in the computation in Figure 8, the following simplifications become possible. The multiplication $(2d)T_1 \cdot T_2$ becomes $(2dT_1) \cdot T_2$; the multiplication $2W_1 \cdot W_2$ becomes $2W_2$; and the computations $U_1 - V_1$ and $U_1 + V_1$ are not required. So, the overall cost becomes $7\mathcal{M} + 6\mathcal{A}$. It had already been pointed out in [13] that using $W_1 = 1$ leads to a cost of $7\mathcal{M} + 1\mathcal{C} + 8\mathcal{A}$. Using $W_1 = 1$ in conjunction with the idea in [6] of using $(U_1 - V_1, U_1 + V_1, 2dT_1)$ representation of the fixed base point leads to the cost of $7\mathcal{M} + 6\mathcal{A}$.

7 Conclusion

This work considered methods to move between Legendre form elliptic curves and associated Kummer lines as well as methods to move between Legendre form elliptic curves and corresponding twisted Edwards form elliptic curves. Complete details of the methods are presented. Further, new concrete twisted Edwards form elliptic curves are proposed. These correspond to previously proposed concrete Kummer lines at the 128-bit security level which admit very fast scalar multiplication on modern architectures supporting SIMD operations.

Table 8: General d.	Table 9: $d = d_1/d_2$ with d_1, d_2 small.
$A \leftarrow (V_1 - U_1) \cdot (V_2 - U_2)$,	$A \leftarrow (V_1 - U_1) \cdot (V_2 - U_2)$,
$B \leftarrow (V_1 + U_1) \cdot (V_2 + U_2)$,	$B \leftarrow (V_1 + U_1) \cdot (V_2 + U_2)$,
$C \leftarrow (2d)T_1 \cdot T_2$,	$C \leftarrow (2d_1)T_1 \cdot T_2$,
$D \leftarrow 2W_1 \cdot W_2$,	$D \leftarrow (2d_2)W_1 \cdot W_2$,
$E \leftarrow B - A$,	$E \leftarrow d_2(B - A)$,
$F \leftarrow D - C$,	$F \leftarrow D - C$,
$G \leftarrow D + C$,	$G \leftarrow D + C$,
$H \leftarrow B + A$,	$H \leftarrow d_2(B + A)$,
$U_3 \leftarrow E \cdot F$,	$U_3 \leftarrow E \cdot F$,
$V_3 \leftarrow G \cdot H$,	$V_3 \leftarrow G \cdot H$,
$T_3 \leftarrow E \cdot H$,	$T_3 \leftarrow E \cdot H$,
$W_3 \leftarrow F \cdot G$.	$W_3 \leftarrow F \cdot G$.

References

[1] J. Barwise and P. Eklof. Lefschetz's principle. *Journal of Algebra*, 13(4):554–570, 1969.

[2] D. J. Bernstein. Curve25519: New Diffie-Hellman speed records. In *Public Key Cryptography - PKC*, volume 3958 of *Lecture Notes in Computer Science*, pages 207–228. Springer, 2006.

[3] D. J. Bernstein and T. Lange. Explicit-formulas database. `http://www.hyperelliptic.org/EFD/index.html`, 2007.

[4] D. J. Bernstein and Lange T. Faster addition and doubling on elliptic curves. In *Advances in Cryptology - ASIACRYPT*, volume 4833 of *Lecture Notes in Computer Science*, pages 29–50. Springer, 2007.

[5] Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange, and Christiane Peters. Twisted edwards curves. In Serge Vaudenay, editor, *Progress in Cryptology - AFRICACRYPT 2008, First International Conference on Cryptology in Africa, Casablanca, Morocco, June 11-14, 2008. Proceedings*, volume 5023 of *Lecture Notes in Computer Science*, pages 389–405. Springer, 2008.

[6] Daniel J. Bernstein, Niels Duif, Tanja Lange, Peter Schwabe, and Bo-Yin Yang. High-speed high-security signatures. *J. Cryptographic Engineering*, 2(2):77–89, 2012.

[7] Eric Brier and Marc Joye. Fast point multiplication on elliptic curves through isogenies. In Marc P. C. Fossorier, Tom Høholdt, and Alain Poli, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, 15th International Symposium, AAECC-15, Toulouse, France, May 12-16, 2003, Proceedings*, volume 2643 of *Lecture Notes in Computer Science*, pages 43–50. Springer, 2003.

[8] M. Prem Laxman Das and Palash Sarkar. Pairing computation on twisted edwards form elliptic curves. In Steven D. Galbraith and Kenneth G. Paterson, editors, *Pairing-Based Cryptography - Pairing 2008, Second International Conference, Egham, UK, September 1-3, 2008. Proceedings*, volume 5209 of *Lecture Notes in Computer Science*, pages 192–210. Springer, 2008.

[9] Harold M. Edwards. A normal form for elliptic curves. *Bulletin of the American Mathematical Society*, 44:393–422, 2007.

[10] G. Frey and H.-G. Rück. The strong lefschetz principle in algebraic geometry. *Manuscripta Mathematica*, 55(3):385–401, 1986.

[11] P. Gaudry. Fast genus 2 arithmetic based on theta functions. *J. Mathematical Cryptology*, 1(3):243–265, 2007.

[12] P. Gaudry and D. Lubicz. The arithmetic of characteristic 2 Kummer surfaces and of elliptic Kummer lines. *Finite Fields and Their Applications*, 15(2):246–260, 2009.

[13] Hüseyin Hisil, Kenneth Koon-Ho Wong, Gary Carter, and Ed Dawson. Twisted Edwards curves revisited. In Josef Pieprzyk, editor, *Advances in Cryptology - ASIACRYPT 2008, 14th International Conference on the Theory and Application of Cryptology and Information Security, Melbourne, Australia, December 7-11, 2008. Proceedings*, volume 5350 of *Lecture Notes in Computer Science*, pages 326–343. Springer, 2008.

[14] Jun ichi Igusa. *Theta functions*. Springer, 1972.

[15] Sabyasachi Karati and Palash Sarkar. Kummer for genus one over prime order fields. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part II*, volume 10625 of *Lecture Notes in Computer Science*, pages 3–32. Springer, 2017.

[16] Neal Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, 48(177):203–209, 1987.

[17] Victor S. Miller. Use of elliptic curves in cryptography. In *Advances in Cryptology - CRYPTO'85, Santa Barbara, California, USA, August 18-22, 1985, Proceedings*, pages 417–426. Springer Berlin Heidelberg, 1985.

[18] Peter L. Montgomery. Speeding the Pollard and elliptic curve methods of factorization. *Mathematics of Computation*, 48(177):243–264, 1987.

[19] D. Mumford. *Tata lectures on theta I.* Progress in Mathematics 28. Birkh äuser, 1983.

[20] Katsuyuki Okeya, Hiroyuki Kurumatani, and Kouichi Sakurai. Elliptic curves with the montgomery-form and their cryptographic applications. In Hideki Imai and Yuliang Zheng, editors, *Public Key Cryptography, Third International Workshop on Practice and Theory in Public Key Cryptography, PKC 2000, Melbourne, Victoria, Australia, January 18-20, 2000, Proceedings*, volume 1751 of *Lecture Notes in Computer Science*, pages 238–257. Springer, 2000.

[21] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer, 2009.