Arithmetic of split Kummer surfaces: Montgomery endomorphism of Edwards products

David Kohel
Institut de Mathématiques de Luminy

International Workshop on Codes and Cryptography 2011
Qingdao, 2 June 2011

Elliptic curve scalar multiplication

The cryptographic use of elliptic curves over finite fields in place of the multiplicative group of a finite field in cryptography, in an ElGamal or Diffie–Hellman protocol, is based on performance relative to security. For the same security level, one can take a significantly smaller sized field which compensates for the additional complexity of elliptic curve operations.

On the other hand, the additional complexity of addition on elliptic curves leaves room for more sophisticated ideas for minimizing its cost. In the Diffie–Hellman protocol, it suffices to have a scalar multiplication $P \mapsto nP$, rather than a group. Here we focus on the arithmetic of the *Kummer curve* and *split Kummer surface*

$$\mathcal{K}_1 = E/\langle -1 \rangle, \text{ and } \mathcal{K}_2 = E \times E/\langle (-1,-1) \rangle.$$

which admit scalar multiplications (induced from E).

Montogomery scalar multiplication

Let A be an additive abelian group and $\mathrm{M}_2(\mathbb{Z}) \subset \mathrm{End}(A^2)$, such that

$$\alpha(x,y) = (ax+by, cx+dy) \text{ where } \alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Define endomorphisms σ by $\sigma(x,y) = (y,x)$ and φ_i by

$$\varphi = \varphi_0 = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}, \text{ and } \varphi_1 = \sigma \circ \varphi \circ \sigma = \begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix},$$

The Montgomery ladder for scalar multiplication by an integer n is expressed on A^2 by the recursion

$$v_r = (x,0) \text{ and } v_i = \varphi_{n_i}(v_{i+1}) \text{ for } i = r-1, \ldots, 1, 0,$$

where n has binary representation $n_{r-1} \ldots n_1 n_0$.

Montogomery endomorphism

The successive steps v_i in the ladder are of the form

$$((k+1)x, kx)$$

and $v_0 = (nx, (n-1)x)$, from which we output nx. We refer to φ ($= \varphi_0$ and φ_1) as the *Montgomery endomorphism(s)*.

Example. For $n = 13 = 1101_2$, we have

$$(x,0) \xrightarrow{\varphi_1} (2x,x) \xrightarrow{\varphi_1} (4x,3x) \xrightarrow{\varphi_0} (7x,6x) \xrightarrow{\varphi_1} (13x,12x)$$

Moreover, since -1 is an automorphism in the center of $\mathrm{M}_2(\mathbb{Z})$, an endomorphism of A^2 also acts on the quotient $A^2/\langle -1 \rangle$.

In particular, we will derive expressions for certain endomorphisms of the split Kummer surface associated to an elliptic curve E (as a means of computing φ), when E is in Edwards normal form.

Montgomery endomorphism factorizations

There exists a close relation between the Montgomery endomorphism φ and another endomorphism ρ:

$$\varphi = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} \text{ and } \rho = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Both have determinant 2, up to sign, but the symmetry properties of ρ make it more suitable for its efficient evaluation in the context of elliptic curve products.

We observe that $\tau(x, y) = (x + y, y)$ — determined by a single addition — allows us to compute φ:

$$\varphi_1 = \begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix} = \tau \circ \sigma \circ \rho = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

and $\varphi = \sigma \circ \varphi_1 \circ \sigma$ (where the cost of σ is trivial).

Application to Kummer quotients

Prior work has considered Montgomery addition in relation to the Kummer curves (of a Weierstrass model):

$$\mathcal{K}_1 = E/\{\pm 1\} \cong \mathbb{P}^1,$$

determined by the quotient $\pi(= x) : E \to \mathcal{K}_1$. Such work is usually expresses as "operating only on the x-coordinate".

Caution: *Due to an unfortunate choice of coordinate names, an Edwards curve has the traditional roles of the functions x and y reversed: x is anti-invariant and y invariant under $[-1]$. Thus for an Edwards curve, "eliminating the x-coordinate" refers to the Kummer quotient $\pi(= y) : E \to \mathcal{K}_1$.*

This Kummer curve approaches focus on arithmetic of $\mathcal{K}_1$ and the full quotient $\mathcal{K}_1^2$; we introduce the study of the intermediate surface $\mathcal{K}_2$:

$$E^2 \longrightarrow \mathcal{K}_2 = E^2/\langle(-1,-1)\rangle \longrightarrow \mathcal{K}_1^2 = E^2/\langle(\pm 1, \pm 1)\rangle.$$

Kummer quotients and endomorphisms

In the study of the arithmetic of Kummer quotients, the endomorphism of E^2,

$$\rho = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

satisfying $\rho^2 = 2$, plays an important role. The successive quotients, and the endomorphism ρ, give a hierarchy of commuting maps

$$\begin{array}{ccc} E^2 & \xrightarrow{\rho} & E^2 \\ \downarrow & \searrow & \downarrow \\ \mathcal{K}_2 & \xrightarrow{\rho} & \mathcal{K}_2 \\ \downarrow & \searrow & \downarrow \\ \mathcal{K}_1^2 & & \mathcal{K}_1^2. \end{array}$$

Note that ρ induces an endomorphism of $\mathcal{K}_2$, also denoted ρ, but no such map is induced on $\mathcal{K}_1^2$.

Differential addition of Kummer quotients

Although ρ does not extend to an endomorphism of $\mathcal{K}_1^2$ we obtain a system of polynomial equations in $\mathcal{K}_1^2 \times \mathcal{K}_1^2$ from the graph:

$$\Gamma_\rho = \left\{ \big((P,Q), \rho(P,Q)\big) : (P,Q) \in E^2 \right\} \subset E^2 \times E^2,$$

where $\rho(P,Q) = (P+Q, P-Q)$. We denote by $\overline{\Gamma}_\rho$ the image of Γ_ρ in $\mathcal{K}_2$ or $\mathcal{K}_1^2$.

One recovers $\pi(P+Q)$ by specializing this system at known points

$$\pi(P),\ \pi(Q),\ \pi(P-Q).$$

Such an interpolation algorithm is called a *pseudo-addition* or *differential addition* on $\mathcal{K}_1$.

Edwards model for elliptic curves

In 2007, Edwards introduced a new model for elliptic curves, defined by the affine model

$$x^2 + y^2 = a^2(1 + z^2),\ z = xy,$$

over any field k of characteristic different from 2. The complete linear system associated to the degree 4 model determines a nonsingular model in $\mathbb{P}^3$ with identity $\mathrm{O} = (1 : 0 : a : 0)$:

$$\boxed{a^2(X_0^2 + X_3^2) = X_1^2 + X_2^2,\ X_0X_3 = X_1X_2,}$$

as a family of curves over $k(a) = k(X(4))$. Lange and Bernstein introduced a rescaling to descend to $k(d) = k(a^4) = k(X_1(4))$, and subsequently (with Joye, Birkner, and Peters) a quadratic twist by c, to define the twisted Edwards model with $\mathrm{O} = (1 : 0 : 1 : 0)$:

$$\boxed{X_0^2 + dX_3^2 = cX_1^2 + X_2^2,\ X_0X_3 = X_1X_2.}$$

Edwards model factorization

The (twisted) Edwards model...

$$\boxed{X_0^2 + dX_3^2 = cX_1^2 + X_2^2,\ X_0X_3 = X_1X_2 \text{ with } \mathrm{O} = (1:0:1:0)}$$

admits a factorization $S \circ (\pi_1 \times \pi_2) = \mathrm{id}$ through $\mathbb{P}^1 \times \mathbb{P}^1$, where

$$\pi_1(X_0 : X_1 : X_2 : X_3) = (X_0 : X_1) = (X_2 : X_3),$$
$$\pi_2(X_0 : X_1 : X_2 : X_3) = (X_0 : X_2) = (X_1 : X_3),$$

and $S : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3$ is the Segre embedding

$$S((U_0 : U_1), (V_0 : V_1)) = (U_0V_0 : U_1V_0 : U_0V_1 : U_1V_1).$$

Remark: The inverse morphism is

$$[-1](X_0 : X_1 : X_2 : X_3) = (X_0 : -X_1 : X_2 : -X_3),$$

$\pi_2 : E \to \mathbb{P}^1 = \mathcal{K}_1$ is the Kummer quotient, and $\pi_2(\mathrm{O}) = (1 : 1)$.

Edwards addition law

The remarkable property of the Edwards model is that the composition of the addition morphism

$$\mu : E \times E \longrightarrow E$$

with each of the projectons $\pi_i : E \to \mathbb{P}$ admits a basis of *bilinear* defining polynomials. For $\mu \circ \pi_1$, we have

$$\left\{ \begin{array}{l} (X_0Y_0 + dX_3Y_3,\ X_1Y_2 + X_2Y_1), \\ (cX_1Y_1 + X_2Y_2,\ X_0Y_3 + X_3Y_0) \end{array} \right\},$$

and for $\mu \circ \pi_2$, we have

$$\left\{ \begin{array}{l} (X_1Y_2 - X_2Y_1,\ -X_0Y_3 + X_3Y_0), \\ (X_0Y_0 - dX_3Y_3,\ -cX_1Y_1 + X_2Y_2) \end{array} \right\}.$$

Addition laws given by polynomial maps of bidegree $(2, 2)$ are recovered by composing with the Segre embedding.

Models for Kummer quotients

The Edwards Kummer curve $\mathcal{K}_1 \cong \mathbb{P}^1$ is determined by the projection π_2 to $(X_0 : X_2)$, however *on* $\mathcal{K}_1$ *we denote the coordinate functions* $(X_0 : X_1)$. The following lemma is a consequence of the addition law projection for π_2.

Lemma

The duplication morphism on E *induces* $[2] : \mathcal{K}_1 \to \mathcal{K}_1$, *given by*

$$(X_0 : X_1) \mapsto ((d-1)X_0^4 - d(X_0^2 - X_1^2)^2 : (X_0^2 - X_1^2)^2 + (d-1)X_1^4).$$

This polynomial map is unique and determines $[2]$ *everywhere.*

Remark. Clearly $\pi_2(\mathrm{O}) = (1 : 1)$ maps to itself, and the pre-image of $(1 : 1)$ are the solutions to

$$X_0^4 - (d+1)X_0^2X_1^2 + dX_1^4 = (X_0^2 - dX_1^2)(X_0^2 - X_1^2) = 0,$$

which are the equations cutting out $E[2]$.

Product Kummer curve model

The Segre embedding maps a projective space product $\mathbb{P}^r \times \mathbb{P}^s$ into a projective space $\mathbb{P}^{(r+1)(s+1)-1}$, given by

$$((X_0 : \cdots : X_r), (Y_0 : \cdots : Y_s)) \mapsto (X_0Y_0 : X_1Y_0 : \cdots : X_rY_s).$$

For the Kummer curve product, this gives $S : \mathcal{K}_1^2 \cong \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3$

$$\begin{aligned}((X_0 : X_1), (Y_0 : Y_1)) \mapsto (X_0Y_0 : X_1Y_0 : X_0Y_1 : X_1Y_1) \\ = (U_0 : U_1 : U_2 : U_3).\end{aligned}$$

whose image is $U_0U_3 = U_1U_2$.

We use this representation for $S(\mathcal{K}_1^2) \subset \mathbb{P}^3$ and construct $\mathcal{K}_2$ as a double cover:

$$E^2 \longrightarrow \mathcal{K}_2 = E^2/\langle(-1,-1)\rangle \longrightarrow S(\mathcal{K}_1^2) \cong \mathcal{K}_1^2 = E^2/\langle(\pm 1, \pm 1)\rangle.$$

Split Kummer surface models

We now describe the embeddings of $\mathcal{K}_2$ as a double cover of $\mathcal{K}_1^2$.

Theorem

The Kummer surface $\mathcal{K}_2$ has a model as a hypersurface in $\mathcal{K}_1^2 \times \mathbb{P}^1$ given by

$$(X_0^2 - X_1^2)(Y_0^2 - Y_1^2)Z_0^2 = (X_0^2 - dX_1^2)(Y_0^2 - dY_1^2)Z_1^2,$$

with base point $\pi(\mathrm{O}) = ((1:1),(1:1),(1:0))$.
Under the Segre embedding $S : \mathcal{K}_1^2 \mapsto \mathbb{P}^3$, this determines the variety in $\mathbb{P}^3 \times \mathbb{P}^1$ cut out by

$$(U_0^2 - U_1^2 - U_2^2 + U_3^2)Z_0^2 = (U_0^2 - dU_1^2 - dU_2^2 + d^2U_3^2)Z_1^2,$$

on the hypersurface $U_0U_3 = U_1U_2$ defining $S(\mathcal{K}_1^2)$.

Edwards Kummer quotient maps

Recall that $E : X_0^2 + dX_3^2 = X_1^2 + X_2^2, X_0X_3 = X_1X_3$ is an Edwards elliptic curve in $\mathbb{P}^3$ with identity $\mathrm{O} = (1 : 0 : 1 : 0)$.

For a pair $(P, Q) = \big((X_0 : X_1 : X_2 : X_3), (Y_0 : Y_1 : Y_2 : Y_3)\big)$, the projection

$$E^2 \to \mathcal{K}_2 \subset \mathcal{K}_1^2 \times \mathbb{P}^1$$

is given by

$$\pi_1(P, Q) = (X_0 : X_2),\ \pi_2(P, Q) = (Y_0 : Y_2),$$

and

$$\begin{aligned}\pi_3(P, Q) &= (X_0Y_0 : X_1Y_1) = (X_2Y_0 : X_3Y_1)\\ &= (X_0Y_2 : X_1Y_3) = (X_2Y_2 : X_3Y_3) = (Z_0 : Z_1).\end{aligned}$$

After composition with the Segre embedding, we find

$$(P, Q) \mapsto (X_0Y_0 : X_2Y_0 : X_0Y_2 : X_2Y_2) = (U_0 : U_1 : U_2 : U_3).$$

Kummer endomorphisms

Recall that our objective is to compute φ_0 and φ_1, which can be defined by $\varphi_1 = \tau \circ \sigma \circ \rho$ and $\varphi = \sigma \circ \varphi_1 \circ \sigma$. For ρ (and τ) we describe explicit polynomial maps:

$$((U_0 : U_1 : U_2 : U_3), (Z_0 : Z_1)) \longmapsto ((V_0 : V_1 : V_2 : V_3), (W_0 : W_1)),$$

for V_i and W_j, for which it suffices to define:

$$\begin{aligned}
\pi_1((V_0 : V_1 : V_2 : V_3), (W_0 : W_1)) &= (V_0 : V_1) = (V_2 : V_3), \\
\pi_2((V_0 : V_1 : V_2 : V_3), (W_0 : W_1)) &= (V_0 : V_2) = (V_1 : V_3), \\
\pi_3((V_0 : V_1 : V_2 : V_3), (W_0 : W_1)) &= (W_0 : W_1).
\end{aligned}$$

The image point $((V_0 : V_1 : V_2 : V_3), (W_0 : W_1))$ requires the composition of the Segre embedding with $(\pi_1 \circ \rho) \times (\pi_2 \circ \rho)$.

Kummer automorphism σ

Theorem

The automorphism σ is given on $\mathcal{K}_2 \subset \mathcal{K}_1^2 \times \mathbb{P}^1$ by

$$((X_0 : X_1), (Y_0 : Y_1), (Z_0 : Z_1)) \longmapsto ((Y_0 : Y_1), (X_0 : X_1), (Z_0 : Z_1)),$$

and on $\mathcal{K}_2 \subset S(\mathcal{K}_1^2) \times \mathbb{P}^1$, by

$$((U_0 : U_1 : U_2 : U_3), (Z_0 : Z_1)) \longmapsto ((U_0 : U_2 : U_1 : U_3), (Z_0 : Z_1)).$$

Note. This is on $O(1)$ algorithm (change of pointers).

Kummer endomorphism ρ

Theorem

The projections of the endomorphism $\rho : \mathcal{K}_2 \to \mathcal{K}_2$ are uniquely represented by polynomials of bidegree $(1,1)$, $(1,1)$, and $(2,0)$, explicitly:

$$\pi_1 \circ \rho\big((U_0 : U_1 : U_2 : U_3),(Z_0 : Z_1)\big) = (U_0Z_0 - dU_3Z_1 : -U_0Z_1 + U_3Z_0)$$

$$\pi_2 \circ \rho\big((U_0 : U_1 : U_2 : U_3),(Z_0 : Z_1)\big) = (U_0Z_0 + dU_3Z_1 : U_0Z_1 + U_3Z_0)$$

$$\pi_3 \circ \rho\big((U_0 : U_1 : U_2 : U_3),(Z_0 : Z_1)\big) = (U_0^2 - dU_3^2 \ : \ -U_1^2 + U_2^2)$$

Note. This is fast.

Kummer endomorphism τ

Theorem

The projections $\pi_i \circ \tau : \mathcal{K}_2 \to \mathcal{K}_1$, for $1 \leq i \leq 2$, are uniquely represented by polynomials of bidegree $(1,1)$ and $(1,0)$,

$$\begin{aligned}\pi_1 \circ \tau\big((U_0 : U_1 : U_2 : U_3), (Z_0 : Z_1)\big) \\ = (U_0 Z_0 - d U_3 Z_1 : -U_0 Z_1 + U_3 Z_0),\\ \pi_2 \circ \tau\big((U_0 : U_1 : U_2 : U_3), (Z_0 : Z_1)\big) = (U_0 : U_2) = (U_1 : U_3),\end{aligned}$$

and $\pi_3 \circ \tau\big((U_0 : U_1 : U_2 : U_3), (Z_0 : Z_1)\big)$ is given by any linear combination of the expressions of bidegree $(2,1)$:

$$\begin{aligned}&\big((U_0^2 - dU_3^2)Z_0 \ : \ (U_0U_1 - U_2U_3)Z_0 + (U_0U_2 - dU_1U_3)Z_1\big)\\ &\big(-(U_0U_2 - U_1U_3)Z_0 + (U_0U_1 - dU_2U_3)Z_1 \ : \ (U_1^2 - U_2^2)Z_1\big)\end{aligned}$$

Note. This is not.

A Kummer pseudo-addition for φ

The efficient computation of $\varphi_1 = \tau \circ \sigma \circ \rho : \mathcal{K}_2 \to \mathcal{K}_2$ and $\varphi_0 = \sigma \circ \varphi_1 \circ \sigma$ using the previous theorems is hindered by the expensive computation of the one bit of information lost in the map $\mathcal{K}_2 \to S(\mathcal{K}_1^2)$. But so far we haven't use the special properties of the sequence of points which arise in scalar multiplication.

In the application we apply this map to a sequence

$$(P, Q) = ((k+1)T, kT)$$

for a fixed point T, hence we remain on the irreducible curve

$$\Delta_T = \delta^*(T) = \{(P, Q) \in E^2 \mid \delta(P, Q) = T\},$$

where δ is the difference morphism $(\delta(P, Q) = P - Q)$.

We can derive more efficient algorithms based on the restrictions to Δ_T. In particular note that φ determines a well-defined morphism

$$\varphi_T : \overline{\Delta}_T \longrightarrow \overline{\Delta}_T.$$

Expressing φ_T as a conjugate duplication

More precisely, each φ_i factors through the duplication map:

$$\Delta_T \longrightarrow \Delta \xrightarrow{[2]} \Delta \longrightarrow \Delta_T.$$

In particular, setting τ_T to be the translation–by–T map $\tau_T(P) = P + T$, we have

$$\varphi_0 = (\tau_T \times [1]) \circ [2] \circ (\tau_T \times [1])^{-1}$$

taking

$$(P + T, P) \mapsto (P, P) \mapsto (2P, 2P) \mapsto (2P + T, 2P),$$

and similarly for

$$\varphi_1 = ([1] \times \tau_T)^{-1} \circ [2] \circ ([1] \times \tau_T).$$

A Kummer differential morphism for φ_T

Theorem

Let $T = (T_0 : T_1 : T_2 : T_3)$ be a fixed point of $E\backslash E[2]$. Then the restriction of φ to $\overline{\Delta}_T \subset S(\mathcal{K}_1^2)$ determines a morphism

$$\varphi_T : \overline{\Delta}_T \to \overline{\Delta}_T$$

defined by $\varphi_T(U_0 : U_1 : U_2 : U_3) = S((S_0, S_1), (R_0, R_1))$, where

$$\begin{aligned}(S_0, S_1) &= ((U_0^2 + dU_3^2)T_0 - 2dU_0U_3T_2,\ 2U_0U_3T_0 - (U_0^2 + dU_3^2)T_2),\\ (R_0, R_1) &= [2](U_0 : U_2)\\ &= ((d-1)U_0^4 - d(U_0^2 - U_2^2)^2,\ (U_0^2 - U_2^2)^2 + (d-1)U_2^4).\end{aligned}$$

Note. This is relatively fast.

Lifting back from $S(\mathcal{K}_1^2)$ to $\mathcal{K}_2$ and E^2

Let $T = (T_0 : T_1 : T_2 : T_3)$ be a fixed point in E. When T is not in $E[2]$, the quotient $\mathcal{K}_2 \to S(\mathcal{K}_1^2)$ is easily seen to be injective on $\overline{\Delta}_T$. Consequently there exists a lifting back to $\overline{\Delta}_T \subset \mathcal{K}_2$. Algebraically, it suffices to define $(Z_0 : Z_1)$, which is given by:

$$(Z_0 : Z_1) = (U_0T_0 - dU_3T_2 : U_0T_2 - U_3T_0).$$

As expected, this fails if and only if $(T_0 : T_2) = (U_0 : U_3)$ and $U_0^2 - dU_3^2$ — this defines the 2-torsion subgroup $E[2]$.

Similarly, the map $\Delta_T \to \overline{\Delta}_T \subset \mathcal{K}_2$ is injective on all points except

$$E[2]_T = \{(P + T, P) \ : \ P \in E[2]\}.$$

This gives the following theorem.

Lifting $\overline{\Delta}_T$ back to E^2

Theorem

For all T be in E, the quotient $\Delta_T \to \overline{\Delta}_T \subset \mathcal{K}_2$ is injective for all points outside of $E[2]_T \subset \Delta_T$. The inverse $((X_0 : X_1 : X_2 : X_3), (Y_0 : Y_1 : Y_2 : Y_3))$ of $((U_0 : U_1 : U_2 : U_3), (Z_0 : Z_1))$ is defined by

$$\begin{aligned}(Y_0 : Y_1) = (Y_2 : Y_3) &= (U_2T_0 - U_1T_2 : U_0T_3 - U_3T_1)\\ &= (U_0T_1 - dU_3T_3 : -U_1T_0 + U_2T_2)\\ (Y_0 : Y_2) = (Y_1 : Y_3) &= (U_0 : U_2) = (U_1 : U_3),\end{aligned}$$

and then

$$\begin{aligned}(X_0 : X_1) = (X_2 : X_3) &= (Y_0T_0 + dY_3T_3 : Y_1T_2 + Y_2T_1)\\ &= (Y_1T_1 + Y_2T_2 : Y_0T_3 + Y_3T_0)\\ (X_0 : X_2) = (X_1 : X_3) &= (U_0 : U_1) = (U_2 : U_3),\end{aligned}$$

A lifted Kummer differential morphism for φ_T

Theorem

Let $T = (T_0 : T_1 : T_2 : T_3)$ be a fixed point of $E \backslash E[2]$. Then the morphism $\varphi_T : \overline{\Delta}_T \to \overline{\Delta}_T$ is defined by

$$((U_0 : U_1 : U_2 : U_3), (Z_0 : Z_1)) \mapsto ((V_0 : V_1 : V_2 : V_3), (W_0 : W_1)),$$

where $(V_0 : V_1 : V_2 : V_3) = S((S_0, S_1), (R_0, R_1))$ is determined by

$$\begin{aligned}(S_0, S_1) &= (U_0 Z_0 - d U_3 Z_1 : -U_0 Z_1 + U_3 Z_0),\\ (R_0, R_1) &= [2](U_0 : U_2)\\ &= ((d-1)U_0^4 - d(U_0^2 - U_2^2)^2,\ (U_0^2 - U_2^2)^2 + (d-1)U_2^4),\end{aligned}$$

and then $(W_0 : W_1) = (V_0 T_0 - d V_3 T_2 : V_0 T_2 - V_3 T_0)$.

Note. This is fast (compared to one addition and one doubling)?