Arithmetic of split Kummer surfaces: Montgomery endomorphism of Edwards products

David Kohel

Arithmetic of split Kummer surfaces: Montgomery endomorphism of Edwards products

David Kohel

Institut de Mathématiques de Luminy
Université de la Méditerranée
163, avenue de Luminy, Case 907
13288 Marseille Cedex 9
France

Abstract. Let E be an elliptic curve, $\mathscr{K}_1$ its Kummer curve $E/\{\pm 1\}$, E^2 its square product, and $\mathscr{K}_2$ the split Kummer surface $E^2/\{\pm 1\}$. The addition law on E^2 gives a large endomorphism ring, which induce endomorphisms of $\mathscr{K}_2$. With a view to the practical applications to scalar multiplication on $\mathscr{K}_1$, we study the explicit arithmetic of $\mathscr{K}_2$.

1 Introduction

Let A be an abelian group, whose group law is expressed additively. Let $\mathrm{M}_2(\mathbb{Z})$ be the subring of $\mathrm{End}(A^2)$, acting as

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

Define endomorphisms σ and φ_i by

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

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

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

where n has binary representation $n_{r-1} \ldots n_1 n_0$. The successive steps v_i in the ladder are of the form $(mx, (m+1)x)$ and $v_0 = (nx, (n+1)x)$, from which we output nx (see Montgomery [10] and Joye [8] for general formulation). We refer to φ as the *Montgomery endomorphism*.

Since -1 is an automorphism in the center of $\mathrm{M}_2(\mathbb{Z})$, an endomorphism of A^2 also acts on the quotient $A^2/\{\pm 1\}$. In particular, we will derive expressions of the above operators on the split Kummer surface $\mathscr{K}_2 = E^2/\{\pm 1\}$ associated to an elliptic curve E.

Prior work has focused on Kummer curves $\mathscr{K}_1 = E/\{\pm 1\} \cong \mathbb{P}^1$, determined by the quotient $\pi : E \to \mathscr{K}_1$, often expressed as operating only on the x-coordinate of a Weierstrass model (see Montgomery [10], Brier and Joye [3] and Izu and Takagi [7]). Such methods consider the full quotient $\mathscr{K}_1^2 = E^2/\{(\pm 1, \pm 1)\}$. For this approach one takes the endomorphism

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

arising in duplication formulas for theta functions [11]. This endomorphism satisfies $\rho^2 = 2$, giving a factorization of 2 in $\mathrm{End}(E^2)$, and induces an endomorphism of $\mathscr{K}_2$, which we also refer to as ρ. This gives a commutative diagram:

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

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

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

One recovers $\pi(P+Q)$ from specializing this sytem at known points $\pi(P)$, $\pi(Q)$ and $\pi(P-Q)$. By considering the partial quotient $\mathscr{K}_2$ as a double cover of $\mathscr{K}_1^2$, we obtain endmorphisms of $\mathscr{K}_2$ induced by the isogenies ρ as well as φ_0 and φ_1.

Since the structure of addition laws of abelian varieties, or isogenies in general, depends intrinsically on the embedding in projective space (see [6], [9]), we develop specific models for the Kummer surface $\mathscr{K}_2$ associated to a model of an elliptic curve E with prescribed embedding. For this purpose we investigate Edwards models for elliptic curves embedded in $\mathbb{P}^3$.

2 Projective embeddings of a Kummer variety $\mathscr{K}$

Let k be a field of characteristic different from 2 and A/k an abelian variety. An addition law on A is defined by Lange and Ruppert [9] to be a polynomial representative for the addition morphism $A^2 \to A$. Such maps depend in an essential way on its projective embedding. Similarly, the explicit polynomial maps for morphisms of the Kummer variety $\mathscr{K} = A/\{\pm 1\}$ depend on a choice of its projective embedding. We approach the problem of embedding $\mathscr{K}$ in the following way.

Let $i : A \to \mathbb{P}^r$ be a projectively normal embedding (see [6] for a definition and motivation for this hypothesis), determined by a symmetric invertible sheaf $\mathscr{L} = \mathcal{O}_A(1) = i^*\mathcal{O}_{\mathbb{P}^r}(1)$ and let $\pi : A \to \mathscr{K}$ be the projection morphism.

We say that an embedding $j : \mathscr{K} \to \mathbb{P}^s$ is *compatible* with $i : A \to \mathbb{P}^r$ if π is represented by a linear polynomial map. In terms of the invertible sheaf $\mathscr{L}_1 = \mathcal{O}_{\mathscr{K}}(1) = j^*\mathcal{O}_{\mathbb{P}^s}(1)$, this condition is equivalent to:

$$\mathrm{Hom}(\pi^*\mathscr{L}_1, \mathscr{L}) \cong \Gamma(A, \pi^*\mathscr{L}_1^{-1} \otimes \mathscr{L}) \neq 0,$$

where $\Gamma(A, \mathscr{M})$ is the space of global sections for a sheaf $\mathscr{M}$. If we have $\pi^*\mathscr{L}_1 \cong \mathscr{L}$ then $\mathrm{Hom}(\pi^*\mathscr{L}_1, \mathscr{L}) \cong k$, and π admits a unique linear polynomial map, up to scalar.

Conversely we can construct an embedding of $\mathscr{K}$ comptable with given $i : A \to \mathbb{P}^r$ as follows. The condition that $i : A \to \mathbb{P}^r$ is projectively normal is equivalent to an isomorphism of graded rings

$$k[X_0, X_1, \ldots, X_r]/I_A = \bigoplus_{n=0}^{\infty} \Gamma(A, \mathscr{L}^n),$$

where I_A is the defining ideal for A in $\mathbb{P}^r$. We fix an isomorphism $\mathscr{L} \cong [-1]^*\mathscr{L}$, from which we obtain an eigenspace decomposition of the spaces $\Gamma(A, \mathscr{L}^n)$:

$$\Gamma(A, \mathscr{L}^n) = \Gamma(A, \mathscr{L}^n)^+ \oplus \Gamma(A, \mathscr{L}^n)^-.$$

The sign is noncanonical, but we may choose the sign for the isomorphism $\mathscr{L} \cong [-1]^*\mathscr{L}$ such that $\dim \Gamma(A, \mathscr{L})^+ \geq \dim \Gamma(A, \mathscr{L})^-$. Setting $V = \Gamma(A, \mathscr{L})^+$, we define $j : \mathscr{K} \to \mathbb{P}^s$ by the image of A in $\mathbb{P}^s = \mathbb{P}(V)$. This defines the sheaf $\mathscr{L}_1 = j^*\mathcal{O}_{\mathbb{P}^s}(1)$ and gives a homomorphism $\pi^*\mathscr{L}_1 \to \mathscr{L}$.

In what follows we carry out this construction to determine projective embeddings for the Kummer varieties $\mathscr{K}_1$ and $\mathscr{K}_2$ associated to an elliptic curve embedded as an Edwards model in $\mathbb{P}^3$, and study the form of the endomorphisms σ, φ and ρ.

3 Edwards model and projective embeddings of $\mathscr{K}_1$

Let E be an elliptic curve embedded in $\mathbb{P}^3$ as an Edwards model (see Edwards [4], Bernstein and Lange [1], and Hisil et al. [5] or Kohel [6] for this form):

$$X_0^2 + dX_3^2 = X_1^2 + X_2^2, \quad X_0X_3 = X_1X_2,$$

with identity $\mathrm{O} = (1 : 0 : 1 : 0)$, and negation map

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

The eigenspace decomposition for $\Gamma(E, \mathscr{L})$ is

$$\Gamma(E, \mathscr{L}) = \bigoplus_{i=1}^{4} kX_i = (kX_0 \oplus kX_1) \oplus (kX_2 \oplus kX_3).$$

The Kummer curve of E is $\mathscr{K}_1 \cong \mathbb{P}^1$, with quotient map

$$(X_0 : X_1 : X_2 : X_3) \mapsto (X_0 : X_2) = (X_1 : X_3).$$

We can now express the scalar multiplication by 2 on $\mathscr{K}_1$ in terms of coordinate functions X_0, X_1 on $\mathscr{K}_1$.

Lemma 1. *The duplication morphism* $[2] : \mathscr{K}_1 \to \mathscr{K}_1$ *is uniquely represented by the polynomial map*

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

Proof. The correctness of the polynomial map can be directly verified by the fact that the known endomorphisms [2] on E commutes with π and the above polynomial map for [2] on $\mathscr{K}_1$. The uniqueness follows from the existence of the above degree four polynomial expressions, since from $\deg([2]) = 4$ we obtain $[2]^*\mathscr{L}_1 \cong \mathscr{L}_1^4$. Since degree n polynomial expressions for a morphism ψ are in bijection with

$$\mathrm{Hom}(\psi^*\mathscr{L}_1, \mathscr{L}_1^n) \cong \Gamma(E, \psi^*\mathscr{L}_1^{-1} \otimes \mathscr{L}_1^n),$$

the result follows. □

4 Segre embedings and projective products

In general a projective model behaves well with respect to the theory. In order to characterize a product $X \times Y$ with $X \subseteq \mathbb{P}^r$ and $Y \subseteq \mathbb{P}^s$ we apply the Segre embedding $S : \mathbb{P}^r \times \mathbb{P}^s \to \mathbb{P}^{rs+r+s}$ given by

$$\big((X_0 : X_1 : \cdots : X_r), (Y_0 : Y_1 : \cdots : Y_s)\big) \longmapsto (X_0Y_0 : X_1Y_0 : \cdots : X_rY_s),$$

and consider the image $S(X \times Y)$ in $\mathbb{P}^{rs+r+s}$.

For $r = s = 1$, we have $(r+1) + (s+1) = 4$ coordinates to represent a point in $\mathbb{P}^1 \times \mathbb{P}^1$ and $(r+1)(s+1) = 4$ coordinates for a point in $\mathbb{P}^3$. For higher degrees or powers $\mathbb{P}^{r_1} \times \cdots \times \mathbb{P}^{r_t}$ the Segre embedding becomes unwieldy for explicit computation.

In particular, for the product $\mathscr{K}_1^2 \cong \mathbb{P}^1 \times \mathbb{P}^1$ this gives the embedding of $\mathscr{K}_1^2$ in $\mathbb{P}^3$ as the hypersurface $U_0U_3 = U_1U_2$, given by

$$\big((X_0 : X_1), (Y_0 : Y_1)\big) \longmapsto (U_0 : U_1 : U_2 : U_3) = (X_0Y_0 : X_1Y_0 : X_0Y_1 : X_1Y_1).$$

The inverse is given by the product of projections $\pi_1 : S(\mathscr{K}_1^2) \to \mathscr{K}_1$

$$(U_0 : U_1 : U_2 : U_3) \longmapsto (U_0 : U_1) = (U_2 : U_3),$$

and $\pi_2 : S(\mathscr{K}_1^2) \to \mathscr{K}_1$

$$(U_0 : U_1 : U_2 : U_3) \longmapsto (U_0 : U_2) = (U_1 : U_3).$$

Each projection is represented locally by a two-dimensional space of linear polynomial maps, but no such map defines π_i globally as a morphism.

We use the Segre embedding $\mathscr{K}_1^2 \to S(\mathscr{K}_1^2)$ to provide a projective embedding for $\mathscr{K}_1^2$ and construct $\mathscr{K}_2$ as a double cover of $S(\mathscr{K}_1^2)$ in $S(\mathscr{K}_1^2) \times \mathbb{P}^1 \subseteq \mathbb{P}^3 \times \mathbb{P}^1$. To preserve the compactness of the representation we work with the model in $\mathbb{P}^3 \times \mathbb{P}^1$, rather than its model in $\mathbb{P}^7$, however we give this model in Theorem 1.

In order to define a morphism $\mathscr{K}_2 \to \mathscr{K}_2$ it suffices to make use of the factorization through $\mathscr{K}_1^2 \times \mathbb{P}^1$ to each of the products. Thus a morphism $\psi : X \to \mathscr{K}_2$ is determined by three maps $\psi_i = \pi_i \circ \psi$ for $1 \leq i \leq 3$, and a composition with a Segre embedding of $\mathscr{K}_1^2$ to $\mathbb{P}^3$ gives the map to $\mathscr{K}_2$ in $\mathbb{P}^3 \times \mathbb{P}^1$. We note, however, that expansion of polynomial maps for this factorization $S \circ (\pi_1 \times \pi_2)$ may yield polynomial maps of higher degree than $\mathscr{K}_2 \to S(\mathscr{K}_1^2)$ directly (see Theorem 1).

Note. Despite the isomorphism $\mathscr{K}_1 \cong \mathbb{P}^1$, and even equality under the projective embedding, we write $\mathscr{K}_1^2$ and $\mathscr{K}_1^2 \times \mathbb{P}^1$ rather than $(\mathbb{P}^1)^2$ and $(\mathbb{P}^1)^3$ in order to reflect the distinguished role of the two Kummer curves in this product.

5 Edwards model and projective embeddings of $\mathscr{K}_2$

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

Theorem 1. *Let $E : X_0^2 + dX_3^2 = X_1^2 + X_2^2, X_0X_3 = X_1X_3$ be an elliptic curve in $\mathbb{P}^3$ with identity $\mathrm{O} = (1:0:1:0)$. The Kummer surface $\mathscr{K}_2$ has a model as a hypersurface in $\mathscr{K}_1^2 \times \mathbb{P}^1$ 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 $\pi(\mathrm{O}) = ((1:1),(1:1),(1:0))$, and projection $E^2 \to \mathscr{K}_2$ given by $\pi_1(P,Q) = (X_0 : X_2)$, $\pi_2(P,Q) = (Y_0 : Y_2)$, and

$$\pi_3(P,Q) = (X_0Y_0 : X_1Y_1) = (X_2Y_0 : X_3Y_1) = (X_0Y_2 : X_1Y_3) = (X_2Y_2 : X_3Y_3),$$

where $(P,Q) = \big((X_0 : X_1 : X_2 : X_3), (Y_0 : Y_1 : Y_2 : Y_3)\big)$.

Under the Segre embedding $S : \mathscr{K}_1^2 \mapsto \mathbb{P}^3$, 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 $S(\mathscr{K}_1^2)$. The Segre embedding of $\mathscr{K}_2$ in $\mathbb{P}^7$ is cut out by the quadratic relation

$$T_0^2 - T_1^2 - T_2^2 + T_3^2 = T_4^2 - dT_5^2 - dT_6^2 + d^2T_7^2,$$

on the image of the Segre embedding of $(\mathbb{P}^1)^3 \to \mathbb{P}^7$, determined by:

$$\begin{gathered} T_0T_3 = T_1T_2,\ T_0T_5 = T_1T_4,\ T_0T_6 = T_2T_4, \\ T_0T_7 = T_3T_4,\ T_1T_6 = T_3T_4,\ T_1T_7 = T_3T_5, \\ T_2T_5 = T_3T_4,\ T_2T_7 = T_3T_6,\ T_4T_7 = T_5T_6. \end{gathered}$$

The morphism to $E^2 \to S(\mathscr{K}_2) \subseteq \mathbb{P}^7$ is determined by:

$$(X_0Y_0 : X_2Y_0 : X_0Y_2 : X_2Y_2, X_1Y_1 : X_3Y_1 : X_1Y_3 : X_3Y_3).$$

Proof. The quadratic relation for $\mathscr{K}_2$ in $\mathscr{K}_1^2 \times \mathbb{P}^1$:

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

follows by pulling back the relation to E^2 by

$$\pi^*(Y_1/Y_0) = (Y_2/Y_0),\ \pi^*(X_1/X_0) = (X_2/X_0),\ \pi^*(Z_1/Z_0)^2 = (X_1Y_1/X_0Y_0)^2.$$

Since the morphism maps through $E^2/\{\pm 1\}$, defines a double cover of $\mathscr{K}_1^2$, and is irreducible, we conclude that the quadratic relation determines $\mathscr{K}_2$. The remaining models follow by tracing this quadratic relation through the Segre embeddings.

The last model, in $\mathbb{P}^7$, can be interpreted as coming from the construction of Section 2, applied to the Segre embedding of E^2 in $\mathbb{P}^{15}$. The sixteen-dimensional space of global sections splits into two eight-dimensional subspaces, for which

$$\{X_0Y_0 : X_2Y_0 : X_0Y_2 : X_2Y_2, X_1Y_1 : X_3Y_1 : X_1Y_3 : X_3Y_3\}$$

forms a basis for the plus one eigenspace. The compatibility of the maps from E^2 is verified by projecting from the models in $\mathbb{P}^7$ and $\mathbb{P}^3 \times \mathbb{P}^1$ to $\mathscr{K}_1^2 \times \mathbb{P}^1$. □

The description of the maps in the previous theorem, together with the action of $[-1]$ on the Edwards model, implies the next corollary.

Corollary 1. *The automorphism $\sigma : E^2 \to E^2$ given by $(P, Q) \mapsto (Q, P)$ induces the automorphism of $\mathscr{K}_2$ in the respective models in $\mathscr{K}_1^2 \times \mathbb{P}^1$, $\mathbb{P}^3 \times \mathbb{P}^1$ and $\mathbb{P}^7$:*

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

$$\big((U_0 : U_1 : U_2 : U_3), (Z_0 : Z_1)\big) \mapsto \big((U_0 : U_2 : U_1 : U_3), (Z_0 : Z_1)\big),$$

$$(T_0 : T_1 : T_2 : T_3 : T_4 : T_5 : T_6 : T_7) \mapsto (T_0 : T_2 : T_1 : T_3 : T_4 : T_6 : T_5 : T_7).$$

The automorphism $\iota : \mathscr{K}_2 \to \mathscr{K}_2$ induced by the automorphisms $[-1] \times [1]$ and $[1] \times [-1]$ of E^2 is given by:

$$\big((X_0 : X_1), (Y_0 : Y_1), (Z_0 : Z_1)\big) \mapsto \big((X_0 : X_1), (Y_0 : Y_1), (Z_0 : -Z_1)\big),$$

$$\big((U_0 : U_1 : U_2 : U_3), (Z_0 : Z_1)\big) \mapsto \big((U_0 : U_1 : U_2 : U_3), (Z_0 : -Z_1)\big),$$

$$(T_0 : T_1 : T_2 : T_3 : T_4 : T_5 : T_6 : T_7) \mapsto (T_0 : T_1 : T_2 : T_3 : -T_4 : -T_5 : -T_6 : -T_7).$$

6 Endomorphisms of Kummer surfaces $\mathscr{K}_2$

We are now able to define polynomial maps for the Montgomery endomorphism φ, where ρ, τ, and φ are the endomorphisms

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

as elements of $\mathrm{M}_2(\mathbb{Z})/\{\pm 1\}$. In addition we recall the definitions

$$\iota = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ and } \sigma = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

and note the commuting relations $\rho \circ \iota = \sigma \circ \rho$ and $\rho \circ \sigma = \iota \circ \rho$ for ι, σ, and ρ.

Explicit polynomial maps for the Montgomery endomorphism φ on $\mathscr{K}_2$ follow from the identities

$$\varphi_0 = \varphi = \tau \circ \sigma\rho \text{ and } \varphi_1 = \sigma \circ \varphi \circ \sigma.$$

As a consequence the Montgomery ladder can be expressed in terms of the automorphisms σ, ι, and endomorphisms ρ and τ. The following two theorems, whose proof follows from standard addition laws on the Edwards model (see Bernstein and Lange [1], [2], Hisil [5], and Kohel [6]), and verification of the commutativity relations $\pi \circ \psi = \psi \circ \pi$ for an endomorphism ψ.

Theorem 2. *The projections of the endomorphisms $\rho : \mathscr{K}_2 \to \mathscr{K}_2$ are uniquely represented by polynomials of bidegree $(1,1)$, $(1,1)$, and $(2,0)$, explicitly:*

$$\begin{aligned}
\pi_1 \circ \rho\big((U_0 : U_1 : U_2 : U_3), (Z_0 : Z_1)\big) &= (U_0 Z_0 - dU_3 Z_1 : -U_0 Z_1 + U_3 Z_0) \\
\pi_2 \circ \rho\big((U_0 : U_1 : U_2 : U_3), (Z_0 : Z_1)\big) &= (U_0 Z_0 + dU_3 Z_1 : U_0 Z_1 + U_3 Z_0), \\
\pi_3 \circ \rho\big((U_0 : U_1 : U_2 : U_3), (Z_0 : Z_1)\big) &= (U_0^2 - dU_3^2 \ : \ -U_1^2 + U_2^2).
\end{aligned}$$

The projection $\rho : \mathscr{K}_2 \to S(\mathscr{K}_1^2)$ admits a two-dimensional space of polynomial maps of bidegree $(2,1)$ spanned by:

$$\begin{aligned}
\big(& U_0^2 - dU_1^2 - dU_2^2 + dU_3^2)Z_0 \ : \\
& -(d-1)U_0U_3Z_0 - (U_0^2 - dU_1^2 - dU_2^2 + d^2U_3^2)Z_1 \ : \\
& -(d-1)U_0U_3Z_0 + (U_0^2 - dU_1^2 - dU_2^2 + d^2U_3^2)Z_1 \ : \\
& -(U_0^2 - U_1^2 - U_2^2 + dU_3^2)Z_0 \ \big) \\
\big(& (U_0^2 - dU_1^2 - dU_2^2 + dU_3^2)Z_1 \ : \\
& -(d-1)U_0U_3Z_1 - (U_0^2 - U_1^2 - U_2^2 + U_3^2)Z_0 \ : \\
& -(d-1)U_0U_3Z_1 + (U_0^2 - U_1^2 - U_2^2 + U_3^2)Z_0 \ : \\
& -(U_0^2 - U_1^2 - U_2^2 + dU_3^2)Z_1\big).
\end{aligned}$$

Theorem 3. *The maps $\pi_i \circ \tau : \mathscr{K}_2 \to \mathscr{K}_1$ are given by*

$$\begin{aligned}
\pi_1 \circ \tau\big((U_0 : U_1 : U_2 : U_3), (Z_0 : Z_1)\big) &= (U_0 Z_0 - dU_3 Z_1 : -U_0 Z_1 + U_3 Z_0), \\
\pi_2 \circ \tau\big((U_0 : U_1 : U_2 : U_3), (Z_0 : Z_1)\big) &= (U_0 : U_2) = (U_1 : U_3).
\end{aligned}$$

and $\pi_3 \circ \tau\big((U_0 : U_1 : U_2 : U_3), (Z_0 : Z_1)\big)$ is given by the equivalent expressions

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

7 Conclusion

The above polynomial maps for Montgomery endomorphism φ of $\mathscr{K}_2$ allows one to carry out a simultaneous symmetric addition and doubling on the Kummer surface. Besides the potential efficiency of this computation, this provides a simple geometric description of the basic ingredient for the Montgomery ladder on an Edwards model of an elliptic curve. The symmetry of the derived model for the split Kummer surface, and the endomorphisms ι, σ, and ρ provide the tools necessary for scalar multiplication on Edwards curves in cryptographic applications requiring protection from side channel attacks.

References

1. D. J. Bernstein, T. Lange. Faster addition and doubling on elliptic curves. *Advances in Cryptology: ASIACRYPT 2007*, Lecture Notes in Computer Science, **4833**, Springer, 29–50, 2007.
2. D. J. Bernstein and T. Lange. A complete set of addition laws for incomplete Edwards curves, preprint, http://eprint.iacr.org/2009/580, 2009.
3. E. Brier and M. Joye, Weierstrass elliptic curves and side-channel attacks, *Public Key Cryptography*, *Lecture Notes in Comput. Sci.*, **2274**, 335–345, 2002.
4. H. Edwards. A normal form for elliptic curves. Bulletin of the American Mathematical Society, **44**, 393–422, 2007.
5. H. Hisil, K. K.-H. Wong, G. Carter, E. Dawson, Twisted Edwards curves revisited, *Advances in cryptology – ASIACRYPT 2008*, Lecture Notes in Computer Science, **5350**, Springer, Berlin, 326–343, 2008.
6. D. Kohel. Addition law structure of elliptic curves. to appear in *Journal of Number Theory*, http://arxiv.org/abs/1005.3623, 2011.
7. A Fast Parallel Elliptic Curve Multiplication Resistant against Side Channel Attacks, *Public Key Cryptography*, *Lecture Notes in Comput. Sci.*, **2274**, 280–296, 2002.
8. M. Joye and S.-M. Yen. The Montgomery Powering Ladder, CHES 2002, *Lecture Notes Comp. Sci.*, **2523**, 291–302, 2003.
9. H. Lange and W. Ruppert. Complete systems of addition laws on abelian varieties. *Invent. Math.*, **79** (3), 603–610, 1985.
10. P. Montgomery. Speeding the Pollard and elliptic curve methods of factorization, *Math. Comp.*, **48**, no. 177, 243–264, 1987.
11. D. Mumford. On the equations defining abelian varieties I, *Invent. Math.*, **1**, 287–354, 2966.