Halving differential additions on Kummer lines

Damien Robert, Nicolas Sarkis

HALVING DIFFERENTIAL ADDITIONS ON KUMMER LINES

DAMIEN ROBERT AND NICOLAS SARKIS

Abstract. We study differential additions formulas on Kummer lines that factorize through a degree 2 isogeny φ. We call the resulting formulas half differential additions: from the knowledge of $\varphi(P), \varphi(Q)$ and $P - Q$, the half differential addition allows to recover $P + Q$. We explain how Mumford's theta group theory allows, in any model of Kummer lines, to find a basis of the half differential relations. This involves studying the dimension 2 isogeny $(P, Q) \mapsto (P + Q, P - Q)$.

We then use the half differential addition formulas to build a new type of Montgomery ladder, called the half-ladder, using a time-memory trade-off. On a Montgomery curve with full rational 2-torsion, our half ladder first build a succession of isogeny images $P_i = \varphi_i(P_{i-1})$, which only depends on the base point P and not the scalar n, for a pre-computation cost of $2\mathbf{S} + 1\mathbf{m}_0$ by bit. Then we use half doublings and half differential additions to compute any scalar multiplication $n \cdot P$, for a cost of $4\mathbf{M} + 2\mathbf{S} + 1\mathbf{m}_0$ by bit. The total cost is then $4\mathbf{M} + 4\mathbf{S} + 2\mathbf{m}_0$, even when the base point P is not normalized. By contrast, the usual Montgomery ladder costs $4\mathbf{M} + 4\mathbf{S} + 1\mathbf{m} + 1\mathbf{m}_0$ by bit, for a normalized point.

In the appendix, we extend our approach to higher dimensional ladders in theta coordinates.

1. Introduction

1.1. **Motivation.** Elliptic curves are widely used in cryptography, from Diffie-Hellman key exchange (ECDH) to signature schemes (ECDSA), and are part of the TLS layer [Res18]. The efficiency of these protocols relies on the speed of scalar multiplications. Montgomery provided a method known as the Montgomery ladder [Mon87] that, given the x-coordinate $x(P)$ of a point P on a Montgomery curve, can compute $x(n \cdot P)$ for any integer n. This algorithm relies on two operations: differential addition — that is computing $x(P+Q)$ from $x(P)$, $x(Q)$ and $x(P-Q)$ — and doubling of a point, which are both efficient on a Montgomery curve. One perk of working only with the x-coordinate is that it saves storage and bandwidth, and since the ladder also computes $x((n+1) \cdot P)$, this enables one to recover $y(n \cdot P)$, hence the full point on the curve. We refer to the survey [CS18] for more details.

Working only with the x-coordinate amounts to identifying the points P and $-P$ on an elliptic curve E, and the correct object to study is the Kummer line $\mathcal{K} = E/\pm 1$ associated to the elliptic curve. In [RS24], the authors provided a framework on Kummer lines to derive efficient 2-isogenies formulas, yielding doubling formulas by composing with the dual isogeny. They also give a slightly modified version of the Montgomery ladder to benefit from slightly better doubling formulas on other models of Kummer lines while still using the usual differential addition formulas from Montgomery curves.

In this paper, we extend this framework to find differential addition formulas on models of Kummer lines, with a particular focus on formulas (called half differential additions) that factor through a 2-isogeny φ. The core idea is to re-use the computation of $\varphi(P)$ and $\varphi(Q)$ which happens during the doubling to also determine $P + Q$ on the Kummer line. A half doubling is the special case where $P = Q$, in which case we have $2 \cdot P = \widehat{\varphi}(\varphi(P))$, so half doubling amount

Date: October 7, 2024.

Key words and phrases. Elliptic curve cryptography, Differential addition, Montgomery ladder, Isogenies.

to applying the dual isogeny. Combined with a time/memory trade off to compute all needed isogeny images once, this leads to a new ladder — called half ladder — which is competitive with the Montgomery one. Instead of performing doublings and differential additions at the same time, we first pre-compute images of our base point P via 2-isogenies $\varphi_1, \dots, \varphi_\ell$, and we then go backwards with duals and half differential addition formulas to recover $n \cdot P$. A comparison is available in Table 1 below. We stress that the half ladder formulas cost that we give are only available on Montgomery curves with full rational two torsion, whereas the standard ladder formulas are available on all Montgomery curve. On the other hand, for these curves, our half ladder allows us to gain a $1\mathbf{m}_0 - 1\mathbf{m}$ trade-off on a normalized base point P, and a $1\mathbf{m}_0 - 2\mathbf{M}$ trade-off on a non normalized base point.

	Montgomery ladder	Half ladder, our contribution
Non-normalized base point	$6\mathbf{M} + 4\mathbf{S} + 1\mathbf{m}_0$	$4\mathbf{M} + 4\mathbf{S} + 2\mathbf{m}_0$
Normalized base point	$4\mathbf{M} + 4\mathbf{S} + 1\mathbf{m} + 1\mathbf{m}_0$	

TABLE 1. Ladder costs per bit with no pre-computation

Similarly to what was done in [RS24], we use Mumford's theta group theory to prove the existence of formulas and to determine them. If $\varphi : E \to E'$ is a 2-isogeny on elliptic curves, we relate sections above the divisor $2(\mathcal{O}_{E'}) * 2(\mathcal{O}_{E'})$ of $E' \times E'$ compatible with the diagonal isogeny $\Phi = (\varphi, \varphi)$ with sections above the divisor $2(\mathcal{O}_E) * 2(\mathcal{O}_E)$ of $E \times E$ compatible with the differential addition isogeny $F : (P, Q) \mapsto (P + Q, P - Q)$. Generators of the relations between the sections are what we call half differential addition formulas.

1.2. **Related work.** In [Oli+17, Alg. 4], the authors provide a variant of the Montgomery ladder, performing the operation from right-to-left (RtL), instead of the traditional left-to-right (LtR). This approach implies a pre-computation of points of the form $2^i \cdot P$. Since our half ladder also contains a form of pre-computation, it is more relevant to compare to this version. Tables 2 and 3 compare the pre-computation of Montgomery ladder right-to-left and our half ladder with our best formulas, which happens over a Montgomery curve with full rational 2-torsion. It appears that on each step we lose $1\mathbf{m}_0$, but our pre-computation is significantly faster in both cases, saving $2\mathbf{M}$. Moreover, our approach generalizes well in higher dimension as explained in Appendix A, whereas the natural generalization of the RtL ladder is not interesting, to the best of our knowledge, in dimension $g > 1$.

Algorithm	Pre-computation	Step
Montgomery ladder LtR	—	$4\mathbf{M} + 4\mathbf{S} + 1\mathbf{m} + 1\mathbf{m}_0$
Montgomery ladder RtL	$2\mathbf{M} + 2\mathbf{S} + 1\mathbf{m}_0$	$4\mathbf{M} + 2\mathbf{S}$
Half ladder, our contribution	$2\mathbf{S} + 1\mathbf{m}_0$	$4\mathbf{M} + 2\mathbf{S} + 1\mathbf{m}_0$

TABLE 2. Ladder costs per bit with a pre-computation but no normalization

[1] n inversions can be reduced to $1\mathbf{I} + (3n - 3)\mathbf{M}$ thanks to Montgomery's trick, see [SB01, Lem. 3.1]

Algorithm	Pre-computation	Normalization[1]	Step
Montgomery Ladder LtR	—	—	$4\mathbf{M} + 4\mathbf{S} + 1\mathbf{m} + 1\mathbf{m}_0$
Montgomery Ladder RtL	$2\mathbf{M} + 2\mathbf{S} + 1\mathbf{m}_0$	$1\mathbf{I} + 1\mathbf{M} \overset{\text{asy}}{=} 4\mathbf{M}$	$3\mathbf{M} + 2\mathbf{S}$
Half ladder, our contribution	$2\mathbf{S} + 1\mathbf{m}_0$	$1\mathbf{I} + 1\mathbf{M} \overset{\text{asy}}{=} 4\mathbf{M}$	$3\mathbf{M} + 2\mathbf{S} + 1\mathbf{m}_0$

TABLE 3. Ladder costs per bit when normalizing the pre-computation

1.3. **Our contributions.** In summary, our contributions are first a systematic way to derive half differential addition formulas using Mumford's theory of the theta group, and secondly the existence of a new kind of pre-computed Montgomery like ladder: the half ladder.

As described in more details in Section 4, the key principle behind the half ladder is as follows. Using half doubling and half differential addition formulas, one way to compute the usual Montgomery ladder, is at each step to start with $U_{i-1} = m_{i-1} \cdot P, V_{i-1} = (m_{i-1} + 1) \cdot P$, compute $\varphi(U_{i-1}), \varphi(V_{i-1})$, and use one half doubling and one half differential addition to recover $2U_i, U_i + V_i$ (or $U_i + V_i, 2V_i$ depending on the current bit). This costs two isogeny images, one half doubling, and one half differential addition by steps.

Our idea, is that rather than interleaving the isogeny images and half doublings and differential additions at each step, we can instead pre-compute several iterated isogeny images P_i (pre-computation which only depend on the base point and bit length of the scalar m), and then "unstack" these images at each step by doing one half doubling and one half differential addition. The key point in changing the order, is that one of the two isogeny images we need to compute is the image of the neutral point $\mathcal{O}$, which is "free". This help us save one isogeny image by bit, at the cost of a slightly more expensive half differential addition, because the differences will be given by the isogeny images P_i rather than by the same base point P, hence are not normalized any more even if P was.

We provide an implementation at `https://gitlab.inria.fr/nsarkis/half-diff-add`. An alternative, more experimental, implementation is also available at `https://gitlab.inria.fr/roberdam/kummer-line`.

1.4. **Notations.** We will use the following notations for computational costs:

- $\mathbf{I}$ is a generic inversion,
- $\mathbf{M}$ is a generic multiplication,
- $\mathbf{S}$ is a generic squaring,
- $\mathbf{m}_0$ is a multiplication by a curve constant,
- $\mathbf{m}$ is specific to Montgomery ladder and designate a multiplication by the base point coordinates. It can represent $2\mathbf{M}$ (for a non normalized point) or $1\mathbf{M}$ for a normalized point, depending on the context.

1.5. **Roadmap.** In Section 2, we introduce our terminology, in particular sections of a divisor, Weierstrass coordinates and Kummer lines. In Section 3, we discuss the main isogeny of interest of this article, $F : (P, Q) \mapsto (P + Q, P - Q)$, and we define half differential addition formulas. Assuming we have explicit half differential addition formulas, we then introduce our half ladder in Section 4. Finally, Section 5 details Mumford's theta group theory and how to find these half differential addition formulas in practice, altogether with an example. In Appendix A, we extend the half ladder to abelian varieties in the level 2 theta model. In Appendix B, we use the context of `Curve25519` as another example to find half differential addition formulas.

2. Preliminaries

In this whole article, k is a perfect field of characteristic different from 2. We recall in this section some results and tools introduced in [RS24].

2.1. **Weierstrass coordinates.** Let E/k be an elliptic curve given by an affine short Weierstrass equation $y^2 = x^3 + a_2x^2 + a_4x + a_6$. Let D be a divisor on E, we recall that a local section on a Zariski open U of E is a function $s \in k(E)$ from the function field $k(E)$ of E such that $\operatorname{div} s_{|U} + D_{|U} \geq 0$. The set of local sections associated to D on U is denoted by $\Gamma(U, D)$, or $\Gamma(D)$ when $U = E$ and in that case we say that $s \in \Gamma(D)$ is a global section. We finally denote by $\mathfrak{O}_E(D)$ the line bundle associated to D; this is the sheaf given by the local sections of D, i.e. $\mathfrak{O}_E(D)(U) = \Gamma(U, D)$ on a Zariski open U. It is convenient to work with projective coordinates to avoid divisions, which is naturally given by the line bundle point of view; the elliptic curve has a projective equation $Y^2Z = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$ in $\mathbb{P}^2$.

Let $D_n = n(\mathcal{O}_E)$, we have $\Gamma(D_1) = \langle Z_0 \rangle$, $\Gamma(D_2) = \langle X_0, Z_0^2 \rangle$, $\Gamma(D_3) = \langle X_0Z_0, Y, Z_0^3 \rangle$, the projective coordinates are $X = X_0Z_0$ and $Z = Z_0^3$. Notice that the affine coordinate $x = X/Z$ verifies $x = X_0/Z_0^2$. Since we are only interested in models of Kummer lines in this paper, we will change notations and denote $\Gamma(D_2) = \langle X, Z \rangle$, where $Z = Z_0^2$. With this notation, the full projective Weierstrass coordinates are XZ_0, Y, ZZ_0, and the affine coordinate verifies $x = XZ_0/ZZ_0 = X/Z$.

It will be convenient to work with models of Kummer lines where the neutral point is not at infinity. If $(X : Z)$ are projective Weierstrass coordinates, this amounts to allow working with the projective coordinates $(X' : Z') = (aX + bZ : cX + dZ)$. We remark that X', Z' are still sections of the line bundle $\mathfrak{O}_E(D_2)$.

2.2. **Kummer lines.** Let E be an elliptic curve defined over k. If E is in short Weierstrass form, then the map $E \to \mathbb{P}^1, (x, y) \mapsto (x : 1), \mathcal{O}_E \mapsto \infty$ is a degree 2 cover with ramification at the 2-torsion $E[2]$ of the elliptic curve E. This also yields an isomorphism of curves $E/\pm 1 \simeq \mathbb{P}^1$. A Kummer line is a generalization of this construction.

Definition 2.1. *A Kummer line is a degree 2 covering $\pi : E \to \mathbb{P}^1$ with 4 distinct ramification points, one of which is rational and marked:*

$$\exists \mathcal{O} \in E(k), \exists T_1, T_2, T_3 \in E \text{ with } \#\pi^{-1}(\pi(P)) = \begin{cases} 1 & \text{if } P \in \{\mathcal{O}, T_1, T_2, T_3\}, \\ 2 & \text{otherwise.} \end{cases}$$

This is equivalent to having a degree 2 cover $\pi : E \to \mathbb{P}^1$ with exactly 4 ramification points, one of which is marked. E is then an elliptic curve thanks to Riemann-Hurwitz formula, and it can be shown that the ramification corresponds to the 2-torsion and that the fibres are given by $\pi^{-1}(\pi(P)) = \{-P, P\}$.

Kummer lines will be described only by their ramification like in Example 2.2 below. They will usually be denoted by $\mathcal{K}$ where $\mathcal{K} \simeq \mathbb{P}^1$, and we will forget about the π notation when it is not ambiguous, we will then write $[P] = \pi(P)$ where $P \in E$. Similarly, since this whole article covers arithmetic of Kummer lines, we may drop the bracket notation and write $P, Q \in \mathcal{K}$, as well as $P + Q$ even though there is no addition law on $\mathcal{K}$.

Example 2.2. *The marked point is denoted with a $*$. If the ramification on the Kummer line is given by*

$$(1 : 0)^*, \qquad (\alpha_1 : 1), \qquad (\alpha_2 : 1), \qquad (\alpha_3 : 1),$$

with the α_i potentially defined over an extension of k, then the corresponding elliptic curve has equation, with some $\beta \in k$:

$$E : \beta y^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3). \tag{1}$$

Conversely, starting from Eq. (1)*, if the point at infinity is denoted* $\mathcal{O}$*, then the following map is a degree* 2*-covering with* 4 *ramification points which correspond to the* 2*-torsion:*

$$\pi : E \to \mathbb{P}^1, (x, y) \mapsto (x : 1), \mathcal{O} \mapsto \infty.$$

The addition law does not hold any more on the Kummer line, however there exists differential addition formulas that, given $[P]$, $[Q]$ and $[P - Q]$, return $[P + Q]$. They are our main focus in this article.

Lemma 2.3 (Translation by a 2-torsion point)**.** *Let* E *be an elliptic curve with a rational* 2*-torsion point* $T \in E[2](k)$ *and* $\pi : E \to \mathbb{P}^1$ *a Kummer line. Then the translation by* T *map* $t_T : \pi(P) \mapsto \pi(P + T)$ *is well-defined and is a homography on* $\mathbb{P}^1$*.*

Proof. Since $T = -T$, if $P, Q \in E$ with $P = \pm Q$ then $\pi(P + T) = \pi(Q + T)$, hence the map $P \mapsto \pi(P + T)$ factors through π and t_T is well-defined and is a morphism of $\mathbb{P}^1$ because the translation on E is a morphism of algebraic curves. It is bijective because the translation on E is surjective and if $\pi(P + T) = \pi(Q + T)$ then $\pi(P) = \pi(Q)$ since T is a 2-torsion point. Therefore, t_T is a homography. □

Understanding how t_T acts on the coordinates X and Z will be essential in Section 5. It also helps to determine the 4-torsion on a Kummer line. We end this part by giving some models we will be studying in the sequel.

Example 2.4.

(1) The Kummer line associated to a Montgomery curve $\beta y^2 = x(x^2 + \mathcal{A}x + 1)$ *has the following ramification:*

$$(1 : 0)^*, \qquad (0 : 1), \qquad (a : b), \qquad (b : a),$$

where $\mathcal{A} = -\frac{a}{b} - \frac{b}{a}$*.* $\frac{a}{b}$ *may not be rational, however we always have* $\mathcal{A} \in k$*. We denote it* $M(a : b)$*. There is a rational* 4*-torsion point* $[T'] = (1 : 1)$ *and* $(-1 : 1)$ *above* $[T] = (0 : 1)$*. (Indeed, because* $3T' = T' + T = -T'$ *on the curve, we can find* $[T']$ *via the equation* $t_T([T']) = [T']$*, which becomes* $(X_0 : Z_0) = (Z_0 : X_0)$ *on the Montgomery line).*

(2) Let $\frac{a}{b} \in k$*, the theta model* $\theta(a : b)$ *has the following ramification points:*

$$(a : b)^*, \qquad (-a : b), \qquad (b : a), \qquad (-b : a).$$

The translation by $T = (-a : b)$ *is given by* $t_T : (X : Z) \mapsto (-X : Z)$*, there are* 4*-torsion points above* $(-a : b)$ *given by* $(1 : 0)$ *and* $(0 : 1)$*, as well as above* $(b : a)$ *given by* $(1 : 1)$ *and* $(-1 : 1)$*.*

(3) Let $\frac{a}{b} \in k$*, the theta squared model* $\theta_s(a : b)$ *has the following ramification points:*

$$(a : b)^*, \qquad (b : a), \qquad (1 : 0), \qquad (0 : 1).$$

The translation by $T = (b : a)$ *is* $t_T : (X : Z) \mapsto (Z : X)$ *and the* 4*-torsion above* T *is given by* $(1 : 1)$ *and* $(-1 : 1)$*. Given the shape of the ramification, it is isomorphic to* $M(a : b)$ *via the involution* $(X : Z) \mapsto (aX - bZ : bX - aZ)$*.*

(4) Let $\frac{a}{b} \in k$*, the theta twisted model* $\theta_t(a : b)$ *has the following ramification points:*

$$(a : b)^*, \qquad (-a : b), \qquad (1 : 1), \qquad (-1 : 1).$$

The translation by $T = (-a : b)$ *is* $t_T : (X : Z) \mapsto (-X : Z)$ *and the* 4*-torsion above* T *is given by* $(1 : 0)$ *and* $(0 : 1)$*. It is isomorphic to* $\theta_s(a' : b')$ *via the Hadamard transform* $H : (X : Z) \mapsto (X + Z : X - Z)$ *where* $(a' : b') = (a + b : a - b)$*, and therefore to* $M(a' : b')$*. The isomorphism to the Montgomery model* $M(a' : b')$ *is given by* $(X : Z) \mapsto (b'X + a'Z : a'Z - b'X)$*. Its inverse is* $(X : Z) \mapsto (a(X - Z) : b(X + Z))$*. Hence, a Montgomery curve has a theta squared or equivalently a theta twisted model if and only if it has full rational* 2*-torsion.*

Remark 2.5. *The names theta squared and theta twisted come from the fact that given a theta model $\theta(a:b)$, there is a 2-isogeny $f:\theta(a:b)\to\theta_s(a^2:b^2)$ given by $f:(X:Z)\mapsto(X^2:Z^2)$ and an isomorphism $g:\theta(a:b)\to\theta_t(a^2:b^2)$ given by $g:(X:Z)\mapsto(aX:bZ)$.*

3. Half differential addition

Doubling formulas on Kummer lines are essential to perform scalar multiplication. One natural way to find such formulas is by computing a 2-isogeny $\varphi:E\to E'$ and compose it with its dual $\widetilde{\varphi}$ such that $[2]=\widetilde{\varphi}\circ\varphi$. This decomposition is often more efficient, as computing directly the doubling — which is a degree 4 isogeny — can be slower than splitting it into two degree 2 isogenies. [RS24] discusses how to find such formulas on Kummer lines.

The other important operation on a Kummer line is the differential addition. In this section we study the map

$$F:E\times E\to E\times E,\ (P,Q)\mapsto(P+Q,P-Q).$$

It is a $(2,2)$-isogeny with kernel $K_F=\{(T,T)\mid T\in E[2]\}$, the diagonal of the 2-torsion. Having formulas for F yields differential addition ones. Similarly to the case of doubling with 2-isogenies, we would like to factor it.

Let $\varphi:E\to E'$ be a 2-isogeny with kernel $\{\mathcal{O}_E,T\}$. We will consider the $(2,2)$-diagonal isogeny

$$\Phi:E\times E\to E'\times E',\ (P,Q)\mapsto(\varphi(P),\varphi(Q)),$$

its kernel is $K_\Phi=\langle T\rangle\times\langle T\rangle$. Ideally, one would like to factor F through Φ, unfortunately this is not possible because there is no inclusion of the kernels, in fact $K_F\cap K_\Phi=\{(\mathcal{O}_E,\mathcal{O}_E),(T,T)\}$.

Definition 3.1. *Let $\varphi:E\to E'$ be a 2-isogeny of elliptic curves, $\mathcal{K}$ and $\mathcal{K}'$ the Kummer lines corresponding respectively to E and E', $P,Q\in E$. Formulas that can recover $[P+Q]\in\mathcal{K}$ from the data of $[\varphi(P)],[\varphi(Q)]\in\mathcal{K}'$ and $[P-Q]\in\mathcal{K}$ will be called half differential addition formulas. We will denote such algorithm* $\texttt{HalfDiffAdd}_\varphi(\varphi(P),\varphi(Q),P-Q)$.

If we have $\varphi(P)$, applying the contragedient isogeny $\widetilde{\varphi}$ to it yields $2\cdot P=\widetilde{\varphi}\circ\varphi(P)$. By analogy with the half differential additions, we will also denote this operation as $2\cdot P=\texttt{HalfDouble}_\varphi(\varphi(P))$.

In Section 5 we will explain how to find explicit half differential formulas using the theta group theory. We will first discuss an application of such formulas to build a half ladder in Section 4.

4. Ladders

In this section, assuming we know how to compute half differential addition formulas — which will be discussed in Section 5 —, we explain how to build a new ladder based on those, and we compare it to the Montgomery one.

4.1. The Montgomery ladder.

We first recall some results about the Montgomery ladder, introduced in [Mon87]. Given a Kummer line $\mathcal{K}$ with differential addition and doubling formulas, one can compute $n\cdot P\in\mathcal{K}$ for any $n\in\mathbb{Z}$, $P\in\mathcal{K}$ using Algorithm 1. It is clear that each step of the ladder costs exactly one differential addition and one doubling. Table 4 gives the cost of these on the models discussed in this article, as well as the total Montgomery ladder cost.

The $1\mathbf{m}$ in the differential addition corresponds to the multiplication by the base point P coordinates. Depending on the context, this multiplication could be either $2\mathbf{M}$ if the point is generic and not normalized or $1\mathbf{M}$ if the point is generic and normalized (for instance while recovering the shared secret key during a key exchange). In the best case scenario, this point is set in the protocol and has a small coordinate, in that case $1\mathbf{m}$ reduces to $1\mathbf{m}_0$, this can happen for instance in a signature scheme or the first step of a key exchange.

	Montgomery curve [Mon87]	Theta model [GL09, § 6.2]	Theta squared / twisted [GL09, § 6.2, Thm. 2]
Diff. add.	$2\mathbf{M} + 2\mathbf{S} + 1\mathbf{m}$	$2\mathbf{M} + 4\mathbf{S} + 1\mathbf{m} + 1\mathbf{m}_0$	$2\mathbf{M} + 2\mathbf{S} + 1\mathbf{m} + 1\mathbf{m}_0$
Doubling	$2\mathbf{M} + 2\mathbf{S} + 1\mathbf{m}_0$	$4\mathbf{S} + 2\mathbf{m}_0$	$4\mathbf{S} + 2\mathbf{m}_0$
Total cost	$4\mathbf{M} + 4\mathbf{S} + 1\mathbf{m} + 1\mathbf{m}_0$	$2\mathbf{M} + 8\mathbf{S} + 1\mathbf{m} + 3\mathbf{m}_0$	$2\mathbf{M} + 6\mathbf{S} + 1\mathbf{m} + 3\mathbf{m}_0$

TABLE 4. Montgomery ladder cost on several Kummer lines

Remark 4.1. *The Montgomery ladder on theta squared / twisted models was slightly improved in [RS24, § 5] via a hybrid ladder combining differential addition of Montgomery curves and theta doubling, saving* $1\mathbf{m}_0$ *for a total cost of* $2\mathbf{M} + 6\mathbf{S} + 1\mathbf{m} + 2\mathbf{m}_0$.

Algorithm 1: Scalar multiplication with the Montgomery ladder

Input: $n = (1, b_{\ell-2}, \ldots, b_0)$ an ℓ-bits integer, P a point on $\mathcal{K}$
Output: $n \cdot P$

```
Function MontgomeryLadder(n, P):
    U ← P;
    V ← Doubling(P);
    for i ← ℓ − 2 to 0 do
        if b_i = 0 then
            V ← DiffAdd(U, V, P);
            U ← Doubling(U);
        else if b_i = 1 then
            U ← DiffAdd(U, V, P);
            V ← Doubling(V);
    end
    return U;
```

As discussed in the introduction, there is a variant of the Montgomery ladder including pre-computations described in [Oli+17, Alg. 4]. The authors give an algorithm going through the binary decomposition of n from right-to-left (RtL), whereas Algorithm 1 goes from left-to-right (LtR). The main difference is that for each bit, only one differential addition is needed, given the pre-computation of the points $P_i = 2^i \cdot P$. However, the difference of the points U and V involved in the differential addition in their algorithm is stored in an accumulator and can change throughout the algorithm, hence a differential addition costs $4\mathbf{M} + 2\mathbf{S}$. By going further with the pre-computation by normalizing the points P_i, the differential addition can be reduced to $3\mathbf{M} + 2\mathbf{S}$, this corresponds to the discussion in Section 5.2 of their article. To summarize:

- The Montgomery ladder right-to-left requires the pre-computation of points $2^i \cdot P_i$, at the cost of one doubling per bit, which is $2\mathbf{M} + 2\mathbf{S} + 1\mathbf{m}_0$.
- If for each $P_i = (X_i : Z_i)$, we further pre-compute a constant $\mu_i = \frac{X_i + Z_i}{X_i - Z_i}$, the cost per bit in the main loop is the one of a differential addition performed in $3\mathbf{M} + 2\mathbf{S}$. This pre-computation is $1\mathbf{I} + 1\mathbf{M}$ per bit, which can be reduced to $4\mathbf{M}$ asymptotically thanks to Montgomery's trick, see [SB01, Lem. 3.1].
- Otherwise, each differential addition is performed in $4\mathbf{M} + 2\mathbf{S}$.

$$\mathcal{K}_0 \xrightarrow{\varphi_1} \mathcal{K}_1 \xrightarrow{\varphi_2} \cdots \xrightarrow{\varphi_\ell} \mathcal{K}_\ell$$

$$P_0 \longmapsto P_1 \longmapsto \cdots \longmapsto P_\ell$$

FIGURE 1. Half ladder context

The two situations are described in Tables 2 and 3 at the beginning of the article. Since our approach also involves pre-computations, we will also compare to this version of the Montgomery ladder.

4.2. **Half ladder.**

4.2.1. *Principle.* We will work in the following context, we want to compute $n \cdot P_0$ where n is an ℓ-bit integer and P_0 is a point on the Kummer line $\mathcal{K}_0$. The i-th bit of n is written b_i. Assume we have Kummer lines $\mathcal{K}_1, \dots, \mathcal{K}_\ell$ and 2-isogenies $\varphi_1, \dots, \varphi_\ell$ where $\varphi_i : \mathcal{K}_{i-1} \to \mathcal{K}_i$ for $1 \le i \le \ell$. We also denote $P_i = \varphi_i(P_{i-1})$. The situation is represented in Fig. 1. In practice, we will simply use a 2-isogeny $\varphi : \mathcal{K}_0 \to \mathcal{K}_1$ and its dual $\widetilde{\varphi}$ iteratively: $\varphi_{2i} = \varphi$ and $\varphi_{2i+1} = \widetilde{\varphi}$.

Finally, we assume that for each isogeny φ_i, we have half differential addition formulas which given $\varphi_i(P)$, $\varphi_i(Q)$ and $P - Q$, computes $P + Q$ on the Kummer line $\mathcal{K}_{i-1}$. We will denote such algorithm $\texttt{HalfDiffAdd}_{\varphi_i}(\varphi_i(P), \varphi_i(Q), P - Q)$.

The main idea is that instead of computing at each step the doubling of a point via a 2-isogeny and its dual as well as the differential addition of these two points, we will first pre-compute every image $P_1, \dots, P_\ell$ of our base point $P = P_0$, and then go backwards with half doublings and half differential addition formulas.

Assume on Kummer line $\mathcal{K}_i$, we know $U_i = u_i \cdot P_i$ and $V_i = (u_i + 1) \cdot P_i$, with $1 \le i \le \ell$. In particular, because $P_i = \varphi_i(P_{i-1})$, we have $U_i = \varphi_i(u_i \cdot P_{i-1})$ and $V_i = \varphi_i((u_i + 1) \cdot P_{i-1})$. With the knowledge of P_{i-1}, using $\texttt{HalfDiffAdd}_{\varphi_i}(U_i, V_i, P_{i-1})$, we can compute $(2u_i + 1) \cdot P_{i-1}$. With the dual $\widetilde{\varphi}_i$, we can also compute either $2u_i \cdot P_{i-1} = \widetilde{\varphi}_i(U_i)$ or $2(u_i + 1) \cdot P_{i-1} = \widetilde{\varphi}_i(V_i)$. We set $u_{i-1} = 2u_i + b_{i-1}$ such that we can recover $U_{i-1} = u_{i-1} \cdot P_{i-1}$ and $V_{i-1} = (u_{i-1} + 1) \cdot P_{i-1}$ using one computation with $\texttt{HalfDiffAdd}_{\varphi_i}$ and one with $\widetilde{\varphi}_i$, i.e. $\texttt{HalfDouble}_{\varphi_i}$.

With the initial situation being $U_\ell = \mathcal{O}_\ell$ the neutral element on $\mathcal{K}_\ell$ and $V_\ell = P_\ell$, this process can be iterated and one can derive the formula $u_i = b_{\ell-1}2^{\ell-1-i} + b_{\ell-2}2^{\ell-2-i} + \cdots + b_i 2^0$ for all $0 \le i < \ell$. A corollary is that $u_0 = n$ and consequently $U_0 = n \cdot P_0$, which is the point we were looking for. The generic algorithm is described in Algorithm 2.

In terms of cost, we first need to compute the images via $\varphi_1, \dots, \varphi_\ell$, then when going backwards we require a computation with each $\widetilde{\varphi}_1, \dots, \widetilde{\varphi}_\ell$ and one $\texttt{HalfDiffAdd}_{\varphi_i}$ for all $1 \le i \le \ell$. Similarly to the Montgomery right-to-left ladder, we could pre-compute when possible the images, and even normalize them if this is meaningful, depending on the context. We will look at an example in the following section.

4.2.2. *Application to theta model.* In this section, we focus on the theta model $\theta(a : b)$ described in Example 2.4.2 and given by ramification points

$$(a : b)^*, \qquad (-a : b), \qquad (b : a), \qquad (-b : a),$$

where $\frac{a}{b} \in k$. We will start with the case where there is a 8-torsion point $(r : s)$ above $(-a : b)$. As seen in [RS24, Ex. B.4], if $(A : B) := (r^2 + s^2 : r^2 - s^2)$, then $(A^2 : B^2) = (a^2 + b^2 : a^2 - b^2)$ and the following 2-isogeny ends on the theta model $\theta(A : B)$:

$$\varphi : (X : Z) \in \theta(a : b) \mapsto (B(X^2 + Z^2) : A(X^2 - Z^2)).$$

Algorithm 2: Scalar multiplication with the half ladder

Input: $n = (b_{\ell-1}, b_{\ell-2}, \dots, b_0)$ an ℓ-bits integer, P a point on $\mathcal{K}_0$
Output: $n \cdot P$
Data: $\mathcal{K}_i$ is a Kummer line, $\varphi_i : \mathcal{K}_{i-1} \to \mathcal{K}_i$ a 2-isogeny for $1 \le i \le \ell$

Function `HalfLadder`(n, P)**:**
  $P_0 \leftarrow P$;
  for $i \leftarrow 1$ **to** ℓ **do** `// Potentially a pre-computation`
    $P_i \leftarrow \varphi_i(P_{i-1})$;
  end
  $U \leftarrow \mathcal{O}_\ell$; `// Neutral point on` $\mathcal{K}_\ell$
  $V \leftarrow P_\ell$;
  for $i \leftarrow \ell$ **to** 1 **do**
    if $b_{i-1} = 0$ **then**
      $V \leftarrow \texttt{HalfDiffAdd}_{\varphi_i}(U, V, P_{i-1})$;
      $U \leftarrow \texttt{HalfDouble}_{\varphi_i}(U)$;
    else if $b_{i-1} = 1$ **then**
      $U \leftarrow \texttt{HalfDiffAdd}_{\varphi_i}(U, V, P_{i-1})$;
      $V \leftarrow \texttt{HalfDouble}_{\varphi_i}(V)$;
  end
  return U;

Its dual is simply given by $\widetilde{\varphi} : (X : Z) \in \theta(A : B) \mapsto (b(X^2 + Z^2) : a(X^2 - Z^2))$.

To build our half ladder, if n is an ℓ-bit integer, we set $\mathcal{K}_{2i} = \theta(a : b)$, $\mathcal{K}_{2i+1} = \theta(A : B)$, and $\varphi_{2i} = \widetilde{\varphi}$, $\varphi_{2i+1} = \varphi$ for $0 \le 2i, 2i+1 \le \ell$. The framework of Section 5 gives the following half differential addition formulas, where $(R, S) = (P + Q, P - Q)$:

- $\texttt{HalfDiffAdd}_{\varphi}(\varphi(P), \varphi(Q), S)$ $(P, Q \in \theta(a : b))$:
$$(X_R X_S : Z_R Z_S) = \begin{pmatrix} X_{\varphi(P)} X_{\varphi(Q)} + Z_{\varphi(P)} Z_{\varphi(Q)} \\ X_{\varphi(P)} X_{\varphi(Q)} - Z_{\varphi(P)} Z_{\varphi(Q)} \end{pmatrix}.$$
- $\texttt{HalfDiffAdd}_{\widetilde{\varphi}}(\widetilde{\varphi}(P), \widetilde{\varphi}(Q), S)$ $(P, Q \in \theta(A : B))$:
$$(X_R X_S : Z_R Z_S) = \begin{pmatrix} X_{\widetilde{\varphi}(P)} X_{\widetilde{\varphi}(Q)} + Z_{\widetilde{\varphi}(P)} Z_{\widetilde{\varphi}(Q)} \\ X_{\widetilde{\varphi}(P)} X_{\widetilde{\varphi}(Q)} - Z_{\widetilde{\varphi}(P)} Z_{\widetilde{\varphi}(Q)} \end{pmatrix}.$$

Each operation has the following cost:

- A φ evaluation is $2\mathbf{S} + 1\mathbf{m}_0$, as well as a $\widetilde{\varphi}$ evaluation.
- A half differential addition with respect to φ is $4\mathbf{M}$, as well as a half differential addition with respect to $\widetilde{\varphi}$. We can save $1\mathbf{M}$ by normalizing the points $P_1, \dots, P_\ell$.

The costs are completely symmetric whether we work with φ or $\widetilde{\varphi}$, hence an image is $2\mathbf{S} + 1\mathbf{m}_0$ and a half differential addition is $4\mathbf{M}$. This leads to the following costs per bit:

- If we do not perform any sort of pre-computation, the cost per bit is $4\mathbf{M} + 4\mathbf{S} + 2\mathbf{m}_0$, which is the best case scenario of Montgomery ladder left-to-right on a Montgomery curve where the base point is normalized and has a small x-coordinate, and is in general better than the Montgomery ladder left-to-right on a theta squared model.
- If we pre-compute the images $P_1, \dots, P_\ell$ but we don't normalize them, the pre-computation costs $2\mathbf{S} + 1\mathbf{m}_0$ per bit, and the main loop is $4\mathbf{M} + 2\mathbf{S} + 1\mathbf{m}_0$. The pre-computation saves $2\mathbf{M}$ over Montgomery ladder right-to-left whereas the main loop loses $1\mathbf{m}_0$.

- If we moreover normalize the pre-computed points, the pre-computation cost raises to $4\mathbf{M} + 2\mathbf{S} + 1\mathbf{m}_0$ thanks to Montgomery trick, and the main loop is then $3\mathbf{M} + 2\mathbf{S} + 1\mathbf{m}_0$. The difference with the Montgomery ladder left-to-right is the same as above, saving $2\mathbf{M}$ on the pre-computation but losing $1\mathbf{m}_0$ in the main loop.

If one wants to work with a theta model with no additional assumptions, the isogenies can be chosen differently. We still set $(A^2 : B^2) = (a^2 + b^2 : a^2 - b^2)$. The 2-isogeny given by $\varphi : (X : Z) \in \theta(a : b) \mapsto (X^2 : Z^2)$ ends on the theta squared model $\theta_s(a^2 : b^2)$ with ramification

$$(a^2 : b^2)^*, \qquad (b^2 : a^2), \qquad (1 : 0), \qquad (0 : 1).$$

The dual isogeny is then

$$\widetilde{\varphi} : (X : Z) \in \theta_s(a^2 : b^2) \mapsto (b(B^2(X+Z)^2 + A^2(X-Z)^2) : a(B^2(X+Z)^2 - A^2(X-Z)^2)).$$

The isogenies were computed using [RS24, Ex. B.3] and the isomorphism between Montgomery model and theta squared model from Example 2.4.3.

If n is an ℓ-bit integer, we set $\mathcal{K}_{2i} = \theta(a : b)$, $\mathcal{K}_{2i+1} = \theta_s(a^2 : b^2)$ for $0 \leq 2i, 2i+1 \leq \ell$, and $\varphi_{2i} = \widetilde{\varphi}$, $\varphi_{2i+1} = \varphi$. The differential addition formulas are the following according to Section 5.4, where $(R, S) = (P + Q, P - Q)$:

- $\texttt{HalfDiffAdd}_{\varphi}(\varphi(P), \varphi(Q), S)$:

$$(X_R X_S : Z_R Z_S) = \begin{pmatrix} B^2(X_{\varphi(P)} + Z_{\varphi(P)})(X_{\varphi(Q)} + Z_{\varphi(Q)}) + A^2(X_{\varphi(P)} - Z_{\varphi(P)})(X_{\varphi(Q)} - Z_{\varphi(Q)}) \\ B^2(X_{\varphi(P)} + Z_{\varphi(P)})(X_{\varphi(Q)} + Z_{\varphi(Q)}) - A^2(X_{\varphi(P)} - Z_{\varphi(P)})(X_{\varphi(Q)} - Z_{\varphi(Q)}) \end{pmatrix}.$$

- $\texttt{HalfDiffAdd}_{\widetilde{\varphi}}(\widetilde{\varphi}(P), \widetilde{\varphi}(Q), S)$:

$$((X_R + Z_R)(X_S + Z_S) : (X_R - Z_R)(X_S - Z_S)) = \begin{pmatrix} A^2(X_{\widetilde{\varphi}(P)} X_{\widetilde{\varphi}(Q)} + Z_{\widetilde{\varphi}(P)} Z_{\widetilde{\varphi}(Q)}) \\ B^2(X_{\widetilde{\varphi}(P)} X_{\widetilde{\varphi}(Q)} - Z_{\widetilde{\varphi}(P)} Z_{\widetilde{\varphi}(Q)}) \end{pmatrix}.$$

As we can see:

- A φ evaluation is $2\mathbf{S}$.
- A $\widetilde{\varphi}$ evaluation is $2\mathbf{S} + 2\mathbf{m}_0$.
- A half differential addition with respect to φ is $4\mathbf{M} + 1\mathbf{m}_0$, as well as a half differential addition with respect to $\widetilde{\varphi}$.

Since half of the images are via φ and the other is via $\widetilde{\varphi}$, an image costs $2\mathbf{S} + 1\mathbf{m}_0$ on average. We see that using these isogenies is a bit less efficient. We will tackle this issue in the next section.

4.2.3. *A variant on the theta twisted model.* In this section, we work on the theta twisted model $\theta_t(a : b)$ as described in Example 2.4.4, with ramification points

$$(a : b)^*, \qquad (-a : b), \qquad (1 : 1), \qquad (-1 : 1)$$

with $\frac{a}{b} \in k$, and set $(a' : b') = (a + b : a - b)$. If $P = (X : Z) \in \theta_t(a : b)$, we set $P^{\times} = (bX : aZ)$. The following 2-isogeny from $\theta_t(a : b)$ to $\theta_t(a' : b')$ can be derived from [RS24, Thm. 4.4] and the isomorphisms between theta squared, twisted and Montgomery models from Example 2.4. We get

$$\varphi : (X : Z) \mapsto (bX^2 + aZ^2 : bX^2 - aZ^2) \tag{2}$$

Its dual is $\widetilde{\varphi} : (X : Z) \mapsto (b'X^2 + a'Z^2 : b'X^2 - a'Z^2)$. The half differential addition formulas are then:

- $\texttt{HalfDiffAdd}_{\varphi}(\varphi(P), \varphi(Q), S)$:

$$(X_R X_S : Z_R Z_S) = \begin{pmatrix} a(b' X_{\varphi(P)} X_{\varphi(Q)} + a' Z_{\varphi(P)} Z_{\varphi(Q)}) \\ b(b' X_{\varphi(P)} X_{\varphi(Q)} - a' Z_{\varphi(P)} Z_{\varphi(Q)}) \end{pmatrix}.$$

- $\texttt{HalfDiffAdd}_{\widetilde{\varphi}}(\widetilde{\varphi}(P), \widetilde{\varphi}(Q), S)$:

$$(X_R X_S : Z_R Z_S) = \begin{pmatrix} a'(bX_{\varphi(P)} X_{\varphi(Q)} + a Z_{\varphi(P)} Z_{\varphi(Q)}) \\ b'(bX_{\varphi(P)} X_{\varphi(Q)} - a Z_{\varphi(P)} Z_{\varphi(Q)}) \end{pmatrix}.$$

R can be computed with $4\mathbf{M} + 2\mathbf{m}_0$. However, if we use the point $\varphi(P)^{\times}$, we can recover $R^{\times}$ in $4\mathbf{M}$ thanks to the following formula:

$$(X_{R^{\times}} X_S : Z_{R^{\times}} Z_S) = \begin{pmatrix} X_{\varphi(P)^{\times}} X_{\varphi(Q)} + Z_{\varphi(P)^{\times}} Z_{\varphi(Q)} \\ X_{\varphi(P)^{\times}} X_{\varphi(Q)} - Z_{\varphi(P)^{\times}} Z_{\varphi(Q)} \end{pmatrix}.$$

The roles of $\varphi(P)^{\times}$ and $\varphi(Q)$ are interchangeable, as well as those of φ and $\widetilde{\varphi}$ because of the symmetries of the formulas. Moreover, it is also possible to compute $\widetilde{\varphi}(P)$ with the knowledge of $P^{\times}$ because

$$\widetilde{\varphi}(P) = (b' X_P^2 + a' Z_P^2 : b' X_P^2 - a' Z_P^2) = (a' X_{P^{\times}}^2 + b' Z_{P^{\times}}^2 : a' X_{P^{\times}}^2 - b' Z_{P^{\times}}^2).$$

The cost is $2\mathbf{S} + 1\mathbf{m}_0$ whether we use P or $P^{\times}$. Hence, we can adapt Algorithm 2 into Algorithm 3 below for theta twisted models by storing either $(U^{\times}, V)$ or $(U, V^{\times})$ and by keeping track of this information. Evaluation by φ and $\widetilde{\varphi}$ always costs $2\mathbf{S} + 1\mathbf{m}_0$, and in this context half differential addition cost $4\mathbf{M}$, so the cost per bit of Algorithm 3 is the same as the case of a theta model with a 8-torsion point. This is the variant we compare to in Tables 1 to 3 in the introduction.

Hence, we can always achieve the best case scenario of the Montgomery ladder left-to-right if we have a Montgomery curve with full rational 2-torsion, even if the base point is not normalized, and we can significantly improve the pre-computation of the Montgomery ladder right-to-left at the cost of $1\mathbf{m}_0$ in the main loop. In the last section on half ladder, we discuss the case where the 2-torsion of the Montgomery curve is not completely rational, but there is a rational 8-torsion point.

4.2.4. *Scalar multiplication on* `Curve25519`. `Curve25519`[Ber06] is a Montgomery curve over $\mathbb{F}_p$ with $p = 2^{255} - 19$ and equation $\mathcal{C} : y^2 = x(x^2 + \mathcal{A}x + 1)$ where $\mathcal{A} = 486662$. It is a well-known curve used in several cryptographic protocols. Its 2-torsion is not rational, however it has a rational 8-torsion point above $(0 : 1)$. We will then work in the following context: let $M(A : B)$ be a Kummer line associated to a Montgomery curve with ramification

$$(1 : 0)^*, \qquad (0 : 1), \qquad (A : B), \qquad (B : A),$$

as described in Example 2.4.1. We will not assume $\frac{A}{B} \in k$, however we suppose there is a rational 8-torsion point $\widetilde{T} = (r : s)$ above $T' = (1 : 1)$, itself above $T = (0 : 1)$. According to [RS24, Thm. 4.11], we have a 2-isogeny from this curve to a Montgomery curve $\mathcal{C}'$ with full rational 2-torsion. We can then compose it with the isomorphism from Example 2.4.4. We set the constants $(\gamma : \delta) = (4rs : (r - s)^2)$, $(a : b) = (\gamma - \delta : \gamma + \delta)$ and $(a' : b') = (a + b : a - b) = (-\gamma : \delta)$. We have the following 2-isogeny $\psi : M(A : B) \to \theta_t(a : b)$ given by

$$\psi : (X : Z) \mapsto (ab(X - Z)^2 - a\delta(X + Z)^2 : ab(X - Z)^2 + b\delta(X + Z)^2).$$

The dual is given by

$$\widetilde{\psi} : (X : Z) \mapsto (aZ^2 - bX^2 + 2\delta XZ : aZ^2 - bX^2 - 2\delta XZ).$$

We can afford to have these two isogenies being a bit slower than usual since they will only intervene once during the computations. The details on how we obtain the half differential addition formulas below are available in Appendix B.

Algorithm 3: Scalar multiplication on theta twisted model with the twisted half ladder

Input: $n = (b_{\ell-1}, b_{\ell-2}, \ldots, b_0)$ an ℓ-bits integer, P a point on $\theta_t(a:b)$
Output: $n \cdot P$
Data: $\mathcal{K}_{2i} = \theta_t(a:b)$, $\mathcal{K}_{2i+1} = \theta_t(a':b')$, $\varphi_{2i} = \varphi$, $\varphi_{2i+1} = \widetilde{\varphi}$, with $0 \leq 2i, 2i+1 \leq \ell$

Function `TwistedHalfLadder`(n, P)**:**
  $P_0 \leftarrow P$;
  for $i \leftarrow 1$ **to** ℓ **do** `// Potentially a pre-computation`
    $P_i \leftarrow \varphi_i(P_{i-1})$;
  end
  $U^\times \leftarrow \mathcal{O}_\ell^\times = (1:1)$; `// Neutral point on` $\mathcal{K}_\ell$
  $V \leftarrow P_\ell$;
  $b_\ell \leftarrow 1$;
  for $i \leftarrow \ell$ **to** 1 **do**
    if $b_{i-1} = 0$ **then**
      if $b_i = 0$ **then** `// Known points:` $U, V^\times$
        $V^\times \leftarrow \texttt{HalfDiffAdd}_{\varphi_i}(U, V^\times, P_{i-1})$;
        $U \leftarrow \texttt{HalfDouble}_{\varphi_i}(U)$
      end
      else if $b_i = 1$ **then** `// Known points:` $U^\times, V$
        $V^\times \leftarrow \texttt{HalfDiffAdd}_{\varphi_i}(U^\times, V, P_{i-1})$;
        $U \leftarrow \texttt{HalfDouble}_{\varphi_i}(U^\times)$;
      end
    else if $b_{i-1} = 1$ **then**
      if $b_i = 0$ **then** `// Known points:` $U, V^\times$
        $U^\times \leftarrow \texttt{HalfDiffAdd}_{\varphi_i}(U, V^\times, P_{i-1})$;
        $V \leftarrow \texttt{HalfDouble}_{\varphi_i}(V^\times)$;
      end
      else if $b_i = 1$ **then** `// Known points:` $U^\times, V$
        $U^\times \leftarrow \texttt{HalfDiffAdd}_{\varphi_i}(U^\times, V, P_{i-1})$;
        $V \leftarrow \texttt{HalfDouble}_{\varphi_i}(V)$;
      end
  end
  return U; `// Derived from` $U^\times$ `if` $b_0 = 1$

We then set $\mathcal{K}_0 = M(A:B)$, $\varphi_1 = \psi$, $\mathcal{K}_{2i} = \theta_t(a':b')$, $\mathcal{K}_{2i+1} = \theta_t(a:b)$, $\varphi_{2i} = \varphi$ and $\varphi_{2i+1} = \widetilde{\varphi}$ when $1 \leq 2i, 2i+1 \leq \ell$, where φ is the 2-isogeny of Eq. (2).

Using the tools from Section 5, we can derive half differential addition formulas for ψ. If $P, Q \in \mathcal{K}_0$, $(R, S) = (P+Q, P-Q)$, $\texttt{HalfDiffAdd}_\psi(\psi(P), \psi(Q), S)$ is given by

$$((X_R + Z_R)(X_S + Z_S) : (X_R - Z_R)(X_S - Z_S)) = \begin{pmatrix} aZ_{\psi(P)}Z_{\psi(Q)} - bX_{\psi(P)}X_{\psi(Q)} \\ \delta(X_{\psi(P)}Z_{\psi(Q)} + Z_{\psi(P)}X_{\psi(Q)}) \end{pmatrix}.$$

Again, we can afford to spend a bit more time on this step because it is used only once. The steps on $\theta_t(a:b)$ and $\theta_t(a':b')$ can be done using Algorithm 3, and the last step to go back to $M(A:B)$ is done via $\texttt{HalfDiffAdd}_\psi$ and $\widetilde{\psi}$ as in Algorithm 2, so the cost per step is the same as Algorithm 3.

Hence, the conclusion from previous section also holds on a Montgomery curve with a rational 8-torsion point above $(0:1)$, like `Curve25519`. There is however one very important caveat: using the half ladder, the $\mathbf{m}_0$ correspond to the curve constant on $\mathcal{C}'$ rather than on $\mathcal{C}$. In the specific case of `Curve25519`, although the curve constant on $\mathcal{C}$ is small, this is unfortunately not the same for its isogenous curve $\mathcal{C}'$ where the Montgomery constant is $\mathcal{A}' = 2466411551445368652830633256402301446674828588060392731221299501445526714860 7$. Hence, this reduces the utility of the half ladder for `Curve25519`, at least when the pre-computations are not reused.

5. A framework to derive half differential addition formulas

We now give more details on the framework yielding half differential addition formulas. The whole theory is based on the theta group defined by Mumford in [Mum66].

5.1. **Generalities on the theta group.** In this section, we first introduce some general notations on the theta group over a generic abelian variety. The reason is that in the upcoming sections, we will specialize the study to an elliptic curve E and a product of elliptic curves $E \times E$. We will denote the abelian variety A. While Mumford uses the language of ample line bundles, for convenience we use the one of ample divisors in this paper. In this section we work over an algebraically closed field $k = \overline{k}$.

Two divisors D and D' are linearly equivalent if there is a section $s \in k(A)$ such that $\operatorname{div} s = D - D'$, this is an equivalence relation denoted $\sim$ and the set of linear equivalence classes, denoted $[D]$ for D a divisor, is the Picard group $\operatorname{Pic}(A)$. It is also a proper group scheme, and we denote the connected component of $[0]$ by $\operatorname{Pic}^0(A)$, a subgroup of $\operatorname{Pic}(A)$ which is an abelian variety: the dual abelian variety $\hat{A}$ of A.

Let D be a divisor on A, it induces a polarization $\Lambda(D) : A \to \operatorname{Pic}^0(A)$ which maps an element $x \in A$ to the element $[t_x^* D - D] \in \operatorname{Pic}^0(A)$, where $t_x : A \to A$ is the translation by x. We denote its kernel $H(D) = \ker \Lambda(D)$. Two divisors D and D' are algebraically equivalent if $\Lambda(D) = \Lambda(D')$. For ample divisors this is equivalent to D being linearly equivalent to $t_x^* D'$ for some $x \in A$. In particular, if D and D' are linearly equivalent, then they are algebraically equivalent, but the converse does not hold in general.

If $x \in H(D)$, then there is an element $s \in k(A)$ such that $\operatorname{div} s = t_x^* D - D$, this is how we construct the theta group:

Definition 5.1. *Let D be a divisor on A, we set*

$$G(D) = \{g_x \in k(A) \mid \exists x \in H(D), \operatorname{div} g_x = t_x^* D - D\}.$$

If $g_x, g_y \in G(D)$ for some $x, y \in H(D)$, we set $g_y \cdot g_x : z \mapsto g_x(z) g_y(z + x)$.

One can verify that $\operatorname{div} g_y \cdot g_x = t_{x+y}^* D - D$, which then defines a group law on $G(D)$. There is also an action of $g_x \in G(D)$ over $s \in \Gamma(D)$ given by $g_x \cdot s : z \mapsto g_x^{-1}(z) s(z - x)$ where g_x^{-1} is the inverse for the group law in the theta group, one can compute $g_x^{-1} = \frac{1}{t_{-x}^* g_x}$.

By considering the map from $G(D)$ to $H(D)$ sending an element $g_x \in G(D)$ to the corresponding point $x \in H(D)$, the following sequence is exact:

$$0 \to k^* \to G(D) \to H(D) \to 0.$$

We are particularly interested in subgroups of $H(D)$ preserving this sequence, they are defined in [Mum66, § 1, Def. p. 291].

Definition 5.2. *A level subgroup $\widetilde{K} \subseteq G(D)$ is a subgroup such that $k^* \cap \widetilde{K} = \{0\}$, that is $\widetilde{K}$ is isomorphic to its image $K \subseteq H(D)$. If $K \subseteq H(D)$, any level subgroup $\widetilde{K} \subseteq G(D)$ such that $\widetilde{K} \simeq K$ is called a lift of K.*

In particular, a level subgroup is necessarily abelian; a level subgroup exists over $\overline{k}$ iff it is isotropic for the commutator pairing, which is equal (up to a sign) with the polarized Weil pairing.

Let $\iota : x \in A \mapsto -x$, this is an involution of A. If D is a divisor, D is symmetric if $\iota^* D \sim D$. For such a divisor, an element $g_x \in G(D)$ is said to be symmetric if $\iota^* g_x = g_x^{-1}$.

If $f : A \to B$ is an isogeny between two abelian varieties, a divisor D' on B is a descent of a divisor D on A if $f^* D'$ is linearly equivalent to D. Mumford's theory helps to understand those descents. The main theorem we will be using from Mumford is the following:

Theorem 5.3 (Mumford)**.** *Let D be a divisor on A, K a subgroup of $H(D)$, and $f : A \to A/K$ the isogeny with kernel K. Let D' be a descent of D via f, that is $f^* D' \sim D$.*

1. *Let $\alpha \in k(A)$ such that $\operatorname{div} \alpha = D - f^* D'$ and set $\widetilde{K} = \{\frac{t_x^* \alpha}{\alpha} \mid x \in K\}$. The set $\widetilde{K}$ does not depend on the choice of α, it is a lift of K and the map $[D'] \in \operatorname{Pic}(A/K) \mapsto \widetilde{K}$ is a bijection between the set of descents of D via f and the set of lifts of K.*
2. *$f^{-1}(H(D')) \subseteq H(D)$ and, if $C(\widetilde{K})$ is the centralizer of $\widetilde{K}$ in $G(D)$, then*

$$C(\widetilde{K}) = \{g_x \in G(D) \mid x \in H(D) \text{ and } f(x) \in H(D')\}.$$

   Moreover, $C(\widetilde{K})/\widetilde{K} \simeq G(D')$ canonically.
3. *We have $\Gamma(D)^{\widetilde{K}} \simeq \Gamma(D')$, where $\Gamma(D)^{\widetilde{K}}$ is the set of sections of $\Gamma(D)$ invariant by the action of $\widetilde{K} \subseteq G(D)$.*
4. *Assume D is symmetric. Then D' is symmetric if and only if the elements of $\widetilde{K}$ are symmetric.*

Proof. Item 1 corresponds to [Mum66, § 1, Prop. 1] and the preceding discussion, it is based in particular on Grothendieck descent theory.

Item 2 is [Mum66, § 1, Prop. 2], the isomorphism comes from the map from $C(\widetilde{K})$ to $G(D')$ that to some g_x associate the only g_y such that $g_x = \frac{t_x^* \alpha}{\alpha} f^* g_y$, where $y = f(x)$ and α is as in Item 1. It is a surjective morphism and the kernel is $\widetilde{K}$.

To prove Item 3, we set $\varphi : s' \in \Gamma(D') \mapsto \frac{f^* s'}{\alpha}$ where α is as in Item 1. We have

$$\operatorname{div} \varphi(s') + D = f^*(\operatorname{div} s' + D') \geq 0,$$

so $\varphi(s') \in \Gamma(D)$, and if $g_x = \frac{t_x^* \alpha}{\alpha} \in \widetilde{K}$ for some $x \in K$, $g_x^{-1} = \frac{t_{-x}^* \alpha}{\alpha}$ which yields:

$$g_x \cdot \varphi(s') = g_x^{-1} t_{-x}^* \left(\frac{f^* s'}{\alpha} \right) = \frac{(t_{-x}^* \alpha)(t_{-x}^* f^* s')}{\alpha (t_{-x}^* \alpha)} = \frac{f^* s'}{\alpha} = \varphi(s').$$

The last equality holds because $x \in K$ so $f \circ t_{-x} = f$, hence $\operatorname{im} \varphi \subseteq \Gamma(D)^{\widetilde{K}}$. φ is clearly a morphism, if $\varphi(s') = 0$ then $f^* s' = 0$ and because f is surjective, f^* is injective so $s' = 0$: φ is injective. Let $s \in \Gamma(D)^{\widetilde{K}}$, we set $s'' = \alpha s$, this is an element of $\Gamma(f^* D')$. Moreover, if $x \in K$ and $g_x \in \widetilde{K}$ is the associated element, we have $g_x \cdot s = s$ which is equivalent to $t_{-x}^*(\alpha s) = \alpha s$. Hence, for any $x \in K$, $t_x^* s'' = s''$, it is invariant by K and can then be factored by f: there is $s' \in k(A/K)$ such that $s'' = s' \circ f = f^* s'$, so $\varphi(s') = s$ and φ is surjective.

We now prove Item 4. We have the following linear equivalences: $D \sim \iota^* D \sim \iota^* f^* D' \sim f^* \iota^* D'$. Hence, $\iota^* D'$ also descends to D, the corresponding kernel being $\iota^* \widetilde{K}$. So D' being symmetric is equivalent to $[\iota^* D'] = [D']$ and by Item 1, this is the same as $\iota^* \widetilde{K} = \widetilde{K}$. Assume first that D' is symmetric. If $g_x \in \widetilde{K}$ is above $x \in K$, then $\iota^* g_x \in \widetilde{K}$ is above $-x$, but the only element above $-x$ in $\widetilde{K}$ is g_x^{-1}, hence $\iota^* g_x = g_x^{-1}$ and the elements of $\widetilde{K}$ are symmetric. Conversely, if $\widetilde{K}$ consists of symmetric elements, it is clear that $\iota^* \widetilde{K} = \widetilde{K}$ and therefore that D' is symmetric. □

5.2. **Theta group on an elliptic curve.** In this section, we recall the study of the descents of $2(\mathcal{O}_E)$ and $4(\mathcal{O}_E)$ on an elliptic curve E from [RS24, § 3.1], which will be useful in the next section. Assume there is a rational 2-torsion point $T \in E[2](k)$, let $K = \{\mathcal{O}_E, T\}$, and set $\varphi : E \to E' = E/K$ be the 2-isogeny with kernel K. Let $E[2] = \{\mathcal{O}_E, T_1, T_2, T_3\}$ with $T_1 = T$, the remaining points may not be rational. Set also $\overline{T_1}$ and $\underline{T_1}$ the two 4-torsion points above T_1, which again may not be rational, and finally set $T_1' = \varphi(T_2) = \varphi(T_3)$, $T_2' = \varphi(\overline{T_1})$ and $T_3' = \varphi(\underline{T_1})$. T_1' is always rational on E', even if T_2 and T_3 are not.

To understand the theta group of a divisor D of E, we must first look at the kernel of the polarization $H(D)$. On an elliptic curve, two divisors D and D' are algebraically equivalent if and only if they have the same degree. Hence, if $\deg D = n$, we can look at $D_n = n(\mathcal{O}_E)$, then $\Lambda(D) = \Lambda(D_n)$ and $H(D) = H(D_n)$. But $\Lambda(D_n)(P) = n(P) - n(\mathcal{O}_E)$ for $P \in E$ and on an elliptic curve, this divisor is equivalent to 0 if and only if $n \cdot P - n \cdot \mathcal{O}_E = \mathcal{O}_E$, i.e. $n \cdot P = \mathcal{O}_E$. So $H(D) = E[n]$, this is why we focus on divisors of the form $n(\mathcal{O}_E)$, which are symmetric.

Let $D = 2n(\mathcal{O}_E)$, it is symmetric and of even degree, hence $E[2] \subset E[2n] = H(D)$. Let $P \neq \mathcal{O}_E$ be a 2-torsion point, there is a corresponding element $g_P \in G(D)$. A result of Mumford [Mum66, § 2, Prop. 2, p. 307] then states that $\iota^* g_P = g_P$, so g_P is of order 2 if and only if $g_P = g_P^{-1}$, i.e. if and only if $\iota^* g_P = g_P^{-1}$. So g_P is of order 2 if and only if g_P is symmetric in this situation.

5.2.1. *Descents of* $2(\mathcal{O}_E)$. We start by studying the descents of $D_2 = 2(\mathcal{O}_E)$. If D' is a descent of D_2, there is a lift $\widetilde{K}$ of K to $G(D_2)$ by Theorem 5.3.1. This lift must be generated by an element g_T above $T \in E[2]$, and g_T is of order 2, that is symmetric by the above discussion. So $\widetilde{K}$ is composed of symmetric elements and D' must be symmetric by Theorem 5.3.4.

We also have $\varphi^* D'$ linearly equivalent to D_2, so $\deg \varphi^* D'$ must be 2, which implies $\deg D' = 1$ because $\deg \varphi^* D' = (\deg \varphi)(\deg D')$. Finally, because this is up to linear equivalence, we can look at $D' \geq 0$. These two conditions forces $D' \sim (P)$ for some $P \in E'$, and because D' is symmetric, $\iota^* D' = D'$ i.e. $(-P) \sim (P)$, which happens if and only $P \in E'[2]$. We then have four possible descents for D_2, but:

- $\varphi^*(\mathcal{O}_{E'}) = (\mathcal{O}_E) + (T_1) \nsim D_2$ because $T_1 \neq \mathcal{O}_E$.
- $\varphi^*(T_1') = (T_2) + (T_3) \nsim D_2$ because $T_2 + T_3 = T_1 \neq \mathcal{O}_E$.
- $\varphi^*(T_2') = (\overline{T_1}) + (\overline{T_1} + T_1) \sim D_2$ because $2 \cdot \overline{T_1} + T_1 = 2 \cdot T_1 = \mathcal{O}_E$.
- $\varphi^*(T_3') = (\underline{T_1}) + (\underline{T_1} + T_1) \sim D_2$ because $2 \cdot \underline{T_1} + T_1 = 2 \cdot T_1 = \mathcal{O}_E$.

In the end, there is at most two descents of D_2, and those are distinct because $(T_2') \nsim (T_3')$ since $T_2' \neq T_3'$. We now try to compute a symmetric element $\widetilde{g_T} \in G(D_2)$ above T.

Let $g_T \in G(D_2)$ be above T, with no further assumption. This exists because we assumed that T is rational. Because T is a 2-torsion point, we must have $\operatorname{div} g_T^2 = 0$, hence there is $\lambda_T \in k^*$ such that $g_T^2 = \lambda_T$. This element, called the type of T, is well-defined up to a square as explained in [RS24, § 3.1, Def. 3.3]. Moreover, the element $\widetilde{g_T} = \frac{g_T}{\sqrt{\lambda_T}}$ does not depend on the choice of g_T and is symmetric, but may not be rational. This is the symmetric element we were looking for, as well as $-\widetilde{g_T}$, they are the two elements giving the descents of D_2.

5.2.2. *Descents of* $4(\mathcal{O}_E)$. The situation is easier when regarding descents of $D_4 = 4(\mathcal{O}_E)$. The goal of [RS24] was to find descents of D_4 to $D_2' = 2(\mathcal{O}_{E'})$ with associated lift $\widetilde{K}$, to then exploit the isomorphism $\Gamma(D_2') \simeq \Gamma(D_4)^{\widetilde{K}}$ from Theorem 5.3.3 to find 2-isogenies formulas.

If D' is a descent of D_4 with respect to φ, let $\widetilde{K}$ be the associated lift of the kernel to $G(D_4)$. By the same argument as in the case of D_2, $\widetilde{K}$ consists of symmetric elements, so we must look for a symmetric D'. Furthermore, by the degree we must have $\deg D' = 2$ and since we are looking for divisors up to linear equivalence, we can look at $D' \geq 0$. We can therefore restrict to $D' \sim 2(P)$

or $D' \sim (P) + (Q)$ for $P, Q \in E'$. But $2(P) \sim (2P) + (\mathcal{O}_{E'})$ and $(P) + (Q) \sim (P - Q) + (\mathcal{O}_{E'})$, we then are looking at $D' \sim (P) + (\mathcal{O}_{E'})$ for some $P \in E'$. This last divisor is symmetric if and only $P \in E'[2]$, we have once again four potential choices for descents of D_4:

- $\varphi^*(2(\mathcal{O}_{E'})) = 2(\mathcal{O}_E) + 2(T_1) \sim D_4$ because $2 \cdot T_1 = \mathcal{O}_E$.
- $\varphi^*((T_1') + (\mathcal{O}_{E'})) = (T_2) + (T_3) + (\mathcal{O}_E) + (T_1) \sim D_4$ because $T_1 + T_2 + T_3 = 2 \cdot T_1 = \mathcal{O}_E$.
- $\varphi^*((T_2') + (\mathcal{O}_{E'})) = (\overline{T_1}) + (\overline{T_1} + T_1) + (\mathcal{O}_E) + (T_1) \nsim D_4$ because $2 \cdot \overline{T_1} + 2 \cdot T_1 = T_1 \neq \mathcal{O}_E$.
- $\varphi^*((T_3') + (\mathcal{O}_{E'})) = (\underline{T_1}) + (\underline{T_1} + T_1) + (\mathcal{O}_E) + (T_1) \nsim D_4$ because $2 \cdot \underline{T_1} + 2 \cdot T_1 = T_1 \neq \mathcal{O}_E$.

There are only two descents, we can give the elements of $G(D_4)$ generating the lifts. If $\widetilde{g_T}$ is a symmetric element in $G(D_2)$ above T, we consider $\widetilde{g_T}^{\otimes 2} : P \mapsto \widetilde{g_T}(P)^2$ (the tensor product here is the usual scalar multiplication of sections, not the product in $G(D_2)$). This is an element of $G(D_4)$, it preserves symmetry and it is above T, so it is of order 2 and generates a lift $\widetilde{K}$. On top of that, if $\widetilde{g_T} = \frac{g_T}{\sqrt{\lambda_T}}$, then $\widetilde{g_T}^{\otimes 2} = \frac{g_T^{\otimes 2}}{\lambda_T}$, which is always rational. Moreover, this $\widetilde{g_T}^{\otimes 2}$ does not depend on the choice of sign in $\widetilde{g_T}$ and the lift $\widetilde{K}$ corresponds to the descent of D_4 to $D_2' \sim 2(T_2') \sim 2(T_3')$, because of the shape of the kernels in Theorem 5.3.1. We obtain an isomorphism $\Gamma(D_4)^{\widetilde{g_T}^{\otimes 2}} \simeq \Gamma(D_2')$.

The other descent of D_4 to $(T_1') + (\mathcal{O}_{E'})$ is then given by $-\widetilde{g_T}^{\otimes 2}$. We will reuse these elements in the upcoming section on the product of elliptic curves.

5.3. **Theta group on a product of elliptic curves.** In this section, we will extend the notions of Section 5.2 to the case of $E \times E$ where E is an elliptic curve. Recall from Section 3 that our goal is to study the isogeny $F : (P, Q) \mapsto (P + Q, P - Q)$.

Remark 5.4. *For the sake of simplicity and because this is the context we are working on, the results in this section are only stated on $E \times E$, however most of those still hold on $A \times B$ where A and B are abelian varieties.*

5.3.1. *Product divisor.* Let $\pi_1 : E \times E \to E$ and $\pi_2 : E \times E \to E$ be the projection on the first and the second component respectively, $\pi_1 : (P, Q) \mapsto P$ and $\pi_2 : (P, Q) \mapsto Q$.

Definition 5.5. *Let D_1 and D_2 be divisors on E. $\pi_1^* D_1$ and $\pi_2^* D_2$ are divisors on $E \times E$, we define the product divisor on $E \times E$ as $D_1 * D_2 := \pi_1^* D_1 + \pi_2^* D_2$.*

This is the correct notion of product because it has good compatibility with the tools from Section 5.1. If $f, g \in k(E)$, we define $f \otimes g \in k(E \times E)$ as:

$$\forall (P, Q) \in E \times E, f \otimes g(P, Q) := f(P)g(Q). \tag{3}$$

Lemma 5.6. *Let $f, g \in k(E)$, then* $\operatorname{div}(f \otimes g) = (\operatorname{div} f) * (\operatorname{div} g)$.

Proof. We have $f \otimes g = (\pi_1^* f)(\pi_2^* g)$ where $\pi_1^* f$ and $\pi_2^* g$ are elements of $k(E \times E)$. Hence, $\operatorname{div}(f \otimes g) = \operatorname{div}(\pi_1^* f) + \operatorname{div}(\pi_2^* g) = \pi_1^*(\operatorname{div} f) + \pi_2^*(\operatorname{div} g) = (\operatorname{div} f) * (\operatorname{div} g)$. □

Let D_1, D_2 be divisors on E. We can relate the global sections of D_1 and D_2 over E to the global sections of $D_1 * D_2$ over $E \times E$:

Lemma 5.7. *Let D_1 and D_2 be divisors on E. The following canonical map is an isomorphism of vector spaces:*

$$\begin{aligned} \Gamma(D_1) \otimes \Gamma(D_2) &\xrightarrow{\sim} \Gamma(D_1 * D_2) \\ f \otimes g &\longmapsto f \otimes g \end{aligned}$$

where on the left side, $f \otimes g$ is an element of $k(E) \otimes k(E)$ and on the right side $f \otimes g$ is the element defined in Eq. (3).

Proof. This is a particular case of Künneth formula where $n = 0$, see [The24, Lemma 0BED]. □

Since we want to study the theta group on $E \times E$ for product divisors, we have to study the associated polarization. We recall that we have a canonical identification $\mathrm{Pic}^0(A \times B) \simeq \mathrm{Pic}^0(A) \times \mathrm{Pic}^0(B)$ via $(D_1, D_2) \mapsto D_1 \star D_2$, and that we can see $\mathrm{Pic}^0(A)$ inside $\mathrm{Pic}^0(A \times B)$ via the pullback π_1^*. Modulo these identifications applied to $A = B = E$, we have

$$\Lambda(D_1 * D_2) : E \times E \to \mathrm{Pic}^0(E) \times \mathrm{Pic}^0(E) : (P, Q) \mapsto (\Lambda_{D_1}(P), \Lambda_{D_2}(Q))$$

Unraveling the identifications, we need to check that if D_1 and D_2 are divisors on E, the polarization associated to $D_1 * D_2$ is

$$\begin{aligned} \Lambda(D_1 * D_2) : E \times E &\to \mathrm{Pic}^0(E \times E) \\ (P, Q) &\mapsto [t^*_{(P,Q)}(D_1 * D_2) - D_1 * D_2]. \end{aligned}$$

If $(P, Q) \in E \times E$, since $\pi_1 \circ t_{(P,Q)} = t_P \circ \pi_1$ and $\pi_2 \circ t_{(P,Q)} = t_Q \circ \pi_2$, we get:

$$t^*_{(P,Q)}(D_1 * D_2) = t^*_{(P,Q)}\pi_1^* D_1 + t^*_{(P,Q)}\pi_2^* D_2 = \pi_1^* t_P^* D_1 + \pi_2^* t_Q^* D_2 = (t_P^* D_1) * (t_Q^* D_2).$$

Because of this, $\Lambda(D_1 * D_2)(P, Q) = \Lambda(D_1)(P) * \Lambda(D_2)(Q)$.

The kernel is thus given by:

Lemma 5.8. *Let D_1 and D_2 be two divisors on E, then $H(D_1 * D_2) = H(D_1) \times H(D_2)$.*

We then recover a statement similar to Lemma 5.7 on the theta group (see [Mum66, § 3, Lem. 1, p. 323])

Lemma 5.9. *Let D_1 and D_2 be divisors on E. The following canonical map is a surjective morphism of groups:*

$$\begin{aligned} G(D_1) \times G(D_2) &\longrightarrow G(D_1 * D_2) \\ (f, g) &\longmapsto f \otimes g. \end{aligned}$$

Its kernel is given by $\{(\lambda, \lambda^{-1}) \mid \lambda \in k^*\} \simeq k^*$. Moreover, if $f \in G(D_1)$ lies above $P \in H(D_1)$ and $g \in G(D_2)$ lies above $Q \in H(D_2)$, then $f \otimes g$ lies above $(P, Q) \in \ker H(D_1 * D_2)$.

Proof. The surjectivity and the computation of the kernel correspond to [Mum66, § 3, Lem. 1, p. 323]. Consider f, g, P and Q as in the statement, then, by Lemma 5.6 $\operatorname{div} f \otimes g = \operatorname{div} f * \operatorname{div} g$. As seen above, $\operatorname{div} f * \operatorname{div} g = t^*_{(P,Q)}(D_1 * D_2) - D_1 * D_2$, hence $f \otimes g$ lies above (P, Q). □

Finally, a straight-forward computation shows that the action of $G(D_1 * D_2)$ on $\Gamma(D_1 * D_2)$ is compatible with these maps. Let $s_1 \in \Gamma(D_1)$, $s_2 \in \Gamma(D_2)$, $g_1 \in G(D_1)$ and $g_2 \in G(D_2)$, then:

$$(g_1 \otimes g_2) \cdot (s_1 \otimes s_2) = (g_1 \cdot s_1) \otimes (g_2 \cdot s_2).$$

5.3.2. *A commutative diagram for half differential additions.* We set the following divisors on E and E': $D_2 = 2(\mathcal{O}_E)$, $D_2' = 2(\mathcal{O}_{E'})$ and $D_4 = 4(\mathcal{O}_E)$. Recall that F is the differential addition isogeny and Φ is the diagonal isogeny of φ, where φ is a 2-isogeny on E, as in Section 3.

Because of Lemma 5.7, if $R, S \in E$ with coordinates $(X_R : Z_R)$ and $(X_S : Z_S)$ — each coordinate being a section above D_2 — then a natural basis of $\Gamma(D_2 * D_2)$ is given by:

$$\Gamma(D_2 * D_2) = \left\langle \begin{matrix} X_R X_S & X_R Z_S \\ Z_R X_S & Z_R Z_S \end{matrix} \right\rangle.$$

By general theory, because of the uniqueness of totally symmetric line bundles in their algebraic equivalent classes, $D_4 * D_4$ descends to $D_2 * D_2$ via F (since both are totally symmetric). This descent corresponds to a lift of the kernel $\widetilde{K}$; then we obtain an isomorphism $\Gamma(D_4 * D_4)^{\widetilde{K}} \simeq \Gamma(D_2 * D_2)$ by Theorem 5.3, from which we can express a basis of $\Gamma(D_2 * D_2)$ via a basis of

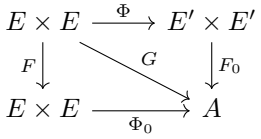

FIGURE 2. Factoring $G = F_0 \circ \Phi = \Phi_0 \circ F$ through F and Φ

$\Gamma(D_4 * D_4)$, which we can also compute. This give differential addition formulas, and with a more thorough study of those descents that are compatible with a suitable descent of $D_4 * D_4$ through Φ, we are able to find half differential addition formulas. We now give more details.

As discussed in Section 3, if K_F and K_Φ are the kernels of F and Φ respectively, then $K_F \cap K_\Phi = \{(\mathcal{O}_E, \mathcal{O}_E), (T, T)\}$, so we can't factor Φ through F or the converse. We then consider the isogeny $G : E \times E \to A$ with kernel $K_G = K_F + K_\Phi$, where A is an abelian variety, with a polarization of type $(1, 2)$ (hence which is not principal). Since $K_F, K_\Phi \subset K_G$, we can factor F and Φ through G. Let $\Phi_0 : E \times E \to A$ and $F_0 : E' \times E' \to A$ be such that $G = F_0 \circ \Phi = \Phi_0 \circ F$. The situation is summarized in Fig. 2.

The kernel of Φ_0 is $K_{\Phi_0} = F(K_G) = F(K_\Phi) = \{(\mathcal{O}_E, \mathcal{O}_E), (T, T)\}$. Similarly, the kernel of F_0 is $K_{F_0} = \Phi(K_G) = \Phi(K_F) = \{(\mathcal{O}_{E'}, \mathcal{O}_{E'}), (T', T')\}$, where $T' = \varphi(T_0)$ for $T_0 \in E[2] \setminus \{\mathcal{O}_E, T\}$.

5.3.3. *Descents of $D_4 * D_4$ with respect to Φ.* We have seen in Section 5.2 that D_4 descends to D_2' via φ, the lift of the kernel $\widetilde{K}_\varphi$ is generated by a symmetric element $\widetilde{g_T}^{\otimes 2}$ of order 2. Let $\alpha \in k(E)$ with divisor $D_4 - \varphi^* D_2'$, then $\widetilde{g_T}^{\otimes 2} = \frac{t_T^* \alpha}{\alpha}$.

If we look at the image of $\widetilde{K}_\varphi \times \widetilde{K}_\varphi$ via the map of Lemma 5.9, we get a subgroup

$$\widetilde{K} = \{1 \otimes 1,\ \widetilde{g_T}^{\otimes 2} \otimes 1,\ 1 \otimes \widetilde{g_T}^{\otimes 2},\ \widetilde{g_T}^{\otimes 2} \otimes \widetilde{g_T}^{\otimes 2}\}.$$

If we look for instance at the second element, for $(P, Q) \in E \times E$:

$$(\widetilde{g_T}^{\otimes 2} \otimes 1)(P, Q) = \frac{t_T^* \alpha(P)}{\alpha(P)} = \frac{\alpha(P+T)\alpha(Q)}{\alpha(P)\alpha(Q)} = \frac{t^*_{(T,\mathcal{O})}\alpha \otimes \alpha(P, Q)}{\alpha \otimes \alpha(P, Q)}.$$

With a similar computation,

$$\widetilde{K} = \left\{ \frac{t^*_{(\mathcal{O},\mathcal{O})}\alpha \otimes \alpha}{\alpha \otimes \alpha},\ \frac{t^*_{(T,\mathcal{O})}\alpha \otimes \alpha}{\alpha \otimes \alpha},\ \frac{t^*_{(\mathcal{O},T)}\alpha \otimes \alpha}{\alpha \otimes \alpha},\ \frac{t^*_{(T,T)}\alpha \otimes \alpha}{\alpha \otimes \alpha} \right\},$$

and we check that it is a lift of K_Φ to $G(D_4 * D_4)$. We just have to compute $\operatorname{div} \alpha \otimes \alpha$, which can be done using Lemma 5.6:

$$\operatorname{div} \alpha \otimes \alpha = \pi_1^*(D_4 - \varphi^* D_2') + \pi_2^*(D_4 - \varphi^* D_2') = D_4 * D_4 - (\pi_1^* \varphi^* D_2' + \pi_2^* \varphi^* D_2').$$

For $i = 1, 2$, if π_i' is the projection from $E' \times E'$ on the i-th component of E', then $\pi_i' \circ \Phi = \varphi \circ \pi_i$ by construction, hence $\pi_i^* \varphi^* D_2' = \Phi^* \pi_i'^* D_2'$ which leads to $\operatorname{div} \alpha \otimes \alpha = D_4 * D_4 - \Phi^*(D_2' * D_2')$.

To summarize $D_4 * D_4$ descends to $D_2' * D_2'$ with respect to Φ and the lift of the kernel $\widetilde{K} =: \widetilde{K}_\Phi$ is naturally constructed as the product of the lift $\widetilde{K}_\varphi$ with itself.

This gives an isomorphism $\Gamma(D_4 * D_4)^{\widetilde{K}_\Phi} \simeq \Gamma(D_2' * D_2')$ by Theorem 5.3.3.

5.3.4. *Descents of $D_4 * D_4$ with respect to F.* The isogeny F is not diagonal this time. Fortunately, if D is a symmetric divisor on E, [Mum66, § 3, Prop. 1, p. 320] states that $F^*(D * D) \sim (2D) * (2D)$. Considering $D = D_2$, we get $F^*(D_2 * D_2) \sim D_4 * D_4$. So $D_4 * D_4$ descends to $D_2 * D_2$ with respect to F, we denote by $\widetilde{K}_F$ the lift of K_F to $G(D_4 * D_4)$. Moreover, the elements of $\widetilde{K}_F$

are of the shape $g_P \otimes g_P$ for $P \in E[2]$ and $g_P \in G(D_4)$. This implies $\widetilde{g_T}^{\otimes 2} \otimes \widetilde{g_T}^{\otimes 2} \in \widetilde{K}_F$ is the element above (T,T).

This gives an isomorphism $\Gamma(D_4 * D_4)^{\widetilde{K}_F} \simeq \Gamma(D_2 * D_2)$, which permits to recover differential addition formulas by expressing sections of $D_2 * D_2$ — which are coordinates — in terms of sections of $D_4 * D_4$ invariant by F.

5.3.5. *Descents of $D_2 * D_2$ and $D_2' * D_2'$ with respect to Φ_0 and F_0.* Since T is a rational 2-torsion point on E, we have seen in Section 5.2 that there are elements $g_T \in G(D_2)$ such that $g_T^2 = \lambda_T$ where the class of λ_T modulo squares is the type of T. Via the morphism of Lemma 5.9, we consider $g_{(T,T)} := \frac{1}{\lambda_T} g_T \otimes g_T \in G(D_2 * D_2)$. This element does not depend on the choice of g_T, lies above (T,T), and is of order 2 because

$$\left(\frac{1}{\lambda_T} g_T \otimes g_T\right)^2 = \frac{1}{\lambda_T^2} g_T^2 \otimes g_T^2 = 1.$$

Hence, $\widetilde{K}_{\Phi_0} = \{1, g_{(T,T)}\}$ is a lift of K_{Φ_0} to $G(D_2 * D_2)$, and by Theorem 5.3.1 there is a divisor D_A on the abelian variety A on which $D_2 * D_2$ descends with respect to Φ_0. This also means that $D_4 * D_4$ descends to D_A with respect to G because $\Phi_0^* D_A \sim D_2 * D_2$ and $F^*(D_2 * D_2) \sim D_4 * D_4$, which implies $G^* D_A \sim D_4 * D_4$. This produces a kernel $\widetilde{K}_A$.

Similarly, $\widetilde{K}_{F_0} = \{1, g_{(T',T')}\}$ where $g_{(T',T')} = \frac{1}{\lambda_{T'}} g_{T'} \otimes g_{T'}$, $g_{T'} \in G(D_2')$ above T', is a lift of K_{F_0} that descends $D_2' * D_2'$ to some divisor D_A' on the abelian variety A with respect to F_0. Similarly, $D_4 * D_4$ descends to D_A' with respect to G, via a kernel $\widetilde{K}_A'$.

We need to show that $\widetilde{K}_A = \widetilde{K}_A'$. Set $\widetilde{K}_0 = \widetilde{K}_F \cdot \widetilde{K}_\Phi$, the subgroup of $G(D_4 * D_4)$ generated by elements of $\widetilde{K}_F$ and $\widetilde{K}_\Phi$. It is a level subgroup because if $\lambda = g_{(P,Q)} \cdot g_{(P',Q')}^{-1} \in \widetilde{K}_0 \cap k^*$, with $g_{(P,Q)} \in \widetilde{K}_F$ and $g_{(P',Q')} \in \widetilde{K}_\Phi$, then $(P - P', Q - Q') = (\mathcal{O}_E, \mathcal{O}_E)$, and $(P,Q) = (P',Q') \in K_F \cap K_\Phi = \{(\mathcal{O}_E, \mathcal{O}_E), (T,T)\}$. In both cases, $g_{(P,Q)} = g_{(P',Q')}$, proving that $\widetilde{K}_0 \cap k^* = \{1\}$. It then corresponds to another descent of $D_4 * D_4$ with respect to G by Theorem 5.3.1.

The elements of $\widetilde{K}_F$ commutes with the elements of $\widetilde{K}_\Phi$, hence $\widetilde{K}_0 \subseteq C(\widetilde{K}_F), C(\widetilde{K}_\Phi)$ and via the isomorphism $C(\widetilde{K}_F)/\widetilde{K}_F \simeq G(D_2 * D_2)$ of Theorem 5.3.2, $\widetilde{K}_A$ must maps to $\widetilde{K}_{\Phi_0}$ by construction, but $\widetilde{K}_0$ also maps to $\widetilde{K}_{\Phi_0}$. This forces $\widetilde{K}_0 = \widetilde{K}_A$. Similarly, $\widetilde{K}_0 = \widetilde{K}_A'$. Hence, D_A and D_A' are linearly equivalent and corresponds to the same lift $\widetilde{K}_G := \widetilde{K}_0$.

Using Theorem 5.3.3, $\Gamma(D_4 * D_4)^{\widetilde{K}_G} \simeq \Gamma(D_A)$ and using the previous results we have

$$\Gamma(D_2 * D_2)^{\widetilde{K}_{\Phi_0}} \simeq \Gamma(D_4 * D_4)^{\widetilde{K}_G} \simeq \Gamma(D_2' * D_2')^{\widetilde{K}_{F_0}}.$$

This is the main ingredient to derive half differential addition formulas, since from our commutative diagram, $\Gamma(D_2 * D_2)^{\widetilde{K}_{\Phi_0}}$ are precisely the subspace of the differential addition formulas, expressed in terms of coordinates $P+Q, P-Q$, that factorize through $\Phi(P,Q)$. The isomorphism with $\Gamma(D_4 * D_4)^{\widetilde{K}_G}$ allows us to write these formulas in terms of coordinates of P, Q, invariant under the action of $\widetilde{K}_G$. Since we know the action of $\widetilde{K}_G$ and the other lifted kernel on sections, basic linear algebra now gives us formulas to find a basis of invariants.

5.3.6. *Even coordinates.* Recall that over an abelian variety A, $\iota : x \in A \mapsto -x$ is an involution, giving an automorphism $\iota^* : k(A) \to k(A)$. If D is a symmetric divisor, the restriction of ι^* to $\Gamma(D)$ (resp. $G(D)$) is an automorphism of vector spaces (resp. of groups). A section $f \in k(A)$ is said to be even if $\iota^* f = f$ and is said to be odd if $\iota^* f = -f$.

Over E, if $\Gamma(D_2) = \langle X, Z\rangle$, a basis of $\Gamma(D_4)$ is $\langle X^2, Z^2, XZ, T\rangle$ where $T = YZ_0$ is a fourth odd section. The isomorphism of Lemma 5.7 then yields basis of $\Gamma(D_2 * D_2)$ and $\Gamma(D_4 * D_4)$:

$$\Gamma(D_2 * D_2) = \left\langle \begin{matrix} X_P X_Q & X_P Z_Q \\ Z_P X_Q & Z_P Z_Q \end{matrix} \right\rangle,$$

$$\Gamma(D_4 * D_4) = \left\langle \begin{matrix} X_P^2 X_Q^2 & X_P^2 Z_Q^2 & X_P^2 X_Q Z_Q & X_P^2 T_Q \\ Z_P^2 X_Q^2 & Z_P^2 Z_Q^2 & Z_P^2 Z_Q Z_Q & Z_P^2 T_Q \\ X_P Z_P X_Q^2 & X_P Z_P Z_Q^2 & X_P Z_P X_Q Z_Q & X_P Z_P T_Q \\ T_P X_Q^2 & T_P Z_Q^2 & T_P X_Q Z_Q & T_P T_Q \end{matrix} \right\rangle.$$

The issue that arises when looking for differential addition formulas via $\Gamma(D_4 * D_4)^{\widetilde{K}_F} \simeq \Gamma(D_2 * D_2)$ is that, if we only know the Kummer line coordinates $(X : Z)$ of P, Q, we have no information about the section T. We have to restrict our study to even coordinates. We will denote, for any symmetric divisor D, $\Gamma(D)^+ = \Gamma(D)^{\iota^*}$ the subspace of even sections. We have $\Gamma(D_2)^+ = \Gamma(D_2)$ and $\Gamma(D_4)^+ = \langle X^2, Z^2, XZ\rangle$ and there is a canonical surjection $\Gamma(D_2)^+ \otimes \Gamma(D_2)^+ \to \Gamma(D_4)^+$, $f \otimes g \mapsto fg$.

The ι maps over E and $E \times E$ are compatible: if $\iota_1 : E \to E$ and $\iota_2 : E \times E \to E \times E$ are the maps on the corresponding varieties, then $\iota_2^* = \iota_1^* \otimes \iota_1^*$ on $k(E) \otimes k(E) \subseteq k(E \times E)$. Via the isomorphism of Lemma 5.7, we get an injection $\Gamma(D_4)^+ \otimes \Gamma(D_4)^+ \to \Gamma(D_4 * D_4)^+$.

However, one can compute the following basis for $\Gamma(D_4 * D_4)^+$:

$$\Gamma(D_4 * D_4)^+ = \left\langle \begin{matrix} X_P^2 X_Q^2 & X_P^2 Z_Q^2 & X_P^2 X_Q Z_Q & Z_P^2 X_Q^2 & Z_P^2 Z_Q^2 \\ Z_P^2 Z_Q Z_Q & X_P Z_P X_Q^2 & X_P Z_P Z_Q^2 & X_P Z_P X_Q Z_Q & T_P T_Q \end{matrix} \right\rangle.$$

The last section is even as it is the product of two odd sections, but the image of the injection is only of dimension 9 since $\Gamma(D_4)^+$ is of dimension 3. We denote the image of the injection $\Gamma(D_4 * D_4)^{++} \subsetneq \Gamma(D_4 * D_4)^+$:

$$\Gamma(D_4 * D_4)^{++} = \left\langle \begin{matrix} X_P^2 X_Q^2 & X_P^2 Z_Q^2 & X_P^2 X_Q Z_Q \\ Z_P^2 X_Q^2 & Z_P^2 Z_Q^2 & Z_P^2 Z_Q Z_Q \\ X_P Z_P X_Q^2 & X_P Z_P Z_Q^2 & X_P Z_P X_Q Z_Q \end{matrix} \right\rangle.$$

This is the set of sections we would like to work with. One can check immediately that $\Gamma(D_4 * D_4)^{++}$ is the set of sections above $D_4 * D_4$ invariants by $\iota^* \otimes 1$ and $1 \otimes \iota^*$. We will use the following lemma:

Lemma 5.10. *Let D be a symmetric divisor over E, $g_T \in G(D)$ a symmetric element above a 2-torsion point $T \in E[2]$. Then for any $f \in \Gamma(D)$, $\iota^*(g_T \cdot f) = g_T \cdot (\iota^* f)$.*

Proof. Let $P \in E$, $f \in \Gamma(D)$, we have $\iota^*(g_T \cdot f)(P) = (g_T \cdot f)(-P) = g_T(-P) f(-P+T)$. Because T is a 2-torsion point, $-T = T$ and since g_T is symmetric, $g_T(-P) = g_T(P)$:

$$\iota^*(g_T \cdot f)(P) = g_T(P) f(-P - T) = g_T(P) \iota^* f(P + T) = g_T \cdot (\iota^* f)(P).$$

□

Since the kernels $\widetilde{K}_F$, $\widetilde{K}_\Phi$, $\widetilde{K}_{F_0}$, $\widetilde{K}_{\Phi_0}$ and $\widetilde{K}_G$ are all composed of symmetric elements above 2-torsion points, the action of $\iota^* \otimes 1$, $1 \otimes \iota^*$ and $\iota^* \otimes \iota^*$ commutes with the one of the kernels by the above lemma. Denote by $G_\iota = \{\iota^* \otimes 1, 1 \otimes \iota^*, \iota^* \otimes \iota^*\}$, such that $\Gamma(D_4 * D_4)^{++} = \Gamma(D_4 * D_4)^{G_\iota}$.

We start by studying the isomorphism $\Gamma(D_4 * D_4)^{\widetilde{K}_F} \simeq \Gamma(D_2 * D_2)$. What is the action of $\iota^* \otimes 1$ on $\Gamma(D_2 * D_2)$ through the isomorphism? Let $(R, S) \in E \times E$ and $(P, Q) \in E \times E$ such that $F(P, Q) = (R, S) = (P + Q, P - Q)$, $s \in \Gamma(D_2 * D_2)$. Then $(\iota^* \otimes 1) \cdot F^* s(P, Q) = F^* s(-P, Q)$, and

$F(-P,Q) = (-P+Q, -P-Q) = (-S,-R)$, hence $(\iota^* \otimes 1)\cdot F^* s(P,Q) = s(-S,-R)$. Similarly, $(1\otimes \iota^*)\cdot F^* s(P,Q) = s(S,R)$ and $(\iota^*\otimes\iota^*)\cdot F^* s(P,Q) = s(-R,-S)$. Therefore, firstly we have

$$\left(\Gamma(D_4 * D_4)^{\widetilde{K}_F}\right)^{G_\iota} = \left(\Gamma(D_4 * D_4)^{G_\iota}\right)^{\widetilde{K}_F} = \left(\Gamma(D_4 * D_4)^{++}\right)^{\widetilde{K}_F}$$

by Lemma 5.10, and secondly since all elements of $\Gamma(D_2 * D_2)$ are even, if $\tau : (R,S) \mapsto (S,R)$, we have

$$\left(\Gamma(D_4 * D_4)^{+}\right)^{\widetilde{K}_F} \simeq \Gamma(D_2 * D_2) \text{ and } \left(\Gamma(D_4 * D_4)^{++}\right)^{\widetilde{K}_F} \simeq \Gamma(D_2 * D_2)^{\tau^*}.$$

In particular, when looking for differential addition formulas with only X and Z coordinates, we cannot choose whichever section of $\Gamma(D_2 * D_2)$ we want, it must be invariant by permutation of R and S.

The situation is easier regarding Φ because it is a diagonal isogeny, hence one can check

$$\left(\Gamma(D_4 * D_4)^{++}\right)^{\widetilde{K}_\Phi} \simeq \Gamma(D_2' * D_2').$$

If we go down one more level however, the invariance by τ is automatic:

$$\Gamma(D_2 * D_2)^{\widetilde{K}_{\Phi_0}} \simeq \left(\Gamma(D_4 * D_4)^{++}\right)^{\widetilde{K}_G} \simeq \Gamma(D_2' * D_2')^{\widetilde{K}_{F_0}}.$$

In summary, the full set of differential addition formulas $\Gamma(D_4 * D_4)^{\widetilde{K}_F}$ is of dimension 4 and is automatically given by even sections. However, if we want to remove the section $T_P T_Q$ which cannot be computed from X_P, Z_P, X_Q, Z_Q, we need to work with the dimension 3 subspace $\left(\Gamma(D_4 * D_4)^{++}\right)^{\widetilde{K}_F}$. On the codomain of F, this corresponds to level 2 sections of $(R = P+Q, S = P-Q)$ that are also invariant by the permutation of R, S, for instance $X_R X_S, Z_R Z_S, X_R Z_S + Z_R X_S$, but not $X_R Z_S$. Finally, the half differential addition formulas correspond to sections in $\Gamma(D_4 * D_4)^{\widetilde{K}_G} \simeq \Gamma(D_2 * D_2)^{\widetilde{K}_{\Phi_0}}$, this is a space of dimension 2 which is automatically inside $\Gamma(D_4 * D_4)^{++}$.

5.3.7. *Finding formulas.* This is all we required to find our half differential addition formulas. Assume $E[2] = \{\mathcal{O}_E, T_1, T_2, T_3\}$ with T_1 being rational, the method is then as follows:

(1) Set $T = T_1$ such that $\ker\varphi = \{\mathcal{O}_E, T\}$, we first compute the translation by T on the Kummer line associated to E, denoted t_T. If $T' = \varphi(T_2) = \varphi(T_3)$, we compute the translation by T' on the Kummer line associated to E', denoted $t_{T'}$. By considering the affine lifts of these translations, we derive the types of T and T', denoted λ_T and $\lambda_{T'}$.
(2) Compute the invariant subspaces $\Gamma(D_2 * D_2)^{\widetilde{K}_{\Phi_0}}$ and $\Gamma(D_2' * D_2')^{\widetilde{K}_{F_0}}$.
(3) Find the coefficients relating the bases of $\Gamma(D_2 * D_2)^{\widetilde{K}_{\Phi_0}}$ and $\Gamma(D_2' * D_2')^{\widetilde{K}_{F_0}}$.

Remark 5.11. *If $\Gamma(D_2 * D_2)^{\widetilde{K}_{\Phi_0}} = \langle u_1, u_2\rangle$ and $\Gamma(D_2' * D_2')^{\widetilde{K}_{F_0}} = \langle v_1, v_2\rangle$, we then know there are relations*

$$\begin{cases} u_1(P+Q,P-Q) = \alpha_1 v_1(\varphi(P),\varphi(Q)) + \alpha_2 v_2(\varphi(P),\varphi(Q)), \\ u_2(P+Q,P-Q) = \beta_1 v_1(\varphi(P),\varphi(Q)) + \beta_2 v_2(\varphi(P),\varphi(Q)). \end{cases}$$

For our purpose, we consider these relations projectively, so we can multiply u_1 and u_2 by a same factor.

In the first step, we compute $t_T : \mathbb{P}^1 \to \mathbb{P}^1$ projectively, let $\widetilde{t}_T : k^2 \to k^2$ be an affine lift. Then $\widetilde{t}_T^2 = \lambda_T \,\mathrm{id}$. The map $\tau_T = \frac{1}{\lambda_T}(\widetilde{t}_T^* \otimes \widetilde{t}_T^*)$ is an involution of $k(E)\otimes k(E)$. Assume we

have $\widetilde{u} \in \Gamma(D_2 * D_2)$ *such that* $\tau_T(\widetilde{u}) = \widetilde{u}$. *Then, for* $g_{(T,T)} \in \widetilde{K}_{\Phi_0}$ *above* (T,T), *we have* $g_{(T,T)} \cdot \widetilde{u} = g^{-1}_{(T,T)}\lambda_T\tau_T(\widetilde{u}) = g^{-1}_{(T,T)}\lambda_T\widetilde{u}$, *and an element* u *invariant by* $g_{(T,T)}$ *is given by*

$$u := (1 + \lambda_T g^{-1}_{(T,T)})\widetilde{u}.$$

This is how we deal with the second step, we compute two invariants by τ_T, *which projectively will lead to the same result as invariants by* $g_{(T,T)}$ *would have. The same holds for the point* T'.

In the next section we will finally look at an example.

5.4. **Example.** In this example, we will consider the theta model $\theta(a : b)$ associated to E given by 2-torsion points

$$\mathcal{O} = (a : b)^*, \qquad T_1 = (-a : b), \qquad T_2 = (b : a), \qquad T_3 = (-b : a),$$

where $\frac{a}{b} \in k$. The 2-isogeny will be $\varphi : (X : Z) \mapsto (X^2 : Z^2)$. Its kernel is given by $T = T_1$. The Kummer line on the image has ramification points

$$\mathcal{O}' = (a^2 : b^2)^*, \qquad T_1' = (b^2 : a^2), \qquad T_2' = (1 : 0), \qquad T_3' = (0 : 1),$$

this is the theta squared model $\theta_s(a^2 : b^2)$, the interesting 2-torsion point on this model is $T' = \varphi(T_2) = \varphi(T_3) = T_1'$.

As given in Example 2.4, the translations by T and T' on their respective model are $t_T : (X : Z) \mapsto (-X : Z)$ and $t_{T'} : (X : Z) \mapsto (Z : X)$. We consider the affine lifts $\widetilde{t}_T : (X, Z) \mapsto (-X, Z)$ and $\widetilde{t}_{T'} : (X, Z) \mapsto (Z, X)$. The types are then $\lambda_T = \lambda_{T'} = 1$, we set $\tau_T = \widetilde{t}^*_T \otimes \widetilde{t}^*_T$ and $\tau_{T'} = \widetilde{t}^*_{T'} \otimes \widetilde{t}^*_{T'}$.

We will work with the following basis on $\Gamma(D_2 * D_2)$, where $(R, S) = (P + Q, P - Q)$ and $(P, Q) \in E \times E$:

$$\Gamma(D_2 * D_2) = \begin{pmatrix} X_R X_S & X_R Z_S \\ Z_R X_S & Z_R Z_S \end{pmatrix}.$$

τ_T acts as follows on $\Gamma(D_2 * D_2)$:

- $\tau_T(X_R X_S) = X_{R+T} X_{S+T} = (-X_R)(-X_S) = X_R X_S$,
- $\tau_T(X_R Z_S) = X_{R+T} Z_{S+T} = -X_R Z_S$,
- $\tau_T(Z_R X_S) = Z_{R+T} X_{S+T} = -Z_R X_S$,
- $\tau_T(Z_R Z_S) = Z_{R+T} Z_{S+T} = Z_R Z_S$.

$X_R X_S$ and $Z_R Z_S$ are invariant sections, and since $\Gamma(D_2 * D_2)^{\widetilde{K}_{\Phi_0}}$ is of dimension 2, we get

$$\Gamma(D_2 * D_2)^{\widetilde{K}_{\Phi_0}} = \langle X_R X_S, Z_R Z_S \rangle.$$

Regarding $\Gamma(D_2' * D_2')$, we will use the following basis instead:

$$\begin{pmatrix} (X_{\varphi(P)} + Z_{\varphi(P)})(X_{\varphi(Q)} + Z_{\varphi(Q)}) & (X_{\varphi(P)} + Z_{\varphi(P)})(X_{\varphi(Q)} - Z_{\varphi(Q)}) \\ (X_{\varphi(P)} - Z_{\varphi(P)})(X_{\varphi(Q)} + Z_{\varphi(Q)}) & (X_{\varphi(P)} - Z_{\varphi(P)})(X_{\varphi(Q)} - Z_{\varphi(Q)}) \end{pmatrix}.$$

The reason is that the computations with $\tau_{T'}$ are easier. We get two invariants of $\Gamma(D_2 * D_2)^{\widetilde{K}_{F_0}}$:

$$\langle (X_{\varphi(P)} + Z_{\varphi(P)})(X_{\varphi(Q)} + Z_{\varphi(Q)}), (X_{\varphi(P)} - Z_{\varphi(P)})(X_{\varphi(Q)} - Z_{\varphi(Q)}) \rangle.$$

We now set, for $(P, Q) \in E \times E$ and $(R, S) = (P + Q, P - Q)$:

- $u_1(P, Q) = X_R X_S$,
- $u_2(P, Q) = Z_R Z_S$,
- $v_1(P, Q) = (X_{\varphi(P)} + Z_{\varphi(P)})(X_{\varphi(Q)} + Z_{\varphi(Q)})$,
- $v_2(P, Q) = (X_{\varphi(P)} - Z_{\varphi(P)})(X_{\varphi(Q)} - Z_{\varphi(Q)})$,

By the theory, there are constants $\alpha_1, \alpha_2, \beta_1, \beta_2 \in k$ such that for any $(P, Q) \in E \times E$:

$$(u_1(P,Q) : u_2(P,Q)) = (\alpha_1 v_1(P,Q) + \alpha_2 v_2(P,Q) : \beta_1 v_1(P,Q) + \beta_2 v_2(P,Q)).$$

We then evaluate at specific points to get relations on the coefficients. On the theta model $\theta(a : b)$, we denote by $\overline{T_1} = (1 : 0)$ and $\underline{T_1} = (0 : 1)$ the 4-torsion points above T_1, and the usual $(A^2 : B^2) = (a^2 + b^2 : a^2 - b^2)$.

(1) If $(P, Q) = (\mathcal{O}, \mathcal{O})$, then $(R, S) = (\mathcal{O}, \mathcal{O})$ and $(\varphi(P), \varphi(Q)) = (\mathcal{O}', \mathcal{O}')$:
$$(a^2 : b^2) = (\alpha_1 A^4 + \alpha_2 B^4 : \beta_1 A^4 + \beta_2 B^4).$$
(2) If $(P, Q) = (\overline{T_1}, \mathcal{O})$, then $(R, S) = (\overline{T_1}, \overline{T_1})$ and $(\varphi(P), \varphi(Q)) = (T_2', \mathcal{O}')$:
$$(1 : 0) = (\alpha_1 A^2 + \alpha_2 B^2 : \beta_1 A^2 + \beta_2 B^2).$$
(3) If $(P, Q) = (\underline{T_1}, \mathcal{O})$, then $(R, S) = (\underline{T_1}, \underline{T_1})$ and $(\varphi(P), \varphi(Q)) = (T_3', \mathcal{O}')$:
$$(0 : 1) = (\alpha_1 A^2 - \alpha_2 B^2 : \beta_1 A^2 - \beta_2 B^2).$$

The second and third relations give $\beta_1 A^2 = -\beta_2 B^2$ and $\alpha_1 A^2 = \alpha_2 B^2$. When injected in the first one, we get

$$(a^2 : b^2) = (\alpha_2 B^2 (A^2 + B^2) : -\beta_2 B^2 (A^2 - B^2)) = (\alpha_2 a^2 : -\beta_2 b^2).$$

Hence, $\alpha_2 = -\beta_2$ and we can derive the general formula from these relations:

$$\begin{aligned}(\alpha_1 v_1 + \alpha_2 v_2 : \beta_1 v_1 + \beta_2 v_2) &= (\alpha_1 A^2 v_1 + \alpha_2 A^2 v_2 : \beta_1 A^2 v_1 + \beta_2 A^2 v_2) \\ &= (\alpha_2 (B^2 v_1 + A^2 v_2) : \beta_2 (-B^2 v_1 + A^2 v_2)) = (B^2 v_1 + A^2 v_2 : B^2 v_1 - A^2 v_2).\end{aligned}$$

Thus, the formulas $\texttt{HalfDiffAdd}_\varphi(\varphi(P), \varphi(Q), S)$ associated to φ are:

$$(X_R X_S : Z_R Z_S) = \begin{pmatrix} B^2 (X_{\varphi(P)} + Z_{\varphi(P)})(X_{\varphi(Q)} + Z_{\varphi(Q)}) + A^2 (X_{\varphi(P)} - Z_{\varphi(P)})(X_{\varphi(Q)} - Z_{\varphi(Q)}) \\ B^2 (X_{\varphi(P)} + Z_{\varphi(P)})(X_{\varphi(Q)} + Z_{\varphi(Q)}) - A^2 (X_{\varphi(P)} - Z_{\varphi(P)})(X_{\varphi(Q)} - Z_{\varphi(Q)}) \end{pmatrix}.$$

Remark 5.12 (Montgomery differential addition)**.** *On a Montgomery Kummer line given by*

$$(1 : 0)^*, \qquad (0 : 1), \qquad (a : b), \qquad (b : a)$$

where $\frac{a}{b}$ may not be rational, the translation by $T = (0 : 1)$ is $t_T : (X : Z) \mapsto (Z : X)$. As we have seen above, $X_R X_S$ and $Z_R Z_S$ are not invariant by this translation if $(R, S) = (P + Q, P - Q)$. This means that we cannot factor the traditional differential addition formulas into half differential addition formulas. We can still find new formulas like the ones given in Section 4.2 on `Curve25519`*, but they are not as efficient as the usual ones.*

References

[Ber06] Daniel J. Bernstein. "Curve25519: New Diffie-Hellman Speed Records". In: *PKC 2006*. Ed. by Moti Yung, Yevgeniy Dodis, Aggelos Kiayias, and Tal Malkin. Vol. 3958. LNCS. Springer, Berlin, Heidelberg, Apr. 2006, pp. 207–228. DOI: 10.1007/11745853_14.

[CC86] D.V Chudnovsky and G.V Chudnovsky. "Sequences of numbers generated by addition in formal groups and new primality and factorization tests". In: *Advances in Applied Mathematics* 7.4 (1986), pp. 385–434. ISSN: 0196-8858. DOI: 10.1016/0196-8858(86)90023-0.

[CS18] Craig Costello and Benjamin Smith. "Montgomery curves and their arithmetic - The case of large characteristic fields". In: *Journal of Cryptographic Engineering* 8.3 (Sept. 2018), pp. 227–240. DOI: 10.1007/s13389-017-0157-6.

[Dar+24] Pierrick Dartois, Luciano Maino, Giacomo Pope, and Damien Robert. "An Algorithmic Approach to (2, 2)-isogenies in the Theta Model and Applications to Isogeny-based Cryptography". Aug. 2024.

[GL09] Pierrick Gaudry and David Lubicz. "The arithmetic of characteristic 2 Kummer surfaces and of elliptic Kummer lines". In: *Finite Fields Their Appl.* 15.2 (2009), pp. 246–260. DOI: 10.1016/J.FFA.2008.12.006.

[Mon87] Peter L. Montgomery. "Speeding the Pollard and elliptic curve methods of factorization". English. In: *Mathematics of Computation* 48 (1987), pp. 243–264. ISSN: 0025-5718. DOI: 10.2307/2007888.

[Mum66] David Mumford. "On the Equations Defining Abelian Varieties. I." In: *Inventiones mathematicae* 1 (1966), pp. 287–354.

[Oli+17] Thomaz Oliveira, Julio Cesar López-Hernández, Hüseyin Hisil, Armando Faz-Hernández, and Francisco Rodríguez-Henríquez. "How to (Pre-)Compute a Ladder - Improving the Performance of X25519 and X448". In: *SAC 2017*. Ed. by Carlisle Adams and Jan Camenisch. Vol. 10719. LNCS. Springer, Cham, Aug. 2017, pp. 172–191. DOI: 10.1007/978-3-319-72565-9_9.

[Ren+16] Joost Renes, Peter Schwabe, Benjamin Smith, and Lejla Batina. "μKummer: Efficient Hyperelliptic Signatures and Key Exchange on Microcontrollers". In: *CHES 2016*. Ed. by Benedikt Gierlichs and Axel Y. Poschmann. Vol. 9813. LNCS. Springer, Berlin, Heidelberg, Aug. 2016, pp. 301–320. DOI: 10.1007/978-3-662-53140-2_15.

[Res18] Eric Rescorla. *The Transport Layer Security (TLS) Protocol Version 1.3*. Aug. 2018. DOI: 10.17487/RFC8446. URL: https://www.rfc-editor.org/info/rfc8446.

[RS24] Damien Robert and Nicolas Sarkis. "Computing 2-isogenies between Kummer lines". In: *IACR Communications in Cryptology* 1.1 (Apr. 9, 2024). ISSN: 3006-5496. DOI: 10.62056/abvua69p1.

[SB01] Hovav Shacham and Dan Boneh. "Improving SSL Handshake Performance via Batching". In: *CT-RSA 2001*. Ed. by David Naccache. Vol. 2020. LNCS. Springer, Berlin, Heidelberg, Apr. 2001, pp. 28–43. DOI: 10.1007/3-540-45353-9_3.

[The24] The Stacks project authors. *The Stacks project*. 2024. URL: https://stacks.math.columbia.edu.

Appendix A. Half differential additions for abelian varieties in the theta model

The arithmetic of theta function comes from the duplication formula, which can naturally be expressed as `HalfDiffAdd` operations. In this section, we give half differential addition formulas in any dimension, for level 2 theta coordinates. Then we look at the impact of half ladder on the efficiency for abelian surfaces, compared to the standard ladder as introduced in [CC86; GL09].

Let $(A, \mathcal{L}, \Theta_A)$ be a principally polarized abelian variety with a symmetric level 2 theta structure. We let $\theta_i, i \in (\mathbb{Z}/2\mathbb{Z})^g$ be the basis of theta functions of level 2. We also let $\varphi : A \to A'$ be the canonical isogeny induced from the theta structure, and a choice of compatible level 2 theta structure on A', with dual theta functions θ'_i.

Then we have the key formula, used in [Dar+24] to derive efficient 2^n-isogeny formulas.

$$(\theta_i(P+Q))_i \star (\theta_i(P-Q))_i = H((\theta'_i(\varphi(P))) \star (\theta'_i(\varphi(Q)))) \tag{4}$$

Here $(\theta_i(P))_i \star (\theta_i(P))_i$ denotes the component wise product $(\theta_i(P)\theta_i(Q))_i$, and H is the Hadamard transform.

From the knowledge of the theta constant $\theta_i(0)$ on A and the dual theta constants $\theta'_i(0)$ on A', it is possible to both compute the dual theta coordinates $\theta'_i(\varphi(P))$ from the theta coordinates of P (by setting $Q = 0$ in Eq. (4)), and to use Eq. (4) as a half differential addition formula.

In this section, we will assume that these constants are rational; we leave to the reader the adaptation of the higher dimensional half ladder to the theta twisted model, as in Algorithm 3.

Assuming that the theta null points of A and A' have been normalized and their inverse computed (this is a pre-computation which does not depend on the choice of base point P for the ladder), then an isogeny image costs $2^g\mathbf{S} + (2^g - 1)\mathbf{m}_0$, a half doubling costs $2^g\mathbf{S} + (2^g - 1)\mathbf{m}_0$, and a half differential addition costs $2^g\mathbf{M} + 2^g\mathbf{I}$. In dimension 1, since we are working with projective coordinates, these $2\mathbf{I}$ could be easily replaced by $2\mathbf{M}$. This is not the case any more in dimension > 1: the $2^g\mathbf{I}$ can only be replaced by $(2^{g+2} - 6)\mathbf{M}$. This means that in the half ladder, it is quite expensive to use non-normalized pre-computed points P_i, and so it will become interesting only when doing a full normalized pre-computation.

In the standard ladder, at each step we compute two isogeny images, one half doubling and one half differential addition. The differential addition is always done with the same base point P has difference, so via a pre-computation at the start to normalize P these $2^g\mathbf{I}$ become $(2^g - 1)\mathbf{M}$. The total cost is then $(2^{g+1} - 1)\mathbf{M} + 3.2^g\mathbf{S} + 3(2^g - 1)\mathbf{m}_0$ by bit. Using twisted theta coordinates, we have a $(2^g - 1)(\mathbf{M} - \mathbf{S} - \mathbf{m}_0)$ trade-off, which gives a complexity of $(3 \cdot 2^g - 2)\mathbf{M} + (2^{g+1} + 1)\mathbf{S} + 2(2^g - 1)\mathbf{m}_0$ by bit.

In the half ladder, we first compute iterated isogeny images $P_i = \varphi_i(P_{i-1})$ (one by bit), and then at each step we do one half doubling and one half differential additions. Then we use one half doubling $2U_{i-1} = \texttt{HalfDouble}_{\varphi_i}(\varphi_i(U_{i-1}))$ or $2V_{i-1} = \texttt{HalfDouble}_{\varphi_i}(\varphi_i(V_{i-1}))$ and one half differential addition $U_{i-1} + V_{i-1} = \texttt{HalfDiffAdd}_{\varphi_i}(\varphi_i(U_{i-1}), \varphi_i(V_{i-1}), U_{i-1} - V_{i-1})$, where $U_{i-1} - V_{i-1} = P_{i-1}$ has been pre-computed.

This time, the pre-computation to normalize each P_i is much more expensive: one global inversion and around $4(2^g - 1) - 3$ multiplications. However, we note that the P_i only depend on P (and the scalar bit length), not on the actual scalar, so this pre-computation can be reused whenever we do several scalar multiplications with the same base point P. Taking into account the isogeny images, the global cost is one global inversion and $(4(2^g - 1) - 3)\mathbf{M} + 2^g\mathbf{S} + (2^g - 1)\mathbf{m}_0$ by bit for the pre-computations, which only depends on the base point P, and then $(2^{g+1} - 1)\mathbf{M} + 2^g\mathbf{S} + (2^g - 1)\mathbf{m}_0$ by bits for the scalar exponentiations $m \mapsto mP$.

We remark that in the right to left Montgomery ladder, we have the same normalization problem, except that here the base points used in the differential addition formulas depend on the scalar n, so it is not possible to share the pre-computation once and for all. Indeed, the right to left ladder uses normal differential addition of the form $U_i + V_i = \texttt{DiffAdd}(U_i, V_i, U_i - V_i)$ where this time it is $U_i = 2^i P$ which has been pre-computed, rather than the difference $U_i - V_i$.

In Table 5, we put a comparison of the cost between the ladder and half ladder for abelian surfaces. We remark that the $3\mathbf{m}$ in the standard Montgomery ladder assume that the base point P is normalized and that the $1/\theta_i(P)$ have been computed; otherwise these become $6\mathbf{M}$. If the theta constants are small, we can replace the $7\mathbf{M} + 9\mathbf{S} + 3\mathbf{m} + 6\mathbf{m}_0$ cost by $4\mathbf{M} + 12\mathbf{S} + 3\mathbf{m} + 9\mathbf{m}_0$.

As we see from this table, unlike the case of dimension 1 where the pre-computation was so cheap the half ladder was still more efficient than the standard ladder even when including the pre-computation cost, in dimension 2 using the half ladder is only interesting when the same base point P will be reused several times. This will be the case for instance in signature schemes like μ-Kummer [Ren+16].

Algorithm	Pre-computation	Normalization	Step
Montgomery Ladder LtR	—	—	$7\mathbf{M} + 9\mathbf{S} + 3\mathbf{m} + 6\mathbf{m}_0$
Half ladder, our contribution	$2\mathbf{S} + 1\mathbf{m}_0$	$3\mathbf{I} + 3\mathbf{M} \overset{\text{asy}}{=} 12\mathbf{M}$	$7\mathbf{M} + 4\mathbf{S} + 3\mathbf{m}_0$

TABLE 5. Ladder costs per bit for the half ladder in dimension 2

Appendix B. Computations on Curve25519

In this section, we detail how we obtain half differential addition formulas over a Montgomery Kummer line $M(A:B)$ with ramification

$$(1:0)^*, \qquad (0:1), \qquad (A:B), \qquad (B:A),$$

but where $\frac{A}{B}$ may not be rational. We further assume there is a 8-torsion point $(r:s)$ above $(1:1)$, itself above $(0:1)$. `Curve25519` for instance verifies such hypotheses. We set the following additional constants: $(\gamma:\delta) = (4rs : (r-s)^2)$ and $(a:b) = (\gamma-\delta : \gamma+\delta)$. The 2-isogeny with kernel $T = (0:1)$ we are interested in is

$$\psi : (X:Z) \mapsto (ab(X-Z)^2 - a\delta(X+Z)^2 : ab(X-Z)^2 + b\delta(X+Z)^2).$$

Its dual is given by

$$\widetilde{\psi} : (X:Z) \mapsto (aZ^2 - bX^2 + 2\delta XZ : aZ^2 - bX^2 - 2\delta XZ).$$

The translation by T on $M(A:B)$ is simply $t_T : (X:Z) \mapsto (Z:X)$ as explained in Example 2.4.1, with affine lift $\widetilde{t}_T : (X,Z) \mapsto (Z,X)$. The image is the theta twisted model $\theta_t(a:b)$ with ramification

$$(a:b)^*, \qquad (-a:b), \qquad (1:1), \qquad (-1:1).$$

Recall these are derived from [RS24, Thm. 4.11, Prop. 4.12] and the composition with isomorphisms from Example 2.4.4 between theta twisted and Montgomery models.

We have:

- $\psi(1:0) = \psi(0:1) = (a:b)$,
- $\psi(A:B) = \psi(B:A) = (-1:1)$,
- $\psi(1:1) = (-a:b)$,
- $\psi(-1:1) = (1:1)$.

The point of interest on $\theta_t(a:b)$ is then $T' = (-1:1)$. We want to compute $t_{T'}$. It is a homography of $\mathbb{P}^1$, which must verify:

$$t_{T'}(a:b) = (-1:1),\ t_{T'}(-1:1) = (a:b),\ t_{T'}(-a:b) = (1:1),\ t_{T'}(1:1) = (-a:b).$$

This leads to $t_{T'} : (X:Z) \mapsto (-aZ : bX)$, its affine lift is $\widetilde{t}_{T'} : (X,Z) \mapsto (-aZ, bX)$.

We have $\widetilde{t}_T^2 = \mathrm{id}$ so $\lambda_T = 1$ and $\widetilde{t}_{T'}^2 = -ab\,\mathrm{id}$, so $\lambda_{T'} = -ab$. We set $\tau_T = \widetilde{t}_T^* \otimes \widetilde{t}_T^*$ and $\tau_{T'} = \frac{1}{-ab}\widetilde{t}_{T'}^* \otimes \widetilde{t}_{T'}^*$. This is part of the reason we wanted to illustrate this example where the type has no reason to be a square, and we have to consider it in the computations. We work with the usual bases of $\Gamma(D_2 * D_2)$ and $\Gamma(D_2' * D_2')$, where $(R,S) = (P+Q, P-Q)$:

$$\Gamma(D_2 * D_2) = \begin{pmatrix} X_R X_S & X_R Z_S \\ Z_R X_S & Z_R Z_S \end{pmatrix}, \ \Gamma(D_2' * D_2') = \begin{pmatrix} X_{\psi(P)} X_{\psi(Q)} & X_{\psi(P)} Z_{\psi(Q)} \\ Z_{\psi(P)} X_{\psi(Q)} & Z_{\psi(P)} Z_{\psi(Q)} \end{pmatrix}.$$

τ_T acts as follows on $\Gamma(D_2 * D_2)$:

- $\tau_T(X_R X_S) = Z_R Z_S$,
- $\tau_T(X_R Z_S) = Z_R X_S$.

This gives two invariants $X_R X_S + Z_R Z_S$ and $X_R Z_S + Z_R X_S$. With some linear algebra, we can derive the two invariants $(X_R + Z_R)(X_S + Z_S)$ and $(X_R - Z_R)(X_S - Z_S)$ (or by checking directly that those are indeed invariant):

$$\Gamma(D_2 * D_2)^{\widetilde{K}_{\Phi_0}} = \langle (X_R + Z_R)(X_S + Z_S), (X_R - Z_R)(X_S - Z_S) \rangle.$$

In the same manner, we look at invariants for $\tau_{T'}$:

- $\tau_{T'}(X_{\psi(P)} X_{\psi(Q)}) = \frac{a^2}{-ab} Z_{\psi(P)} Z_{\psi(Q)} = -\frac{a}{b} Z_{\psi(P)} Z_{\psi(Q)}$,
- $\tau_{T'}(X_{\psi(P)} Z_{\psi(Q)}) = \frac{-ab}{-ab} Z_{\psi(P)} X_{\psi(Q)} = Z_{\psi(P)} X_{\psi(Q)}$.

By rescaling the first invariant, we get the following basis:

$$\Gamma(D_2' * D_2')^{\widetilde{K}_{F_0}} = \langle aZ_{\psi(P)}Z_{\psi(Q)} - bX_{\psi(P)}X_{\psi(Q)}, X_{\psi(P)}Z_{\psi(Q)} + Z_{\psi(P)}X_{\psi(Q)}\rangle.$$

We then set, for $(R,S) = (P+Q, P-Q)$:

- $u_1(P,Q) = (X_R + Z_R)(X_S + Z_S)$,
- $u_2(P,Q) = (X_R - Z_R)(X_S - Z_S)$,
- $v_1(P,Q) = aZ_{\psi(P)}Z_{\psi(Q)} - bX_{\psi(P)}X_{\psi(Q)}$,
- $v_2(P,Q) = X_{\psi(P)}Z_{\psi(Q)} + Z_{\psi(P)}X_{\psi(Q)}$.

We are looking for the constants $\alpha_1, \alpha_2, \beta_1, \beta_2 \in k$ such that:

$$(u_1(P,Q) : u_2(P,Q)) = (\alpha_1 v_1(P,Q) + \alpha_2 v_2(P,Q) : \beta_1 v_1(P,Q) + \beta_2 v_2(P,Q)).$$

Consider $\overline{T} = (1:1)$ and $\underline{T} = (-1:1)$ the 4-torsion points above $T = (0:1)$, then:

- $F(\overline{T}, \mathcal{O}) = (\overline{T}, \overline{T})$, $\psi(\overline{T}) = (-a:b)$, $\psi(\mathcal{O}) = (a:b)$, giving the equation
$$(1:0) = (\alpha_1 ab(b-a) + 0 : \beta_1 ab(b-a) + 0) \implies \beta_1 = 0.$$
- $F(\underline{T}, \mathcal{O}) = (\underline{T}, \underline{T})$, $\psi(\underline{T}) = (1:1)$, $\psi(\mathcal{O}) = (a:b)$, giving the equation
$$(0:1) = (0 + \alpha_2(a+b) : \beta_2(a+b)) \implies \alpha_2 = 0.$$
- $F(\underline{T}, \underline{T}) = (T, \mathcal{O})$, $\psi(\underline{T}) = (1:1)$, giving the equation
$$(1:-1) = (\alpha_1(a-b) : 2\beta_2) \implies \alpha_1(b-a) = 2\beta_2 \implies \beta_2 = \delta\beta_1.$$

The half differential addition formulas $\texttt{HalfDiffAdd}_\psi(\psi(P), \psi(Q), P-Q)$ are then:

$$((X_R + Z_R)(X_S + Z_S) : (X_R - Z_R)(X_S - Z_S)) = \begin{pmatrix} aZ_{\psi(P)}Z_{\psi(Q)} - bX_{\psi(P)}X_{\psi(Q)} \\ \delta(X_{\psi(P)}Z_{\psi(Q)} + Z_{\psi(P)}X_{\psi(Q)}) \end{pmatrix}.$$

Univ. Bordeaux, CNRS, INRIA, Bordeaux INP, IMB, UMR 5251, INRIA CANARI team, F-33400 Talence, France
Email address: damien.robert@inria.fr
URL: http://www.normalesup.org/~robert/pro

Email address: nicolas.sarkis@math.u-bordeaux.fr
URL: https://nsarkis.pages.math.cnrs.fr/webpage/index.html