On Kummer Lines With Full Rational 2-torsion and Their Usage in Cryptography

Huseyin Hisil[1] and Joost Renes[2*]

[1] Yasar University, Izmir, Turkey
huseyin.hisil@yasar.edu.tr
[2] Digital Security Group, Radboud Universiteit, The Netherlands
j.renes@cs.ru.nl

Abstract. A paper by Karati and Sarkar at Asiacrypt'17 has pointed out the potential for Kummer lines in genus one, by observing that its SIMD-friendly arithmetic is competitive with the status quo. A more recent preprint explores the connection with (twisted) Edwards curves. In this paper we extend this work and significantly simplify their treatment. We show that their Kummer line is the x-line of a Montgomery curve translated by a point of order two, and exhibit a natural isomorphism to a twisted Edwards curve. Moreover, we show that the Kummer line presented by Gaudry and Lubicz can be obtained via the action of a point of order two on the y-line of an Edwards curve. The maps connecting these curves and lines are all very simple. As an example, we present the first implementation of the qDSA signature scheme based on the squared Kummer line. Finally we present close estimates on the number of isomorphism classes of Kummer lines.

Keywords: Montgomery curves, Edwards curves, Kummer lines, Montgomery ladder, Digital signatures

1 Introduction

A decade after the introduction of public-key cryptography by Diffie and Hellman [DH76] it was observed (independently) by Miller [Mil86] and Koblitz [Kob87] that one can instantiate protocols based on the hardness of the discrete logarithm problem with the group of rational points of an elliptic curve E defined over a finite field. Moreover, it was immediately noted by Miller that one can do a full key exchange by solely relying on the line of x-coordinates of points. That is, one can identify points with their inverses and as a result only work with points up to sign. In other words, one can work on the corresponding Kummer line $K = E/\{\pm 1\}$, possibly simplifying the arithmetic. Recently it was shown that one can also directly use K for digital signatures very efficiently with the qDSA scheme [RS17, §2]. In short, Kummer lines are a very interesting topic of study from a cryptographic perspective.

[*] This work has been supported by the Technology Foundation STW (project 13499 - TYPHOON & ASPASIA), from the Dutch government.

Because a reduction in the number of field operations needed for a scalar multiplication directly affects the efficiency of the cryptographic scheme, there have been multiple proposals for Kummer lines. Probably the most available example is Curve25519 [Ber06b], which is the Kummer line of a Montgomery curve. One can show that every Montgomery curve is birationally equivalent to a twisted Edwards curve [BBJ+08, Theorem 3.2], which currently needs the least number of field operations to perform group operations [HWCD08] and underlies the very efficient Four$\mathbb{Q}$ curve [CL15]. As a result, the Kummer lines of Montgomery and twisted Edwards curves are strongly related, and one can move easily from one to the other [BBJ+08, CGF08]. Through the usage of theta functions Gaudry and Lubicz [GL09, §6] derived yet another Kummer line. We shall refer to this as the *canonical* Kummer line, following the terminology of the genus 2 analogue presented by Renes and Smith [RS17, §4]. By squaring its coefficients we arrive on a different variety, which we refer to as the *squared* Kummer line (again c.f. the genus 2 analogue [CC86, Ber06a]). Although Gaudry and Lubicz only presented arithmetic on the canonical line, the differential addition formulae on the squared Kummer line are well-known [BL]. The squared Kummer line has the advantage that it is easier to find suitable small parameters, and it was shown by Karati and Sarkar [KS17b] that its arithmetic leads to very efficient implementations when single-instruction multiple-data (SIMD) instructions are available.

In a follow-up paper [KS17a] the same authors present connections to twisted Edwards curves. This requires the associated Legendre curve to be put in Montgomery form or have a rational point of order 4, or otherwise relies on the usage of a 2-isogeny. Consequently, there are case distinctions and one must deal with the doubling induced by moving through a 2-isogeny and its dual. In [KS17a, Table 7] they present the possibility of birational maps and isogenies between the Legendre form for certain choices of small constants.

In this paper we significantly simplify the connections between the various Kummer lines. Since the field of definition of the canonical and squared Kummer lines corresponds to their rational 2-torsion, we shall assume all points of order 2 to be rational. In that case, we show that the squared (resp. canonical) Kummer arises as the x-line (resp. y-line) of a Montgomery (resp. Edwards) curve translated by a suitable point of order 2. Moreover, a third Kummer line (referred to as the *intermediate* Kummer) appears as the y-line of a *twisted* Edwards curve via a translation by a point of order 2. These observations induce very simple isomorphisms between them. Furthermore, the respective translations by a point of order 2 lead to fast isomorphisms (in fact, involutions) with the well-known x-lines (or y-lines) of Montgomery, Edwards and twisted Edwards curves. As a result, we unify the most popular Kummer lines in the literature and conclude that their usage is completely interchangeable on an implementation level. For example, we can directly use the squared Kummer line in the qDSA scheme through its connection with a Montgomery curve [RS17, §3]. Moreover, although there exist efficient implementations of Montgomery curves based on 4-way SIMD parallelization by optimizing the field arithmetic [FL15], it is unclear how to optimally parallelize instructions 4-way on the level of the x-line [Cho15]. This is straightforward on the squared Kummer line, and therefore by extension becomes trivial on Montgomery curves with full rational 2-torsion by moving through the isomorphism. Of course, if desired, one can also do arithmetic on the full group of points of the twisted Edwards curve (as also noted by Karati and Sarkar [KS17a]). In particular, we provide isomorphic Montgomery and twisted Edwards models for all the Kummer lines present in [KS17a, Table 7] (see Table 1 in §3.2).

2 Preliminaries

Let k be a field such that $\mathrm{char}(k) \neq 2$. This assumption is implicit in the whole document unless mentioned otherwise. An elliptic curve is a smooth projective curve of genus 1 with a specified base point O, and it is said to be defined over k if E is defined over k and $O \in E(k)$ [Sil09, §III.3]. Its points form an abelian group with neutral element O. One can show [Sil09, Proposition III.3.1] that any elliptic curve defined over k can be put in *Weierstrass form*[3]

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \subset \mathbb{P}^2$$

with $O = (0 : 1 : 0)$, but the curves we consider in this paper are not necessarily in this standard model. If we want to emphasize the base point of the curve we are working with, we shall write (E, O).

Montgomery curves. Let $A, B \in k$ such that $B(A^2 - 4) \neq 0$ and let

$$M/k : By^2 = x^3 + Ax^2 + x$$

be (the affine part of) a smooth projective curve of genus one. We may write $M_{A,B}$ for M to emphasize the coefficients of the curve we are referring to. Denoting $\mathcal{O}_M = (0 : 1 : 0)$, the elliptic curve $(M, \mathcal{O}_M)$ is commonly referred to as a *Montgomery curve* [Mon87] and is ubiquitous in elliptic-curve-based cryptography protocols (see e.g. [Ber06b]). By projecting the points to $\mathbb{P}^1$ via the (surjective) map

$$\begin{aligned} \mathbf{x} : M &\to \mathbb{P}^1 \\ (X : Y : Z) &\mapsto \begin{cases} (X : Z) & \text{if } Z \neq 0 \\ (1 : 0) & \text{if } Z = 0 \end{cases}, \end{aligned}$$

the projective line inherits a pseudo-group structure. That is, by viewing $\mathbb{P}^1$ as the image of $(M, \mathcal{O}_M)$ under $\mathbf{x}$ we obtain the well-known scalar multiplication on

[3] We shall in many cases talk about *affine* curves and maps for simplicity, but always mean their projective counterparts. This depends on the particular embedding of the affine curve into projective space, but it should be clear from context what is meant. In particular, we always embed Montgomery curves into $\mathbb{P}^2$ while (twisted) Edwards curves are embedded into $\mathbb{P}^3$ (as opposed to $\mathbb{P}^1 \times \mathbb{P}^1$, which is also commonplace).

$\mathbb{P}^1$ as first used by Montgomery [Mon87, §10]. Since inversion on (affine points of) $(M, \mathcal{O}_M)$ is simply negation of the y-coordinate, it is immediate that $\mathbf{x}$ is well-defined on $(M, \mathcal{O}_M)/\{\pm 1\}$ and induces a bijection between $(M, \mathcal{O}_M)/\{\pm 1\}$ and $\mathbb{P}^1$. We denote the projective line with the induced pseudo-group structure of $(M, \mathcal{O}_M)$ by $K_M^{\mathcal{O}_M}$, and refer to it as its Kummer line.

Now suppose that $T \in (M, \mathcal{O}_M)$ is a point such that $[2]T = \mathcal{O}_M$. Then the translation-by-T map

$$\begin{aligned} \tau_T : (M, \mathcal{O}_M) &\to (M, T) \\ P &\mapsto P + T \end{aligned}$$

is an isomorphism of elliptic curves. Moreover, the map $\mathbf{x}$ is again well-defined on $(M, T)/\{\pm 1\}$ and we denote its Kummer line by K_M^T. In summary, we have a commutative diagram

$$\begin{tikzcd}
(M, \mathcal{O}_M) \arrow[r, leftrightarrow, "\tau_T"] \arrow[d, "\mathbf{x}"] & (M, T) \arrow[d, "\mathbf{x}"] \\
K_M^{\mathcal{O}_M} \arrow[r, leftrightarrow, "\overline{\tau}_T"] & K_M^T
\end{tikzcd}$$

where $\overline{\tau}_T$ is the induced isomorphism (again, involution) between the corresponding Kummer lines. For example, we obtain the map $\overline{\tau}_{(0,0)} : (X : Z) \mapsto (Z : X)$. Since $\#(M, \mathcal{O}_M)[2] = 4$, there are at most two other points of order 2. This gives rise to only a single non-trivial action on the Kummer line $K_M^{\mathcal{O}_M}$, since the other is simply the composition with $\overline{\tau}_{(0,0)}$.

Twisted Edwards curves. Let $\alpha, \delta \in k$ such that $\alpha\delta(\alpha - \delta) \neq 0$ and let

$$\alpha x^2 + y^2 = 1 + \delta x^2 y^2$$

be (the affine part of) a smooth projective curve of genus one. This is commonly referred to as the *twisted Edwards* model [BBJ+08], where the base point is chosen as $\mathcal{O}_E = (0, 1)$. It is closely related to a Montgomery curve via a birational map [BBJ+08, Theorem 3.2(i)].

Embedding the curve into $\mathbb{P}^2$ via $(x, y) \mapsto (x : y : 1)$ gives two singularities at $(1 : 0 : 0)$ and $(0 : 1 : 0)$. We can resolve these by blowing up (see e.g. [His10, §2.3.4] or [Gal12, Lemma 9.12.18]) to obtain the curve

$$E/k = V(\alpha X^2 + Y^2 - Z^2 - \delta T^2, XY - TZ) \subset \mathbb{P}^3 \qquad (1)$$

and embedding $(x, y) \mapsto (xy : x : y : 1)$. When referring to twisted Edwards curves, we will mean its embedding into $\mathbb{P}^3$ conform (1) and may write $E_{\alpha,\delta}$ to emphasize its coefficients. For affine points we will sometimes use the affine notation and expect that this should not cause confusion. Note that this is a purely theoretical tool, since once all is set and done the cryptographically relevant arithmetic is performed in a prime order subgroup in which all points are affine. On E there exist 4 points at infinity

$$\begin{aligned} \mathit{\Omega}_1 &= (1 : \sqrt{\delta/\alpha} : 0 : 0)\,, & \mathit{\Omega}_2 &= (1 : -\sqrt{\delta/\alpha} : 0 : 0)\,, \\ \omega_1 &= (1 : 0 : \sqrt{\delta} : 0)\,, & \omega_2 &= (1 : 0 : -\sqrt{\delta} : 0)\,, \end{aligned}$$

where $\mathit{\Omega}_1, \mathit{\Omega}_2$ have order 2 and ω_1, ω_2 have order 4 on $(E, \mathcal{O}_E)$.

Similar to the **x**-map for Montgomery curves arising as a projection away from $\mathcal{O}$, we have a **y**-map

$$\begin{aligned} \mathbf{y} : E &\to \mathbb{P}^1 \\ (T : X : Y : Z) &\mapsto (Y : Z)\,, \\ (\mathit{\Omega}_1, \mathit{\Omega}_2) &\mapsto \Big((1 : \sqrt{\delta/\alpha}), (1 : -\sqrt{\delta/\alpha})\Big) \end{aligned}$$

corresponding to projection away from $\mathit{\Omega}_1$. Since inversion in this case is negation of the x-coordinate, this map is well-defined on $(E, \mathcal{O}_E)/\{\pm 1\}$ and we denote the Kummer line by $K_E^{\mathcal{O}_E}$. The point $S = (0 : 0 : -1 : 1)$ of order 2 induces the commutative diagram

$$\begin{tikzcd} (E, \mathcal{O}_E) \arrow[r, leftrightarrow, "\tau_S"] \arrow[d, "\mathbf{y}"] & (E, S) \arrow[d, "\mathbf{y}"] \\ K_E^{\mathcal{O}_E} \arrow[r, leftrightarrow, "\overline{\tau}_S"] & K_E^S \end{tikzcd} \tag{2}$$

where $\overline{\tau}_S : (Y : Z) \mapsto (-Y : Z)$. The two other 2-torsion points induce one other non-trivial translation (analogous to the Montgomery model).

Edwards curves. Let $c \in \bar{k}$ such that $c^5 \neq c$ and

$$\mathcal{E} : x^2 + y^2 = c^2(1 + x^2y^2)$$

again a smooth curve of genus 1. This is technically only a subset of the set of curves of the form $x^2 + y^2 = c^2(1 + dx^2y^2)$ originally defined as Edwards curves by Bernstein and Lange [BL07]. But in this paper we are only concerned with the case $d = 1$, which corresponds to the form introduced by Edwards [Edw07], who observed that its arithmetic with respect to the base point $\mathcal{O}_{\mathcal{E}} = (0, c)$ is extremely symmetric. As above, we use the smooth model inside $\mathbb{P}^3$ containing the elements

$$\begin{aligned} \mathit{\Theta}_1 &= (1 : c : 0 : 0)\,, & \mathit{\Theta}_2 &= (1 : -c : 0 : 0) \\ \theta_1 &= (1 : 0 : c : 0)\,, & \theta_2 &= (1 : 0 : -c : 0)\,, \end{aligned}$$

where $\mathit{\Theta}_1, \mathit{\Theta}_2$ resp. θ_1, θ_2 have order 2 resp. 4 on $(\mathcal{E}, \mathcal{O}_{\mathcal{E}})$. Again, we have a projection to $\mathbb{P}^1$

$$\begin{aligned} \mathbf{y} : \mathcal{E} &\to \mathbb{P}^1 \\ (T : X : Y : Z) &\mapsto (Y : Z) \\ (\mathit{\Theta}_1, \mathit{\Theta}_2) &\mapsto ((1 : c), (1 : -c))\ . \end{aligned}$$

We denote the Kummer line of $(\mathcal{E}, \mathcal{O}_\mathcal{E})$ obtained by projection through $\mathbf{y}$ by $K_\mathcal{E}^{\mathcal{O}_\mathcal{E}}$. For any point 2-torsion point R of $(\mathcal{E}, \mathcal{O}_\mathcal{E})$ we obtain a commutative diagram as in (2) by translation by R and denote the Kummer line by $K_\mathcal{E}^R$.

Rationality and quadratic twists. Suppose that q is a prime power and $k = \mathbb{F}_q$ is a finite field. Then any elliptic curve E defined over $\mathbb{F}_q$ will have a quadratic twist, i.e. an elliptic curve E^t which is $\mathbb{F}_{q^2}$-isomorphic but not $\mathbb{F}_q$-isomorphic to E. This is unique up to $\mathbb{F}_q$-isomorphism (hence why we talk about *the* quadratic twist).

In all the curve models (c.f. the above) that we consider there is an immediate connection between $\mathbb{F}_q$-rational points on the Kummer line $\mathcal{K}_E$ of E, and $\mathbb{F}_q$-rational points of E and E^t. As such, when thinking about Kummer lines it is natural not to distinguish these (i.e., to consider everything up to $\mathbb{F}_{q^2}$-isomorphism). As a result, although some maps may only be defined over $\mathbb{F}_{q^2}$, this will at most induce a twist. Since we are only concerned with the $\mathbb{F}_q$-rational points of the Kummer line, this is not an issue. In all that follows we *could* easily make everything defined over $\mathbb{F}_q$, but as we shall see in §4 this may limit us when finding instantiations.

3 Maps between Kummer lines

In this section we present the theoretical basis. We observe first that many Kummer lines have appeared in the literature; the work of Gaudry and Lubicz [GL09] present the so-called *canonical* Kummer line, while Karati and Sarkar use[4] the *squared* Kummer line [KS17b]. Moreover, there is the x-line of Montgomery curve (e.g. Curve25519 [Ber06b] by Bernstein) and the y-line of a (twisted) Edwards curve [CGF08, FH17]. It is not immediately clear how these are all connected, in particular the relation between the (canonical and squared) Kummer lines and Montgomery and (twisted) Edwards curves is not clear. Though a recent paper by Karati and Sarkar [KS17a] provides some connections, this is not completely satisfying. For instance, it relies on having rational points or using 2-isogeny, and does not give a unique connection.

In this section we settle this and, in essence, show that they are all the same up to isomorphism. These isomorphisms are natural and simple (including computationally) and lead to natural connections between all the above Kummer lines. The core is summarized in Theorem 5, and a more complete overview is shown in Appendix A.

3.1 Models with rational 2-torsion

It is immediate (through their description via theta functions) that the canonical and squared Kummer lines are projections of curves that have full rational 2-

[4] The formulas for this model had already appeared in the Explicit-Formulas Database [BL] referring to a discussion between Bernstein, Kohel and Lange and contributing the main idea to Gaudry [Gau06].

torsion. As such, we shall always assume to have this. We begin by showing that this allows a nice parametrization of Montgomery curves.

Proposition 1. *Let k be a field such that* $\mathrm{char}(k) \neq 2$ *and let* $(M_{A,B}, \mathcal{O}_M)$ *be a Montgomery curve such that* $M_{A,B}[2] \subset M_{A,B}(k)$*. Then there exist* $a, b \in \bar{k}^*$ *such that* $ab(a^4 - b^4) \neq 0$ *and* $a^2/b^2 \in k$ *such that*

$$A = -\frac{a^4 + b^4}{a^2 b^2}\,, \quad \Delta_M = 16B^6 \cdot \frac{(a^4 - b^4)^2}{a^4 b^4}\,.$$

Moreover, its points of order 2 are $(0 : 0 : 1)$, $(a^2 : 0 : b^2)$ *and* $(b^2 : 0 : a^2)$.

Proof. As $M_{A,B}[2] \subset M_{A,B}(k)$, the polynomial $x^2 + Ax + 1$ splits over k and thus $\sqrt{A^2 - 4} \in k$. Now fix any $b \in \bar{k}^*$ and take $a \in \bar{k}^*$ such that $a^2/b^2 = (\sqrt{A^2 - 4} - A)/2$. Note that $\sqrt{A^2 - 4} - A \neq 0, \pm 2$ because $\mathrm{char}(k) \neq 2$. Moreover $a^4 - b^4 = 0 \iff a^4/b^4 - 1 = 0 \iff a^2/b^2 = \pm 1$. Again, this is not possible since $\mathrm{char}(k) \neq 2$. The statements for A, Δ_M and the 2-torsion points are simple calculations, recalling that M has discriminant $\Delta_M = 16B^6(A^2 - 4)$. □

For simplicity we would like to have $B = 1$. Note that the curve $M_{A,B}$ is isomorphic to the curve $M_{A,1} : y^2 = x^3 + Ax^2 + x$ over $\bar{k}$, but not necessarily over k. Therefore, by making the assumption that $B = 1$ we are working *up to twist*. In what follows this shall not give rise to any issues, and as remarked earlier it does not impact the k-rational points of the Kummer line (even though it does change the k-rational point of the curve itself). So from this point on we consider

$$M/k : y^2 = x^3 - \frac{a^4 + b^4}{a^2 b^2} x^2 + x\,,$$

where $a, b \in \bar{k}^*$ such that $ab(a^4 - b^4) \neq 0$ and $a^2/b^2 \in k$.

Given this model we can define a *dual* curve. For this purpose, we define $\hat{a}, \hat{b} \in \bar{k}^*$ such that

$$2\hat{a}^2 = a^2 + b^2\,, \quad 2\hat{b}^2 = a^2 - b^2\,.$$

It is easily checked that $\hat{a}^2/\hat{b}^2 \in k^*$ and that $\hat{a}\hat{b}(\hat{a}^4 - \hat{b}^4) \neq 0$. Therefore

$$\widehat{M} : y^2 = x^3 - \frac{\hat{a}^4 + \hat{b}^4}{\hat{a}^2 \hat{b}^2} x^2 + x\,, \quad \Delta_{\widehat{M}} = 16 \cdot \frac{(\hat{a}^4 - \hat{b}^4)^2}{\hat{a}^4 \hat{b}^4}$$

is a Montgomery curve whose elements of order 2 are $(0 : 0 : 1)$, $(\hat{a}^2 : 0 : \hat{b}^2)$ and $(\hat{b}^2 : 0 : \hat{a}^2)$. We call $\widehat{M}$ the *dual* of M. More generally, for any curve model we call the action of swapping a resp. b by $\hat{a}$ resp. $\hat{b}$ (and vice versa) *dualizing* (c.f. Renes and Smith [RS17, §4.1]). The curves M and $\widehat{M}$ are 2-isogenous via a 2-isogeny $\phi : M \to \widehat{M}$, and the kernel of both ϕ and $\widehat{\phi}$ is generated by the point $(0 : 0 : 1)$ on the respective curves [Ren18, Remark 6]. This leads to a decomposition of the doubling map [2], which we use to construct the following sequence of maps.

Proposition 2. *Let $a, b \in \bar{k}^*$ with $ab(a^4 - b^4) \neq 0$ and $a^2/b^2 \in k^*$ and*

$$M/k : y^2 = x^3 - \frac{a^4 + b^4}{a^2 b^2} x^2 + x \,.$$

Then there exists a commutative diagram[5] *of isogenies (over $\bar{k}$)*

$$\begin{tikzcd}
 & (\widehat{\mathcal{E}}, \mathcal{O}_{\widehat{\mathcal{E}}}) \arrow[r, "\phi_5"] & (M, \mathcal{O}_M) \arrow[dr, "\phi_0"] \arrow[ddl, bend left, "\phi"] & \\
(\widehat{E}, \mathcal{O}_{\widehat{E}}) \arrow[ur, "\phi_4"] & & & (E, \mathcal{O}_E) \arrow[dl, "\phi_1"] \\
 & (\widehat{M}, \mathcal{O}_{\widehat{M}}) \arrow[ul, "\phi_3"] \arrow[uur, bend left, "\widehat{\phi}"] & (\mathcal{E}, \mathcal{O}_{\mathcal{E}}) \arrow[l, "\phi_2"] &
\end{tikzcd} \tag{3}$$

where

$$E/k : -x^2 + y^2 = 1 - \frac{(a^2 - b^2)^2}{(a^2 + b^2)^2} x^2 y^2 \,, \quad \mathcal{E}/k : x^2 + y^2 = \frac{a^2 - b^2}{a^2 + b^2} \left(1 + x^2 y^2\right)$$

and $\widehat{E}$ and $\widehat{\mathcal{E}}$ are their respective duals. The maps ϕ_2 and ϕ_5 are 2-isogenies with

$$\ker(\phi_2) = \langle (0 : 0 : -\hat{b} : \hat{a}) \rangle \,, \quad \ker(\phi_5) = \langle (0 : 0 : -b : a) \rangle \,,$$

while the maps ϕ_0, ϕ_1, ϕ_3 and ϕ_4 are isomorphisms.

Proof. We define

$$\phi_0 : (x, y) \mapsto \left(\frac{2\hat{a}^2 x}{aby}, \frac{x+1}{x-1} \right) \,, \quad \phi_0^{-1} : (x, y) \mapsto \left(\frac{y+1}{y-1}, \frac{2\hat{a}^2 (y+1)}{abx(y-1)} \right) \,.$$

Note that this is a priori only a birational map, but naturally becomes an isomorphism when (canonically) extended to the smooth $\mathbb{P}^3$ model, see e.g. [Sil09, Proposition II.2.1]. In particular, $\phi_0 : \mathcal{O}_M \mapsto \mathcal{O}_E \,, (0 : 0 : 1) \mapsto (0 : 0 : -1 : 1)\,.$ It is similar to the maps used by Bernstein et al. [BBJ+08, Theorem 3.2(i)] and by Castryck et al. [CGF08], but composed with the map by Hisil et al. [HWCD08, §3.1] to ensure a twisted Edwards curve $E_{\alpha,\delta}$ with $\alpha = -1$ that is well-defined everywhere. Moreover, we tweak it such that it acts as an involution (i.e. a Hadamard transformation) on the Kummer line. We define the isomorphism ϕ_1 as

$$\phi_1 : (x, y) \mapsto \Big(-\frac{i\hat{b}}{\hat{a}} x, \frac{\hat{b}}{\hat{a}} y \Big) \,, \quad \phi_1^{-1} : (x, y) \mapsto \Big(\frac{i\hat{a}}{\hat{b}} x, \frac{\hat{a}}{\hat{b}} y \Big) \,,$$

where $i \in \bar{k}$ is such that $i^2 = -1$. Then we set $\phi_2 = \phi \circ \phi_0^{-1} \circ \phi_1^{-1}$. It follows that

$$\ker(\phi_2) = \langle \phi_1 \phi_0 (0, 0) \rangle = \langle (0 : 0 : -\hat{b} : \hat{a}) \rangle \,.$$

A completely analogous construction can be made for ϕ_3, ϕ_4 and ϕ_5. □

[5] The diagram is drawn in the shape of a hexagon because its induced diagram on the Kummer lines after translations by points of order 2 is the genus-1 analogue of the hexagon in genus 2 by Renes–Smith [RS17, Figure 1].

Remark 3. Note that one can argue that the above construction can be done for any sequence of isomorphisms starting at M. Indeed this is the case, but the above choice is a natural one and gives rise to nice arithmetic on the Kummer lines. Moreover, it is a choice that allows to explain the connection between Montgomery curves and the genus-1 Kummer lines arising from theta functions (i.e. [GL09, §6.2] and [KS17b, §2.4]).

The maps behave very nicely on the Kummer lines.

Corollary 4. *There is an induced commutative diagram of Kummer lines*

$$\begin{tikzcd}
& K_{\widehat{\mathcal{E}}}^{\mathcal{O}_{\widehat{\mathcal{E}}}} \arrow[r, "\bar{\phi}_5"] & K_M^{\mathcal{O}_M} \arrow[dr, "\bar{\phi}_0"] & \\
K_{\widehat{E}}^{\mathcal{O}_{\widehat{E}}} \arrow[ur, "\bar{\phi}_4"] & & & K_E^{\mathcal{O}_E} \arrow[dl, "\bar{\phi}_1"] \\
& K_{\widehat{M}}^{\mathcal{O}_{\widehat{M}}} \arrow[ul, "\bar{\phi}_3"] & K_{\mathcal{E}}^{\mathcal{O}_{\mathcal{E}}} \arrow[l, "\bar{\phi}_2"] &
\end{tikzcd} \tag{4}$$

such that

$$\begin{aligned}
\bar{\phi}_0 &: (X : Z) \mapsto (X + Z : X - Z)\,, \\
\bar{\phi}_1 &: (X : Z) \mapsto (\hat{b}X : \hat{a}Z)\,, \\
\bar{\phi}_2 &: (X : Z) \mapsto (\hat{b}^2X^2 - \hat{a}^2Z^2 : \hat{a}^2X^2 - \hat{b}^2Z^2)\,,
\end{aligned}$$

while $\overline{\phi}_3 = \overline{\phi}_0$ *and* $\overline{\phi}_4$ *resp.* $\overline{\phi}_5$ *are obtained from* $\overline{\phi}_1$ *resp.* $\overline{\phi}_2$ *by dualizing.*

Proof. Apply the respective $\mathbf{x}$ and $\mathbf{y}$ projection maps to the curves in (3). □

This provides clear connections between the x- and y- lines of Montgomery and (twisted) Edwards curves with full rational 2-torsion. We now show that we can use these 2-torsion points to obtain simple isomorphisms to the canonical and squared Kummer lines.

3.2 Actions of points of order 2

First recall from §2 that we have points of order 2

$$\begin{aligned}
T &= (a^2 : 0 : b^2) \in (M, \mathcal{O}_M)\,, & \widehat{T} &= (\hat{a}^2 : 0 : \hat{b}^2) \in (\widehat{M}, \mathcal{O}_{\widehat{M}})\,, \\
\Omega_1 &= (\hat{a}^2 : \hat{b}^2 : 0 : 0) \in (E, \mathcal{O}_E)\,, & \widehat{\Omega}_1 &= (a^2 : b^2 : 0 : 0) \in (\widehat{E}, \mathcal{O}_{\widehat{E}})\,, \\
\Theta_1 &= (\hat{a} : \hat{b} : 0 : 0) \in (\mathcal{E}, \mathcal{O}_{\mathcal{E}})\,, & \widehat{\Theta}_1 &= (a : b : 0 : 0) \in (\widehat{\mathcal{E}}, \mathcal{O}_{\widehat{\mathcal{E}}})\,.
\end{aligned}$$

One can check that these are all respective images of one another under the ϕ_i. They correspond to translations[6] τ by the respective points which commute

[6] Translations are morphisms [Sil09, Theorem 3.6] and are therefore isogenies if and only if they send the base point of the domain curve to the base point of the codomain curve. For example, $\tau_T : (M, \mathcal{O}_M) \to (M, T)$ is an isogeny. As such, it is a group homomorphism.

with the projection maps to $\mathbb{P}^1$. As a result, we obtain induced involutions $\overline{\tau}$ on the Kummer lines. More concretely, we can show that

$$\begin{aligned}
\overline{\tau}_T &: (X:Z) \mapsto (a^2X - b^2Z : b^2X - a^2Z)\,, & \overline{\tau}_{\widehat{\Omega}_1} &: (X:Z) \mapsto (a^2Z : b^2X)\,, \\
\overline{\tau}_{\widehat{T}} &: (X:Z) \mapsto (\hat{a}^2X - \hat{b}^2Z : \hat{b}^2X - \hat{a}^2Z)\,, & \overline{\tau}_{\Theta_1} &: (X:Z) \mapsto (Z:X)\,, \\
\overline{\tau}_{\Omega_1} &: (X:Z) \mapsto (\hat{a}^2Z : \hat{b}^2X)\,, & \overline{\tau}_{\widehat{\Theta}_1} &: (X:Z) \mapsto (Z:X)\,.
\end{aligned}$$

Note that we could apply the maps τ to the diagram (3), but that requires keeping track of multiple coordinates and is somewhat tedious. Instead, for simplicity, we will focus on the Kummer lines. Applying the maps $\overline{\tau}$ to (4), we obtain the following result.

Theorem 5. *The diagram*[7]

$$\begin{tikzcd}
 & K_{\widehat{E}}^{\widehat{\Omega}_1} \arrow[rr, leftrightarrow, "\overline{\psi}_4"] \arrow[dl, leftrightarrow, "\overline{\tau}_{\widehat{\Omega}_1}"'] \arrow[dd, leftrightarrow, "\overline{\psi}_3"'] & & K_{\widehat{\mathcal{E}}}^{\widehat{\Theta}_1} \arrow[rr, "\overline{\psi}_5"] \arrow[dl, leftrightarrow, "\overline{\tau}_{\widehat{\Theta}_1}"'] & & K_M^T \arrow[dl, leftrightarrow, "\overline{\tau}_T"'] \arrow[dd, leftrightarrow, "\overline{\psi}_0"] \\
K_{\widehat{E}}^{\mathcal{O}_{\widehat{E}}} \arrow[rr, leftrightarrow, "\overline{\phi}_4"] \arrow[dd, leftrightarrow, "\overline{\phi}_3"'] & & K_{\widehat{\mathcal{E}}}^{\mathcal{O}_{\widehat{\mathcal{E}}}} \arrow[rr, "\overline{\phi}_5"] & & K_M^{\mathcal{O}_M} \arrow[dd, leftrightarrow, "\overline{\phi}_0"] & \\
 & K_{\widehat{M}}^{\widehat{T}} \arrow[dl, leftrightarrow, "\overline{\tau}_{\widehat{T}}"'] & & K_{\mathcal{E}}^{\Theta_1} \arrow[ll, "\overline{\psi}_2"] \arrow[rr, leftrightarrow, "\overline{\psi}_1"'] \arrow[dl, leftrightarrow, "\overline{\tau}_{\Theta_1}"] & & K_E^{\Omega_1} \arrow[dl, leftrightarrow, "\overline{\tau}_{\Omega_1}"] \\
K_{\widehat{M}}^{\mathcal{O}_{\widehat{M}}} & & K_{\mathcal{E}}^{\mathcal{O}_{\mathcal{E}}} \arrow[ll, "\overline{\phi}_2"] \arrow[rr, leftrightarrow, "\overline{\phi}_1"'] & & K_E^{\mathcal{O}_E} &
\end{tikzcd} \tag{5}$$

is commutative, where

$$\begin{aligned}
\overline{\psi}_0 &: (X:Z) \mapsto (X+Z : X-Z)\,, & \overline{\psi}_3 &: (X:Z) \mapsto (X+Z : X-Z)\,, \\
\overline{\psi}_1 &: (X:Z) \mapsto (\hat{b}X : \hat{a}Z)\,, & \overline{\psi}_4 &: (X:Z) \mapsto (bX : aZ)\,, \\
\overline{\psi}_2 &: (X:Z) \mapsto (X^2 : Z^2)\,, & \overline{\psi}_5 &: (X:Z) \mapsto (X^2 : Z^2)\,,
\end{aligned}$$

and every ↔ *is an isomorphism.*

Proof. This is the diagram from (3) translated by corresponding points of order 2 through the different τ, projected to their respective Kummer lines. We construct

$$\overline{\psi}_0 = \overline{\tau}_{\Omega_1} \circ \overline{\phi}_0 \circ \overline{\tau}_T$$

and proceed similarly for the other $\overline{\psi}_i$. □

Recall that (the duals of) $K_M^{\mathcal{O}_M}$, $K_E^{\mathcal{O}_E}$ resp. $K_{\mathcal{E}}^{\mathcal{O}_{\mathcal{E}}}$ are the Kummer lines of (the duals of) a Montgomery, twisted Edwards resp. Edwards curve. Hence it remains

[7] This is no longer a hexagon due to the authors' inability to draw it in a readable way.

to identify K_M^T, $K_E^{\Omega_1}$ and $K_{\mathcal{E}}^{\Theta_1}$ (and their duals). Since they are all simply $\mathbb{P}^1$ as an algebraic variety, we analyze their (pseudo-)addition formulae.

First note that Proposition 1 tells us that moving through the sequence $\overline{\phi}_0, \dots, \overline{\phi}_5$ corresponds to the [2] map (starting at any of the $\overline{\phi}_i$). Since the $\overline{\tau}$ are isomorphisms, the same is true for $\overline{\psi}_0, \dots, \overline{\psi}_5$. In other words, for example

$$\begin{aligned}[2] &= \overline{\psi}_5 \circ \cdots \circ \overline{\psi}_0 \text{ on } K_M^T\,,\\ [2] &= \overline{\psi}_4 \circ \cdots \circ \overline{\psi}_0 \circ \overline{\psi}_5 \text{ on } K_{\widehat{\mathcal{E}}}^{\widehat{\Theta}_1}\,.\end{aligned}$$

Comparing these with the algorithm from Gaudry–Lubicz [GL09, §6.2] (and the formulas also appear in [BL]) reveals that these are the doubling formulae for the squared and canonical Kummer lines. One readily[8] verifies that the same is true for the differential addition formulae. The third Kummer line $K_E^{\Omega_1}$ has not appeared to our knowledge, and has similar arithmetic to the squared Kummer line. We refer to it as the *intermediate* Kummer, c.f. [RS17, §4.3]. Interestingly, it appears as the y-line of a twisted Edwards curve where the coefficient of x^2 is -1, in which case the optimal formulas by Hisil et al. [HWCD08] are available. For completeness, we summarize the associated curve constants for the instances provided by Karati and Sarkar in Table 1, connecting the squared Kummer line to the Kummer lines of Montgomery and twisted Edwards models via isomorphisms (as opposed to birational maps or isogenies).

Table 1. Kummer lines over a finite field $\mathbb{F}_q$ and their associated (i) squared Kummer $(a^2 : b^2)$ (ii) Montgomery A (iii) twisted Edwards δ and (iv) Edwards c^2 constants.

q	$(a^2 : b^2)$	$(A : 1)$	$(\delta : 1)$	$(c^2 : 1)$
$2^{251} - 9$	$(81 : 20)$	$(-6961 : 1620)$	$(-3721 : 10201)$	$(61 : 101)$
$2^{251} - 9$	$(186 : 175)$	$(-65221 : 130200)$	$(-121 : 130221)$	$(11 : 361)$
$2^{255} - 19$	$(82 : 77)$	$(-12653 : 6314)$	$(-25 : 25281)$	$(5 : 159)$
$2^{266} - 3$	$(260 : 139)$	$(-86921 : 36140)$	$(-14641 : 159201)$	$(121 : 399)$

Remark 6. We reiterate that only the intermediate Kummer line is new, while all the others have already appeared in the literature and are well-known. However, there had been little work in providing explicit maps between them, and this is exactly what we provide.

[8] This can be done by using the known addition formulae on the elliptic curves whose identities are at infinity, and composing with the translation and projection maps. This is somewhat tedious, but is relatively straightforward by using a computer algebra package [BCP97, The18].

3.3 Hybrid Kummer lines

Since the arithmetic on these Kummer lines is generally well-studied, the (cryptographic) value of this study does not come from improved operation counts. Beside its theoretical contribution, we ease the problem of selecting which curves to use for best performance (e.g. for standardization). That is, the simplicity of the isomorphisms gives quasi-cost-free transformations that allow interchangeable usage of any of the models. This is similar to the usage of a birational map to move between the Montgomery and twisted Edwards model, but we extend it with the squared Kummer line. We summarize this in Figure 1. In particular, Karati and Sarkar [KS17b] show the benefits of the squared Kummer line on platforms where SIMD instructions are available.

$$\begin{tikzcd}
 & & E \arrow[d, "\mathbf{y}"] \\
\mathcal{K}_M^T \arrow[r, leftrightarrow, "(a^2X-b^2Z\,:\,b^2X-a^2Z)"] & \mathcal{K}_M^{\mathcal{O}_M} \arrow[r, leftrightarrow, "(X+Z\,:\,X-Z)"] & \mathcal{K}_E^{\mathcal{O}_E}
\end{tikzcd}$$

Fig. 1. The squared Kummer line, the x-line of a Montgomery curve and the y-line of a twisted Edwards curve E, connected by involutions.

Remark 7. Recall that all the above works under the assumption of having full rational 2-torsion. Although Montgomery and (twisted) Edwards curves always have a group order divisible by 4, it does not necessarily mean that they have full 2-torsion (i.e. they could have a point of order 4). Note that standardized curves such as Curve25519 and Curve448 do not have full 2-torsion, so this theory does not directly apply.

Moreover, results from the well-studied Montgomery model immediately carry over to the squared Kummer line. For example, we can straightforwardly fit a (squared) Kummer line into the qDSA signature scheme. For signature verification, given $\mathbf{x}(P), \mathbf{x}(Q), \mathbf{x}(R) \in \mathcal{K}_M^T$ we must be able to check whether $\mathbf{x}(R) = \mathbf{x}(P \pm Q)$. Although this can certainly be directly defined on $\mathcal{K}_M^T$, we note that it is equivalent to checking whether

$$\overline{\tau}_T(\mathbf{x}(R)) = \overline{\tau}_T(\mathbf{x}(P \pm Q))\,.$$

This is simply the function $\texttt{Check}(\overline{\tau}_T(\mathbf{x}(P)), \overline{\tau}_T(\mathbf{x}(Q)), \overline{\tau}_T(\mathbf{x}(R)))$, where `Check` is defined in [RS17, Algorithm 2].

To demonstrate feasibility of this approach, we extend[9] the publicly available Curve25519-based instantiation of qDSA from Renes–Smith [RS17] on the ARM Cortex M0 architecture. For this purpose we choose a squared Kummer line over $\mathbb{F}_{2^{255}-19}$, allowing field arithmetic to remain essentially unchanged.

[9] All code is available in the public domain at `http://www.cs.ru.nl/~jrenes/`.

A notable exception to this is an efficient assembly implementation of 16×256-bit field multiplication, which is used for the multiplications by the line constants. This replaces the highly optimized multiplication by 121666 from Düll et al. [DHH+15]. We select $(a^2, b^2) = (159, 5)$, so that the squared Kummer line $\mathcal{K}_M^T$ corresponds to the *dual*[10] of `KL25519(82,77)` presented and implemented by Karati–Sarkar [KS17b]. This implies the Montgomery constant of $K_M^{\mathcal{O}_M}$ to be $(A + 2 : 4) = (-5929 : 795)$.

Remark 8. The implementations that we present are constant-time, and all standard countermeasures (e.g. projective blinding, scalar blinding [Cor99, §5]) against more advanced side-channel and fault attacks can be applied if required. In particular, as mentioned by the authors, the recent fault attack by Takahashi, Tibouchi and Abe [TTA18] can (cheaply) be thwarted by requiring nonces to be multiples of the cofactor (i.e. by "clamping"). However, such countermeasures are only necessary when an implementation is used in a context where fault attacks are considered part of the attacker model. We emphasize that our implementation is intended as a reference and *not* for production use.

4 Isomorphism classes over finite fields

For cryptographic purposes, we are mostly concerned with the case that $k = \mathbb{F}_q$, for some prime (power) q. As using extension fields is generally expensive, we would like to set things up such that all computation is performed in $\mathbb{F}_q$. Whether or not we can do this in a way such that constants remain small, depends on the number of Kummer lines that exist. Following earlier studies on the number of isomorphism classes for certain curve models [BBJ+08, FS10, FMW12], we provide counts for the canonical, squared and intermediate Kummer lines.

4.1 Identifying Kummer lines

For this purpose it is interesting to ask when two Kummer lines should be considered to be the same. Given two Kummer lines $K_1 = E_1/\{\pm 1\}$ and $K_2 = E_2/\{\pm 1\}$ of elliptic curves E_1, E_2 defined over $\mathbb{F}_q$, it could be natural to identify K_1 with K_2 whenever E_1 is $\mathbb{F}_q$-isomorphic to E_2. However, as noted in §2, the arithmetic on the $\mathbb{F}_q$-rational points of the Kummer lines will be identical whenever E_1 is $\mathbb{F}_{q^2}$-isomorphic to E_2 (i.e. E_2 is the quadratic twist of E_1). Since the curves are defined over $\mathbb{F}_q$, this will happen if and only if $j(E_1) = j(E_2)$. As such, we equate the number of Kummer lines with the number of elliptic curves defined over $\mathbb{F}_q$ up to $\bar{\mathbb{F}}_q$-isomorphism.

Recall that we parametrize Kummer lines by $a, b \in \bar{\mathbb{F}}_q$ such that $ab(a^4 - b^4) \neq 0$ and $a^2/b^2 \in \mathbb{F}_q$. Since $b \neq 0$, a Kummer line is defined by the fraction a/b or, equivalently, by the point $(a : b) \in \mathbb{P}^1$. Again, since $b \neq 0$ we can therefore

[10] The constants $(a^2, b^2) = (88, 77)$ lead to $(A + 2 : 4) = (-25 : 25256)$ which has slightly larger constants on $K_M^{\mathcal{O}_M}$ than its dual. However, results should be very similar.

simply assume $b = 1$. As such, we can consider $a \in \bar{\mathbb{F}}_q$ such that $a^2 \in \mathbb{F}_q$ and $a^5 - a \neq 0$.

4.2 Canonical Kummer lines

We begin by considering the canonical Kummer line from Gaudry and Lubicz [GL09] defined by some a as above. Recall that it corresponds to the y-line of the curve

$$\widehat{\mathcal{E}}/\mathbb{F}_q : x^2 + y^2 = \frac{1}{a^2}\left(1 + x^2y^2\right) .$$

with identity $\widehat{\Omega}_1 = (a : 1 : 0 : 0)$, whose image in $\mathbb{P}^1$ is $(a : 1)$. Therefore, we certainly require that $a \in \mathbb{F}_q$. It is easily seen that $\hat{a}^2, \hat{b}^2 \in \mathbb{F}_q$ and that this is enough to perform all arithmetic with $\mathbb{F}_q$ operations.

Now note that $(\widehat{\mathcal{E}}, \widehat{\Omega}_1)$ is $\mathbb{F}_q$-isomorphic to $(\widehat{\mathcal{E}}, \mathcal{O}_{\widehat{\mathcal{E}}})$ via $\tau_{\widehat{\Omega}_1}$, which is an Edwards curve if and only if $a \in \mathbb{F}_q$ and $1/a^5 \neq 1/a$. The first is true by assumption, while the latter follows from $a^5 \neq a$. Therefore we simply count the number of Edwards curves defined over $\mathbb{F}_q$ up to $\bar{\mathbb{F}}_q$-isomorphism. A result by Farashahi and Shparlinski [FS10, Theorem 5] shows that there are exactly

$$\begin{cases} \left\lfloor \dfrac{q+23}{24} \right\rfloor & \text{if } q \equiv 1, 9, 13, 17 \pmod{24}\,, \\ \left\lfloor \dfrac{q-5}{24} \right\rfloor & \text{if } q \equiv 5 \pmod{24}\,, \\ \left\lfloor \dfrac{q+1}{8} \right\rfloor & \text{if } q \equiv 3 \pmod{4}\,. \end{cases}$$

Thus, in general there will be no problem to find Kummer lines with the desired security properties. However, it may not be easy to find them such that its constants are small. For that reason, we look towards the squared and intermediate Kummer lines.

4.3 Squared and intermediate Kummer lines

If we use canonical Kummer lines, we restrict ourselves to $a \in \mathbb{F}_q$ for all of the arithmetic to be in $\mathbb{F}_q$. This (seemingly) limits the number of Kummer lines that we can use. This is no longer the case on squared and intermediate Kummer lines; it suffices to only have $a^2 \in \mathbb{F}_q$. Note that this implies that $a \in \mathbb{F}_{q^2}$.

Since the j-invariants of M, E and $\mathcal{E}$ and their duals are all equal, we can count the number of curves up to isomorphism of the form

$$\widehat{\mathcal{E}} : x^2 + y^2 = \frac{1}{a^2}\left(1 + x^2y^2\right)$$

such that $a^5 \neq a$ (but note that $\widehat{\mathcal{E}}$ is not necessarily an Edwards curve over $\mathbb{F}_q$). There are exactly $q - 3$ such curves, so it remains to determine how many are in the same $\bar{\mathbb{F}}_q$-isomorphism class. This question has already been considered by Edwards [Edw07, Proposition 6.1], whose statement implies that two Edwards curves determined by $a^2, \overline{a}^2 \in \mathbb{F}_q$ have the same j-invariant whenever $\overline{a}^2$ is one of the following:

$$\pm\, a^2 \,, \pm\frac{1}{a^2} \,, \pm\left(\frac{a-1}{a+1}\right)^2 \,, \pm\left(\frac{a+1}{a-1}\right)^2 \,, \pm\left(\frac{a-i}{a+i}\right)^2 \,, \pm\left(\frac{a+i}{a-i}\right)^2 \,. \tag{6}$$

If $q \equiv 1 \pmod 4$, then $i^q = i$ and a straightforward computation show that

$$\pm\left(\frac{a-1}{a+1}\right)^2 \,, \pm\left(\frac{a+1}{a-1}\right)^2 \,, \pm\left(\frac{a-i}{a+i}\right)^2 \,, \pm\left(\frac{a+i}{a-i}\right)^2 \in \mathbb{F}_q \iff a \in \mathbb{F}_q \,.$$

If $q \equiv 3 \pmod 4$, then $i^q = -i$ and a similar computation shows that

$$\begin{aligned} \pm\left(\frac{a-1}{a+1}\right)^2 \,, \pm\left(\frac{a+1}{a-1}\right)^2 &\in \mathbb{F}_q \iff a \in \mathbb{F}_q \,, \\ \pm\left(\frac{a-i}{a+i}\right)^2 \,, \pm\left(\frac{a+i}{a-i}\right)^2 &\in \mathbb{F}_q \iff i \cdot a \in \mathbb{F}_q \,. \end{aligned}$$

Given that either $a \in \mathbb{F}_q$ or $i \cdot a \in \mathbb{F}_q$, while half the elements of $\mathbb{F}_q$ are squares, we closely approximate[11] that the number of isomorphism classes is

$$\approx \begin{cases} \left\lfloor \left(\frac{1}{4} + \frac{1}{12}\right) \frac{q}{2} \right\rfloor = \left\lfloor \frac{q}{6} \right\rfloor & \text{if } q \equiv 1 \pmod 4 \,, \\ \left\lfloor \left(\frac{1}{8} + \frac{1}{8}\right) \frac{q}{2} \right\rfloor = \left\lfloor \frac{q}{8} \right\rfloor & \text{if } q \equiv 3 \pmod 4 \,. \end{cases}$$

A more careful analysis c.f. [FS10] could be done, but such a close estimate suffices for our purposes. Interestingly, for $q \equiv 3 \pmod 4$ the number of canonical and squared Kummer lines is about the same. Thus although $a^2 \in \mathbb{F}_q$ is a weaker restriction than $a \in \mathbb{F}_q$, it does not actually lead to more Kummer lines (up to isomorphism). This is explained by the fact that -1 is a non-square since $q \equiv 3 \pmod 4$, hence exactly one of a^2 or $-a^2$ must be a square in $\mathbb{F}_q$, while their corresponding Edwards curves are isomorphic. For $q \equiv 1 \pmod 4$ there is a clear difference in the number of Kummer lines, so in that case there is a significant advantage in finding small parameters for a squared or intermediate Kummer line over a canonical Kummer line.

Acknowledgements. We thank the anonymous reviewers of Asiacrypt 2018 for their valuable comments.

[11] This statement is exact up to the observation that some of the elements in (6) can be the same, which happens only exceptionally.

References

[BBJ+08] D. J. Bernstein, P. Birkner, M. Joye, T. Lange, and C. Peters. Twisted Edwards Curves. In S. Vaudenay, editor, *Progress in Cryptology - AFRICACRYPT 2008, First International Conference on Cryptology in Africa, Casablanca, Morocco, June 11-14, 2008. Proceedings*, volume 5023 of *Lecture Notes in Computer Science*, pages 389–405. Springer, 2008. 2, 4, 8, 13

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993). 11

[Ber06a] D. J. Bernstein. Elliptic vs. Hyperelliptic, part I. Talk at ECC (slides at `http://cr.yp.to/talks/2006.09.20/slides.pdf`), September 2006. 2

[Ber06b] Daniel J. Bernstein. Curve25519: New Diffie-Hellman Speed Records. In *Public Key Cryptography - PKC 2006, 9th International Conference on Theory and Practice of Public-Key Cryptography, New York, NY, USA, April 24-26, 2006, Proceedings*, pages 207–228, 2006. 2, 3, 6

[BL] Daniel J. Bernstein and Tanja Lange. Explicit-Formulas Database. `http://hyperelliptic.org/EFD/g1p/auto-edwards-yzsquared.html` (accessed 2018-05-08). 2, 6, 11

[BL07] Daniel J. Bernstein and Tanja Lange. Faster Addition and Doubling on Elliptic Curves. In *Advances in Cryptology - ASIACRYPT 2007, 13th International Conference on the Theory and Application of Cryptology and Information Security, Kuching, Malaysia, December 2-6, 2007, Proceedings*, pages 29–50, 2007. 5

[CC86] David V. Chudnovsky and Gregory V. Chudnovsky. Sequences of numbers generated by addition in formal groups and new primality and factorization tests. *Advances in Applied Mathematics*, 7(4):385–434, 1986. 2

[CGF08] W. Castryck, S. Galbraith, and R. R. Farashahi. Efficient arithmetic on elliptic curves using a mixed Edwards-Montgomery representation. Cryptology ePrint Archive, Report 2008/218, 2008. `http://eprint.iacr.org/2008/218`. 2, 6, 8

[Cho15] Tung Chou. Sandy2x. Message on the Curves mailing list at `https://moderncrypto.org/mail-archive/curves/2015/000637.html`, September 2015. 3

[CL15] Craig Costello and Patrick Longa. Fourℚ: Four-Dimensional Decompositions on a ℚ-curve over the Mersenne Prime. In *Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part I*, pages 214–235, 2015. 2

[Cor99] J.S. Coron. Resistance Against Differential Power Analysis for Elliptic Curve Cryptosystems. In Çetin K. Koç and C. Paar, editors, *Cryptographic Hardware and Embedded Systems – CHES'99*, volume 1717, pages 292–302, 1999. 13

[DH76] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Trans. Information Theory*, 22(6):644–654, 1976. 1

[DHH+15] Michael Düll, Björn Haase, Gesine Hinterwälder, Michael Hutter, Christof Paar, Ana Helena Sánchez, and Peter Schwabe. High-speed Curve25519 on 8-bit, 16-bit and 32-bit microcontrollers. *Design, Codes and Cryptography*, 77(2), 2015. http://cryptojedi.org/papers/#mu25519. 13

[Edw07] Harold M. Edwards. A normal form for elliptic curves. In *Bulletin of the American Mathematical Society*, pages 393–422, 2007. 5, 15

[FH17] Reza Rezaeian Farashahi and Seyed Gholamhossein Hosseini. Differential Addition on Twisted Edwards Curves. In *Information Security and Privacy - 22nd Australasian Conference, ACISP 2017, Auckland, New Zealand, July 3-5, 2017, Proceedings, Part II*, pages 366–378, 2017. 6

[FL15] Armando Faz-Hernández and Julio López. Fast Implementation of Curve25519 Using AVX2. In *Progress in Cryptology - LATINCRYPT 2015 - 4th International Conference on Cryptology and Information Security in Latin America, Guadalajara, Mexico, August 23-26, 2015, Proceedings*, pages 329–345, 2015. 2

[FMW12] Reza Rezaeian Farashahi, Dustin Moody, and Hongfeng Wu. Isomorphism classes of Edwards curves over finite fields. *Finite Fields and Their Applications*, 18(3):597–612, 2012. 13

[FS10] Reza Rezaeian Farashahi and Igor E. Shparlinski. On the number of distinct elliptic curves in some families. *Des. Codes Cryptography*, 54(1):83–99, 2010. 13, 14, 15

[Gal12] Steven D. Galbraith. *Mathematics of Public Key Cryptography.* Cambridge University Press, 2012. 4

[Gau06] Pierrick Gaudry. Variants of the montgomery form based on theta functions, 2006. http://www.fields.utoronto.ca/audio/06-07/number_theory/gaudry/. 6

[GL09] Pierrick Gaudry and David Lubicz. The arithmetic of characteristic 2 Kummer surfaces and of elliptic Kummer lines. *Finite Fields and Their Applications*, 15(2):246 – 260, 2009. 2, 6, 9, 11, 14

[His10] H. Hisil. *Elliptic Curves, Group Law, and Efficient Computation.* PhD thesis, Queensland University of Technology, 2010. 4

[HWCD08] Huseyin Hisil, Kenneth Koon-Ho Wong, Gary Carter, and Ed Dawson. Twisted Edwards curves revisited. In Josef Pieprzyk, editor, *Advances in Cryptology - ASIACRYPT 2008*, pages 326–343, Berlin, Heidelberg, 2008. Springer Berlin Heidelberg. 2, 8, 11

[Kob87] N. Koblitz. Elliptic Curve Cryptosystems. *Mathematics of Computation*, 48:203–209, 1987. 1

[KS17a] Sabyasachi Karati and Palash Sarkar. Connecting Legendre with Kummer and Edwards. Cryptology ePrint Archive, Report 2017/1205, 2017. https://eprint.iacr.org/2017/1205. 2, 3, 6

[KS17b] Sabyasachi Karati and Palash Sarkar. Kummer for Genus One over Prime Order Fields. In *Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part II*, pages 3–32, 2017. 2, 6, 9, 12, 13

[Mil86] Victor Miller. Use of Elliptic Curves in Cryptography. In *Advances in Cryptology - CRYPTO 85 Proceedings*, volume 218 of *Lecture Notes in Computer Science*, pages 417–426. Springer Berlin / Heidelberg, Berlin, Germany, 1986. 1

[Mon87] P. L. Montgomery. Speeding the Pollard and elliptic curve methods of factorization. *Mathematics of computation*, 48(177):243–264, 1987. 3, 4

[Ren18] Joost Renes. Computing Isogenies Between Montgomery Curves Using the Action of $(0, 0)$. In *PQCrypto*, volume 10786 of *Lecture Notes in Computer Science*, pages 229–247. Springer, 2018. https://ia.cr/2017/1198. 7

[RS17] Joost Renes and Benjamin Smith. qDSA: Small and Secure Digital Signatures with Curve-Based Diffie–Hellman Key Pairs. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology – ASIACRYPT 2017: 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part II*, pages 273–302. Springer International Publishing, 2017. 1, 2, 7, 8, 11, 12

[Sil09] J. H. Silverman. *The Arithmetic of Elliptic Curves, 2nd Edition*. Graduate Texts in Mathematics. Springer, 2009. 3, 8, 9

[The18] The Sage Developers. *SageMath, the Sage Mathematics Software System (version 8.1)*, 2018. https://sagemath.org. 11

[TTA18] Akira Takahashi, Mehdi Tibouchi, and Masayuki Abe. New Bleichenbacher Records: Practical Fault Attacks on qDSA Signatures. Cryptology ePrint Archive, Report 2018/396, 2018. https://eprint.iacr.org/2018/396. 13

A GENUS 1 KUMMER ISOGENIES

In the maps below, $\overline{\tau}_T$, $\overline{\tau}_{\Omega_1}$, $\overline{\tau}_{\Theta_1}$, $\overline{\tau}_{\widehat{T}}$, $\overline{\tau}_{\widehat{\Omega}_1}$, $\overline{\tau}_{\widehat{\Theta}_1}$, $\bar{\phi}_0$, $\bar{\phi}_3$, $\overline{\psi}_0$, $\overline{\psi}_3$ are involutions; $\bar{\phi}_1$, $\bar{\phi}_4$, $\overline{\psi}_1$, $\overline{\psi}_4$ are isomorphisms; $\bar{\phi}_2$, $\bar{\phi}_5$, $\overline{\psi}_2$, $\overline{\psi}_5$ are 2-isogenies.

$$\begin{tikzcd}
 & K_{\widehat{E}}^{\widehat{\Omega}_1} \arrow[rr, leftrightarrow, "\overline{\psi}_4"] \arrow[dd, leftrightarrow, "\overline{\psi}_3"'] & & K_{\widehat{\mathcal{E}}}^{\widehat{\Theta}_1} \arrow[rr, "\overline{\psi}_5"] & & K_M^T \arrow[dd, leftrightarrow, "\overline{\psi}_0"] \\
K_{\widehat{E}}^{\mathcal{O}_{\widehat{E}}} \arrow[ur, leftrightarrow, "\overline{\tau}_{\widehat{\Omega}_1}"] \arrow[rr, leftrightarrow, crossing over, "\bar{\phi}_4"] \arrow[dd, leftrightarrow, "\bar{\phi}_3"'] & & K_{\widehat{\mathcal{E}}}^{\mathcal{O}_{\widehat{\mathcal{E}}}} \arrow[ur, leftrightarrow, "\overline{\tau}_{\widehat{\Theta}_1}"] \arrow[rr, "\bar{\phi}_5"] & & K_M^{\mathcal{O}_M} \arrow[ur, leftrightarrow, "\overline{\tau}_T"] & \\
 & K_{\widehat{M}}^{\widehat{T}} & & K_{\mathcal{E}}^{\Theta_1} \arrow[ll, "\overline{\psi}_2"] & & K_E^{\Omega_1} \arrow[ll, leftrightarrow, "\overline{\psi}_1"] \\
K_{\widehat{M}}^{\mathcal{O}_{\widehat{M}}} \arrow[ur, leftrightarrow, "\overline{\tau}_{\widehat{T}}"'] & & K_{\mathcal{E}}^{\mathcal{O}_{\mathcal{E}}} \arrow[ll, "\bar{\phi}_2"] \arrow[ur, leftrightarrow, "\overline{\tau}_{\Theta_1}"'] \arrow[rr, leftrightarrow, "\bar{\phi}_1"'] & & K_E^{\mathcal{O}_E} \arrow[ur, leftrightarrow, "\overline{\tau}_{\Omega_1}"'] \arrow[uu, leftrightarrow, crossing over, "\bar{\phi}_0"'] &
\end{tikzcd}$$

$$\begin{aligned}
&(a^2\colon b^2) = (\hat{a}^2 + \hat{b}^2\colon \hat{a}^2 - \hat{b}^2) \in \mathbb{P}^1\\
&M\colon y^2 = x^3 - \left((a^4+b^4)/(a^2b^2)\right)x^2 + x\\
&E\colon -x^2 + y^2 = 1 - (\hat{b}^4/\hat{a}^4)x^2y^2\\
&\mathcal{E}\colon x^2 + y^2 = (\hat{b}^2/\hat{a}^2)\left(1 + x^2y^2\right)
\end{aligned}$$

$$\begin{aligned}
&(\hat{a}^2\colon \hat{b}^2) = (a^2 + b^2\colon a^2 - b^2) \in \mathbb{P}^1\\
&\widehat{M}\colon y^2 = x^3 - \left((\hat{a}^4+\hat{b}^4)/(\hat{a}^2\hat{b}^2)\right)x^2 + x\\
&\widehat{E}\colon -x^2 + y^2 = 1 - (b^4/a^4)x^2y^2\\
&\widehat{\mathcal{E}}\colon x^2 + y^2 = (b^2/a^2)\left(1 + x^2y^2\right)
\end{aligned}$$

$$\begin{aligned}
&\mathcal{O}_M = (0\colon 1\colon 0),\ T = (a^2\colon 0\colon b^2)\\
&\mathcal{O}_E = (0\colon 0\colon 1\colon 1),\ \Omega_1 = (\hat{a}^2\colon \hat{b}^2\colon 0\colon 0)\\
&\mathcal{O}_{\mathcal{E}} = (0\colon 0\colon \hat{b}\colon \hat{a}),\ \Theta_1 = (\hat{a}\colon \hat{b}\colon 0\colon 0)\\
&\mathcal{O}_{\widehat{M}} = (0\colon 1\colon 0),\ \widehat{T} = (\hat{a}^2\colon 0\colon \hat{b}^2)\\
&\mathcal{O}_{\widehat{E}} = (0\colon 0\colon 1\colon 1),\ \widehat{\Omega}_1 = (a^2\colon b^2\colon 0\colon 0)\\
&\mathcal{O}_{\widehat{\mathcal{E}}} = (0\colon 0\colon b\colon a),\ \widehat{\Theta}_1 = (a\colon b\colon 0\colon 0)
\end{aligned}$$

$$\begin{aligned}
\overline{\tau}_T &: (X\colon Z) \mapsto (a^2X - b^2Z\colon b^2X - a^2Z)\\
\overline{\tau}_{\Omega_1} &: (X\colon Z) \mapsto (\hat{a}^2Z\colon \hat{b}^2X)\\
\overline{\tau}_{\Theta_1} &: (X\colon Z) \mapsto (Z\colon X)\\
\overline{\tau}_{\widehat{T}} &: (X\colon Z) \mapsto (\hat{a}^2X - \hat{b}^2Z\colon \hat{b}^2X - \hat{a}^2Z)\\
\overline{\tau}_{\widehat{\Omega}_1} &: (X\colon Z) \mapsto (a^2Z\colon b^2X)\\
\overline{\tau}_{\widehat{\Theta}_1} &: (X\colon Z) \mapsto (Z\colon X)
\end{aligned}$$

$$\begin{aligned}
\mathbf{id}(K_M^{\mathcal{O}_M}) &= \mathbf{x}(\mathcal{O}_M) = (1\colon 0)\\
\mathbf{id}(K_E^{\mathcal{O}_E}) &= \mathbf{y}(\mathcal{O}_E) = (1\colon 1)\\
\mathbf{id}(K_{\mathcal{E}}^{\mathcal{O}_{\mathcal{E}}}) &= \mathbf{y}(\mathcal{O}_{\mathcal{E}}) = (\hat{b}\colon \hat{a})\\
\mathbf{id}(K_{\widehat{M}}^{\mathcal{O}_{\widehat{M}}}) &= \mathbf{x}(\mathcal{O}_{\widehat{M}}) = (1\colon 0)\\
\mathbf{id}(K_{\widehat{E}}^{\mathcal{O}_{\widehat{E}}}) &= \mathbf{y}(\mathcal{O}_{\widehat{E}}) = (1\colon 1)\\
\mathbf{id}(K_{\widehat{\mathcal{E}}}^{\mathcal{O}_{\widehat{\mathcal{E}}}}) &= \mathbf{y}(\mathcal{O}_{\widehat{\mathcal{E}}}) = (b\colon a)
\end{aligned}$$

$$\begin{aligned}
\bar{\phi}_0 &: (X\colon Z) \mapsto (X + Z\colon X - Z)\\
\bar{\phi}_1 &: (X\colon Z) \mapsto (\hat{b}X\colon \hat{a}Z)\\
\bar{\phi}_2 &: (X\colon Z) \mapsto (\hat{b}^2X^2 - \hat{a}^2Z^2\colon \hat{a}^2X^2 - \hat{b}^2Z^2)\\
\bar{\phi}_3 &: (X\colon Z) \mapsto (X + Z\colon X - Z)\\
\bar{\phi}_4 &: (X\colon Z) \mapsto (bX\colon aZ)\\
\bar{\phi}_5 &: (X\colon Z) \mapsto (b^2X^2 - a^2Z^2\colon a^2X^2 - b^2Z^2)
\end{aligned}$$

$$\begin{aligned}
\mathbf{id}(K_M^T) &= \mathbf{x}(T) = (a^2\colon b^2)\\
\mathbf{id}(K_E^{\Omega_1}) &= \mathbf{y}(\Omega_1) = (\hat{a}^2\colon \hat{b}^2)\\
\mathbf{id}(K_{\mathcal{E}}^{\Theta_1}) &= \mathbf{y}(\Theta_1) = (\hat{a}\colon \hat{b})\\
\mathbf{id}(K_{\widehat{M}}^{\widehat{T}}) &= \mathbf{x}(\widehat{T}) = (\hat{a}^2\colon \hat{b}^2)\\
\mathbf{id}(K_{\widehat{E}}^{\widehat{\Omega}_1}) &= \mathbf{y}(\widehat{\Omega}_1) = (a^2\colon b^2)\\
\mathbf{id}(K_{\widehat{\mathcal{E}}}^{\widehat{\Theta}_1}) &= \mathbf{y}(\widehat{\Theta}_1) = (a\colon b)
\end{aligned}$$

$$\begin{aligned}
\overline{\psi}_0 &: (X\colon Z) \mapsto (X + Z\colon X - Z)\\
\overline{\psi}_1 &: (X\colon Z) \mapsto (\hat{b}X\colon \hat{a}Z)\\
\overline{\psi}_2 &: (X\colon Z) \mapsto (X^2\colon Z^2)\\
\overline{\psi}_3 &: (X\colon Z) \mapsto (X + Z\colon X - Z)\\
\overline{\psi}_4 &: (X\colon Z) \mapsto (bX\colon aZ)\\
\overline{\psi}_5 &: (X\colon Z) \mapsto (X^2\colon Z^2)
\end{aligned}$$

In addition, we have, $\bar{\phi}_1^{-1}\colon (X\colon Z) \mapsto (\hat{a}X\colon \hat{b}Z)$, $\bar{\phi}_4^{-1}\colon (X\colon Z) \mapsto (aX\colon bZ)$, $\overline{\psi}_1^{-1}\colon (X\colon Z) \mapsto (\hat{a}X\colon \hat{b}Z)$, $\overline{\psi}_4^{-1}\colon (X\colon Z) \mapsto (aX\colon bZ)$.