CSIDH on the surface

Wouter Castryck and Thomas Decru

Cosic and Imec, Department of Electrical Engineering, KU Leuven
wouter.castryck@esat.kuleuven.be, thomas.decru@esat.kuleuven.be

Abstract. For primes $p \equiv 3 \bmod 4$, we show that setting up CSIDH on the surface, i.e., using supersingular elliptic curves with endomorphism ring $\mathbf{Z}[(1+\sqrt{-p})/2]$, amounts to just a few sign switches in the underlying arithmetic. If $p \equiv 7 \bmod 8$ then the availability of very efficient horizontal 2-isogenies allows for a noticeable speed-up, e.g., our resulting CSURF-512 protocol runs about 5.68% faster than CSIDH-512. This improvement is completely orthogonal to all previous speed-ups, constant-time measures and construction of cryptographic primitives that have appeared in the literature so far. At the same time, moving to the surface gets rid of the redundant factor $\mathbf{Z}_3$ of the acting ideal-class group, which is present in the case of CSIDH and offers no extra security.

Keywords: isogeny-based cryptography, hard homogeneous spaces, CSIDH, Montgomery curves

1 Introduction

A hard homogeneous space [10] is an efficiently computable free and transitive action $\star : G \times S \to S$ of a finite commutative group G on a set S, for which the parallelization problem is hard: given $s_0, s_1, s_2 \in S$, it should be infeasible to find $g_1 g_2 \star s_0$, where $g_1, g_2 \in G$ are such that $s_1 = g_1 \star s_0$ and $s_2 = g_2 \star s_0$. This generalizes the notion of a cyclic group C in which the Diffie–Hellman problem is hard, as can be seen by considering the set S of generators of C, acted upon by $G = (\mathbf{Z}_{|C|})^\times$ through exponentiation. The main appeal of hard homogeneous spaces lies in their potential for post-quantum cryptography: while exponentiation-based Diffie–Hellman succumbs to Shor's polynomial-time quantum algorithm [21], in this more general setting the best attack available is Kuperberg's subexponential-time algorithm for finding hidden shifts [15]. This line of research has led to number of efficient post-quantum cryptographic primitives, such as non-interactive key exchange [7] and digital signatures [4], which stand out in terms of bandwidth requirements, and verifiable delay functions [11].

Unfortunately, we only know of one source of candidate hard homogeneous spaces that are not based on exponentiation. They descend from CM theory, which yields a family of isogeny-wise actions by ideal-class groups on sets of elliptic curves over finite fields, whose use in cryptography was proposed independently by Couveignes [10] and Rostovtsev–Stolbunov [19,22,23]. The current paper revisits CSIDH [7], which is an incarnation of this idea, using supersingular elliptic curves rather than ordinary elliptic curves (as originally suggested), thereby speeding up the resulting protocols by several orders of magnitude.

Concretely, we focus on the following design choice of CSIDH: as put forward in [7], it works over a large finite prime field $\mathbf{F}_p$ with $p \equiv 3 \bmod 8$, and it acts by $G = \mathcal{C}\ell(\mathbf{Z}[\sqrt{-p}])$ on the set S of $\mathbf{F}_p$-isomorphism classes of elliptic curves with endomorphism ring $\mathbf{Z}[\sqrt{-p}]$ — such curves are said to live on the *floor*. The motivation for this choice comes from [7, Prop. 8], which identifies S with

$$S_p^+ = \{\, a \in \mathbf{F}_p \,|\, y^2 = x^3 + ax^2 + x \text{ is supersingular} \,\},$$

i.e., every curve on the floor has a unique representant in Montgomery form and, conversely, every supersingular Montgomery curve over $\mathbf{F}_p$ has endomorphism ring $\mathbf{Z}[\sqrt{-p}]$. This convenient fact allows for compact and easily verifiable public keys. Furthermore $0 \in S_p^+$ makes for a natural choice of s_0.

One of our main observations is that for $p \equiv 7 \bmod 8$, a very similar statement applies to the *surface*, consisting of $\mathbf{F}_p$-isomorphism classes of elliptic curves with endomorphism ring $\mathbf{Z}[(1 + \sqrt{-p})/2]$. Concretely, this set can be identified with

$$S_p^- = \{\, A \in \mathbf{F}_p \,|\, y^2 = x^3 + Ax^2 - x \text{ is supersingular} \,\}, \tag{1}$$

which again contains 0 as a convenient instance of s_0. The tweaked Montgomery form $y^2 = x^3 + Ax^2 - x$ does not seem to have been studied before. From the viewpoint of efficient arithmetic, it is equivalent with the standard Montgomery form: we will show that the required adaptations to the Montgomery ladder and to Vélu's isogeny formulae (in the version of Renes [18]) just amount to a few sign flips, with the exception of 2-isogenies, which require a separate treatment.

Therefore, the protocols built from the action of $\mathcal{C}\ell(\mathbf{Z}[(1 + \sqrt{-p})/2])$ on S_p^- are near-copies of those built from CSIDH, with two noteworthy benefits:[1]

(a) If $p \equiv 7 \bmod 8$ then the prime 2 splits in $\mathbf{Q}(\sqrt{-p})$. This allows for the use of very fast horizontal 2-isogenies, leading to a noticeable speed-up (e.g., our CSURF-512 protocol below performs about 5.68% faster than CSIDH-512).
(b) By working on the surface, we naturally get rid of the factor $\mathbf{Z}_3$ that is present in $\mathcal{C}\ell(\mathbf{Z}[\sqrt{-p}])$ when $p \equiv 3 \bmod 8$. Because of the interplay between floor and surface, this factor does not give extra security (see Remark 2). Furthermore, it provides a possible hindrance for isogeny-based threshold schemes: when using more than two parties one must map the problem into $\mathcal{C}\ell(\mathbf{Z}[\sqrt{-p}])^3$, which comes at a small cost if the group structure is unknown [12].

We stress that these improvements are totally orthogonal to all previous speed-ups, constant-time measures (see e.g. [9,14]) and cryptographic applications (see e.g. [7,4,11]) that have appeared in the literature so far.

Apart from these benefits, given the limited pool of hard homogeneous spaces available, having the complete supersingular picture at our disposal adds freedom to the parameter selection and leads to a better understanding of the interplay between floor and surface. This being said, primes $p \equiv 1 \bmod 4$ are omitted from our discussion, the main reason being Lemma 1 below: for such p, supersingular

[1] Moreover, if $p \equiv 3 \bmod 4$ then $x^3 + Ax^2 - x$ is automatically square-free, allowing for a marginally simpler key validation. But this deserves a footnote, at most.

elliptic curves over $\mathbf{F}_p$ never admit a model of the form $y^2 = x^3 + Ax^2 \pm x$. This complicates comparison with [7]. It is possible that other elliptic curve models can fill this gap, but we leave that for future research.

Acknowledgments

A partial proof of Theorem 3 below can be found in Berre Baelen's master thesis [1], which was the direct inspiration for this research. We thank Luca De Feo for pointing out the relevance to isogeny-based threshold schemes [12], and Frederik Vercauteren for helpful feedback regarding the proof of Lemma 4.

2 Background, and formulation of our main result

Consider a prime number $p > 3$ and a supersingular elliptic curve $E/\mathbf{F}_p$. Its Frobenius endomorphism π_E satisfies $\pi_E \circ \pi_E = -p$, hence $\mathbf{Z}[\sqrt{-p}]$ can be viewed as a subring of the ring $\mathrm{End}_p(E)$ of $\mathbf{F}_p$-rational endomorphisms of E. If $p \equiv 1 \bmod 4$ then this leaves us with one option for $\mathrm{End}_p(E)$, namely $\mathbf{Z}[\sqrt{-p}]$ itself. If $p \equiv 3 \bmod 4$, which is our main case of interest, then we are left with two options for $\mathrm{End}_p(E)$, namely $\mathbf{Z}[\sqrt{-p}]$ and $\mathbf{Z}[(1+\sqrt{-p})/2]$.

For each such option $\mathcal{O}$, we let $\mathcal{E}\ell\ell_p(\mathcal{O})$ denote the set of $\mathbf{F}_p$-isomorphism classes of elliptic curves $E/\mathbf{F}_p$ for which $\mathrm{End}_p(E) \cong \mathcal{O}$. If $p \equiv 3 \bmod 4$ then $\mathcal{E}\ell\ell_p(\mathbf{Z}[\sqrt{-p}])$ is called the *floor*, whereas $\mathcal{E}\ell\ell_p(\mathbf{Z}[(1+\sqrt{-p})/2])$ is called the *surface*; this terminology stems from the structure of the 2-isogeny graph of supersingular elliptic curves over $\mathbf{F}_p$, see Delfs–Galbraith [13].

Remark 1. If $p \equiv 3 \bmod 4$ then it is easy to decide whether a given supersingular elliptic curve $E/\mathbf{F}_p$ is located on the floor or on the surface: in the former case $|E(\mathbf{F}_p)[2]| = 2$ while in the latter case $|E(\mathbf{F}_p)[2]| = 4$. If $p \equiv 3 \bmod 8$ then the 3 outgoing 2-isogenies from a curve on the surface all go *down*, that is, the codomain curves all live on the floor. If $p \equiv 7 \bmod 8$ then only one of the codomain curves is located on the floor.

Recall that S_p^- denotes the set of all coefficients $A \in \mathbf{F}_p$ such that $E_A^- : y^2 = x^3 + Ax^2 - x$ is a supersingular elliptic curve. The elements of S_p^- will be called Montgomery$^-$ coefficients and the corresponding elliptic curves *Montgomery$^-$ curves*. As we will see below, such curves are always located on the surface. Mutatis mutandis, the set S_p^+ contains the Montgomery$^+$ coefficients $a \in \mathbf{F}_p \setminus \{\pm 2\}$ such that the *Montgomery$^+$ curve* $E_a^+ : y^2 = x^3 + ax^2 + x$ is supersingular. If $p \equiv 3 \bmod 8$ then such curves are necessarily located on the floor. However, this is not true if $p \equiv 7 \bmod 8$, in which case we will occasionally write $S_{p,\mathcal{O}}^+$ to denote the subset of S_p^+ corresponding to curves with endomorphism ring $\mathcal{O}$.

To every $E \in \mathcal{E}\ell\ell_p(\mathcal{O})$ and every $\mathfrak{a} \subseteq \mathcal{O}$ we can associate the subgroup

$$E[\mathfrak{a}] \;=\; \bigcap_{\phi \in \mathfrak{a}} \{\, P \in E \,|\, \phi(P) = \infty \,\} \;\subseteq\; E,$$

where, of course, ϕ should be viewed as an endomorphism of E through the isomorphism $\mathrm{End}_p(E) \cong \mathcal{O}$ identifying π_E with $\sqrt{-p}$. We then have:

Theorem 1. *The map* $\rho : \mathcal{C}\ell(\mathcal{O}) \times \mathcal{E}\ell\ell_p(\mathcal{O}) \to \mathcal{E}\ell\ell_p(\mathcal{O})$ *sending* $([\mathfrak{a}], E)$ *to* $\mathfrak{a} \star E := E/E[\mathfrak{a}]$ *is a well-defined free and transitive group action.*

Proof. See [20, Thm. 4.5] and its proof. □

Here $\mathcal{C}\ell(\mathcal{O})$ denotes the ideal-class group of $\mathcal{O}$, and $[\mathfrak{a}]$ denotes the class of an invertible ideal $\mathfrak{a} \subseteq \mathcal{O}$.

The assumption underlying CSIDH is that this is a hard homogeneous space, as soon as p is large enough. From a constructive point of view, the following version of Theorem 1, obtained by incorporating [7, Prop. 8] and Vélu's isogeny formulas (in the version of [18, Prop. 1]), forms its backbone.

Theorem 2. *If* $p \equiv 3 \bmod 8$ *then the map* $\rho^+ : \mathcal{C}\ell(\mathbf{Z}[\sqrt{-p}]) \times S_p^+ \to S_p^+$ *sending* $([\mathfrak{a}], a)$ *to*

$$[\mathfrak{a}] \star a := \left(a - 3 \sum_{\substack{P \in E_a^+[\mathfrak{a}] \\ P \neq \infty}} \left(x(P) - \frac{1}{x(P)} \right) \right) \cdot \prod_{\substack{P \in E_a^+[\mathfrak{a}] \\ P \neq \infty}} x(P)$$

is a well-defined free and transitive group action. Here we assume $(0,0) \notin E_a^+[\mathfrak{a}]$.

The assumption $(0,0) \notin E_a^+[\mathfrak{a}]$ is not a restriction since $\mathcal{C}\ell(\mathbf{Z}[\sqrt{-p}])$ is generated by ideals of odd norm, and by design CSIDH acts by such ideals only.[2]

Our main result is the following variant of Theorem 2, on which our CSURF-512 protocol from Section 6 relies:

Theorem 3. *If* $p \equiv 3 \bmod 4$ *then the maps*

$$\rho^- : \begin{cases} \mathcal{C}\ell(\mathbf{Z}[\sqrt{-p}]) \times S_p^- \to S_p^- & \text{if } p \equiv 3 \bmod 8, \\ \mathcal{C}\ell(\mathbf{Z}[(1+\sqrt{-p})/2]) \times S_p^- \to S_p^- & \text{if } p \equiv 7 \bmod 8 \end{cases}$$

sending $([\mathfrak{a}], A)$ *to*

$$[\mathfrak{a}] \star A := \left(A - 3 \sum_{\substack{P \in E_A^-[\mathfrak{a}] \\ P \neq \infty}} \left(x(P) + \frac{1}{x(P)} \right) \right) \cdot \prod_{\substack{P \in E_A^-[\mathfrak{a}] \\ P \neq \infty}} x(P)$$

are well-defined free and transitive group actions. Here, we assume that the ideal $\mathfrak{a}$ *representing* $[\mathfrak{a}]$ *has odd norm.*

We again note that the class group is generated by ideals of odd norm. However, if $p \equiv 7 \bmod 8$ then $\mathcal{C}\ell(\mathbf{Z}[(1+\sqrt{-p})/2])$ also admits invertible ideals of norm 2, which can be used to speed up the evaluation of ρ^- significantly. These require a separate treatment, which is outlined in Section 4.

[2] It has been pointed out, e.g. in [16,8], that allowing for the action of $(4, \sqrt{-p} - 1)$ leads to a minor improvement. See Remark 2 for some details on how to handle this.

Apart from a striking analogy with Theorem 2, the reader might notice that Theorem 3 is in seeming conflict with Theorem 1 when $p \equiv 3 \bmod 8$. Indeed, since the curves E_A^- always have endomorphism ring $\mathbf{Z}[(1+\sqrt{-p})/2]$, it seems that ρ^- is acting by the wrong class group! However, in Section 3 we will see that every curve on the surface has *three* representants in S_p^-, and at the same time $|\mathcal{C}\ell(\mathbf{Z}[\sqrt{-p}])| = 3|\mathcal{C}\ell(\mathbf{Z}[(1+\sqrt{-p})/2]|$. It turns out that, somewhat surprisingly, Vélu's formulas consistently link both factors 3 to each other.

We note that Theorem 2 can be extended to cover $p \equiv 7 \bmod 8$ as well, by merely adding a subscript $\mathbf{Z}[\sqrt{-p}]$ to S_p^+. But for such p there is also a surface version of Theorem 2, which is more subtle and will be discussed in Appendix B.

Further notation and terminology

The identity element of an elliptic curve E will be denoted by ∞ and context will make it clear to which curve it belongs. An **important convention** is that if $p \equiv 3 \bmod 4$, then for a a square in $\mathbf{F}_p$ we denote by $\sqrt{a}$ the unique square root which is again a square; this can be computed as $a^{(p+1)/4}$. Finally, for $B \in \mathbf{Z}_{>0}$ we write $[-B; B]$ for the set of integers $[-B, B] \cap \mathbf{Z}$.

3 Properties of Montgomery$^-$ curves

3.1 Montgomery$^-$ arithmetic: just a few sign flips

One of the advantages of Montgomery$^+$ curves is that arithmetic on them can be done very efficiently. Fortunately, this can easily be adjusted to work for Montgomery$^-$ curves. E.g., the formulas for point doubling and differential addition, for use in the Montgomery ladder, take the following form.

Proposition 1. *Let $E_A^- : y^2 = x^3 + Ax^2 - x$ be an elliptic curve over a field K of characteristic different from two, with $P, Q \in E_A^-(K)$.*

1. *If $P = \infty$ or $x(P)^3 + Ax(P)^2 - x(P) = 0$, then $2P = \infty$. Else*

$$x(2P) = \frac{(x(P)^2+1)^2}{4(x(P)^3 + Ax(P)^2 - x(P))}.$$

2. *If $\{P, Q, P+Q, P-Q\} \cap \{\infty\} = \emptyset$, then*

$$x(P+Q)x(P-Q) = \frac{(x(P)x(Q)+1)^2}{(x(P)-x(Q))^2}.$$

Proof. This is almost a copy of the corresponding proofs in [2]. □

Likewise, computing odd degree isogenies between Montgomery$^-$ curves just amounts to a few sign changes with respect to the formulas from [18, Prop. 1], leading to the following statement, whose proof can be found in Appendix A. (we will treat 2-isogenies separately in Section 4).

Proposition 2. *Let $E_A^- : y^2 = x^3 + Ax^2 - x$ be an elliptic curve over a field of characteristic not two. Let $G \subseteq E_A^-(K)$ be a finite subgroup such that $|G|$ is odd, and let ϕ be a separable isogeny such that $\ker(\phi) = G$. Then there exists a curve $E_B^- : y^2 = x^3 + Bx^2 - x$ such that, up to composition with an isomorphism,*

$$\begin{aligned} \phi : E_A^- &\to E_B^- \\ (x, y) &\mapsto (f(x), c_0 y f'(x)), \end{aligned}$$

where

$$f(x) = x \prod_{T \in G \setminus \{\infty\}} \frac{x x_T + 1}{x - x_T}.$$

Writing

$$\pi = \prod_{T \in G \setminus \{\infty\}} x_T, \qquad \sigma = \sum_{T \in G \setminus \{\infty\}} \left(x_T + \frac{1}{x_T} \right),$$

we also have that $B = \pi(A - 3\sigma)$, $c_0^2 = \pi$.

As usual, it is better to use projective coordinates to avoid costly field inversions, i.e., to represent the x-coordinate of a projective point $P = (X : Y : Z)$ as $x(P) = X/Z$; the required adaptations are straightforward.

3.2 Locating supersingular Montgomery$^{\pm}$ curves

We now switch to curves over finite prime fields $\mathbf{F}_p$. The lemma below shows that supersingular Montgomery$^-$ curves over $\mathbf{F}_p$ are always located on the surface.

Lemma 1. *Let $p > 3$ be a prime number and let $A \in \mathbf{F}_p$ be such that $E_A^- : y^2 = x^3 + Ax^2 - x$ is supersingular. Then $p \equiv 3 \bmod 4$, and there is no $P \in E_A^-(\mathbf{F}_p)$ such that $2P = (0, 0)$; in particular, $\mathrm{End}_p(E_A^-) \cong \mathbf{Z}[(1 + \sqrt{-p})/2]$.*

Proof. Let P be a point doubling to $(0, 0)$; note that, necessarily, both coordinates are non-zero. The tangent line at P has slope

$$\frac{3x(P)^2 + 2Ax(P) - 1}{2y(P)}.$$

But, since the line should pass through $(0, 0)$, a simpler expression for this slope is $y(P)/x(P)$. Equating both expressions leads to $x(P)^2 + 1 = 0$. Now:

- If $p \equiv 1 \bmod 4$ then we conclude $x(P) = \pm i \in \mathbf{F}_p$ and hence $y(P)^2 = -A \mp 2i$. If both expressions on the right-hand side are non-squares then their product $A^2 + 4$ is a square, but then $x^3 + Ax^2 - x$ factors completely over $\mathbf{F}_p$. We conclude that in any case $4 \mid |E_A^-(\mathbf{F}_p)| = p + 1$, which is a contradiction.
- If $p \equiv 3 \bmod 4$ then this shows that such a point P cannot be $\mathbf{F}_p$-rational. But then $E_A^-(\mathbf{F}_p)[2^\infty] \cong \mathbf{Z}/(2^e) \times \mathbf{Z}/(2)$ for some $e \geq 1$, since $|E_A^-(\mathbf{F}_p)| = p + 1 \equiv 0 \bmod 4$. Thus there are 3 outgoing $\mathbf{F}_p$-rational 2-isogenies, hence in view of [13, Thm. 2.7] our curve must be located on the surface. □

The conclusion $p \equiv 3 \bmod 4$ also applies to supersingular Montgomery$^+$ curves, since it is known [2] that these always carry an $\mathbf{F}_p$-rational point of order 4.

So, from now on, let us assume that $p \equiv 3 \bmod 4$. Then the above lemma settles the 'if' part of Proposition 4 below, which can be viewed as the surface version of the following statement:

Proposition 3. *Let $p > 3$ be a prime number such that $p \equiv 3 \bmod 4$ and let E be a supersingular elliptic curve over $\mathbf{F}_p$. If $\mathrm{End}_p(E) \cong \mathbf{Z}[\sqrt{-p}]$ then there exists a coefficient $a \in \mathbf{F}_p \setminus \{\pm 2\}$ for which E is $\mathbf{F}_p$-isomorphic to the curve $E_a^+ : y^2 = x^3 + ax^2 + x$. Furthermore,*

- *this coefficient is always unique,*
- *if $p \equiv 3 \bmod 8$ then the converse implication holds as well.*

Proof. If $p \equiv 3 \bmod 8$ then this is [7, Prop. 8]. If $p \equiv 7 \bmod 8$ then the relevant part of the proof of [7, Prop. 8] still applies. □

Proposition 4. *Let $p > 3$ be a prime number such that $p \equiv 3 \bmod 4$ and let E be a supersingular elliptic curve over $\mathbf{F}_p$. Then $\mathrm{End}_p(E) \cong \mathbf{Z}[(1 + \sqrt{-p})/2]$ if and only if there exists a coefficient $A \in \mathbf{F}_p$ for which E is $\mathbf{F}_p$-isomorphic to the curve $E_A^- : y^2 = x^3 + Ax^2 - x$. Furthermore,*

- *if $p \equiv 3 \bmod 8$ then there exist exactly three such coefficients,*
- *if $p \equiv 7 \bmod 8$ then this coefficient is unique.*

We will prove this proposition by means of the following convenient tool, connecting floor and surface:

Lemma 2. *Let $p > 3$ be a prime number such that $p \equiv 3 \bmod 4$. Then*

$$\tau : S^+_{p,\mathbf{Z}[\sqrt{-p}]} \to S^-_p : a \mapsto -2a/\sqrt{4 - a^2}$$

is a well-defined bijection.

Proof. For $a, b \in \mathbf{F}_p$ with $a^2 - 4b \neq 0$ let us write $E_{a,b}$ for the elliptic curve $y^2 = x^3 + ax^2 + bx$, which admits the well-known 2-isogeny

$$E_{a,b} \to E_{-2a,a^2-4b} : P \mapsto \begin{cases} \left(\frac{y(P)^2}{x(P)^2}, y(P)(1 - \frac{b}{x(P)^2})\right) & \text{if } P \neq (0,0), \infty \\ \infty & \text{if } P \in \{(0,0), \infty\}. \end{cases} \tag{2}$$

If $a \in S^+_{p,\mathbf{Z}[\sqrt{-p}]}$ then we find that $E_a^+ = E_{a,1}$ is 2-isogenous to the curve

$$E_{-2a,a^2-4} : y^2 = x^3 - 2ax^2 + (a^2 - 4)x,$$

which is necessarily supersingular. Since E_a^+ lives on the floor we see that $a^2 - 4$ is not a square in $\mathbf{F}_p$, hence $4 - a^2$ is a square and letting $\delta = \sqrt{4 - a^2}$, the substitution $x \leftarrow \delta x$, $y \leftarrow \delta^{3/2} y$ transforms the above equation into $y^2 = x^3 - 2a/\sqrt{4 - a^2}x^2 - x$. We conclude that τ is indeed well-defined.

Conversely, if $A \in S_p^-$ then we find that $E_A^- = E_{A,-1}$ is 2-isogenous to

$$E_{-2A,A^2+4} : y^2 = x^3 - 2Ax^2 + (A^2+4)x.$$

Since E_A^- lives on the surface by Lemma 1, we have that A^2+4 is a square in $\mathbf{F}_p$. Letting $\delta = \sqrt{A^2+4}$, the same substitution transforms our equation into $y^2 = x^3 - 2A/\sqrt{A^2+4}x^2 + x$. It is easily checked that this curve has no $\mathbf{F}_p$-rational points of order 2 besides $(0,0)$, hence the map

$$S_p^- \to S^+_{p,\mathbf{Z}[\sqrt{-p}]} : A \mapsto -2A/\sqrt{A^2+4} \tag{3}$$

is also well-defined. An easy calculation shows that it is an inverse of τ. □

Proof of Proposition 4. By Proposition 3 each $\mathbf{F}_p$-isomorphism class of elliptic curves on the floor is represented by a unique Montgomery$^+$ curve. Since such curves have a unique $\mathbf{F}_p$-rational point of order 2, the proof of Lemma 2 shows that $\mathbf{F}_p$-rational 2-isogenies give a 1-to-1 correspondence between $\mathcal{E}\ell\ell_p(\mathbf{Z}[\sqrt{-p}])$ and S_p^-. But on the level of $\mathbf{F}_p$-isomorphism classes, by [13, Thm. 2.7] this correspondence is 3-to-1 if $p \equiv 3 \bmod 8$ and 1-to-1 if $p \equiv 7 \bmod 8$. □

If $p \equiv 7 \bmod 8$ then Proposition 3 leaves open whether or not there exist $a \in S_p^+$ such that E_a^+ is located on the surface. To answer this, we rely on the following lemma, whose proof can be found in Appendix B.

Lemma 3. *If $p \equiv 7 \bmod 8$ then every $E \in \mathcal{E}\ell\ell_p(\mathbf{Z}[(1+\sqrt{-p})/2])$ comes with three distinguished points of order 2:*

- *P^-, the x-coordinates of whose halves are not defined over $\mathbf{F}_p$,*
- *P_1^+, whose halves are not defined over $\mathbf{F}_p$, but their x-coordinates are,*
- *P_2^+, whose halves are defined over $\mathbf{F}_p$.*

Corollary 1. *If $p \equiv 7 \bmod 8$ then each $E \in \mathcal{E}\ell\ell_p(\mathbf{Z}[(1+\sqrt{-p})/2])$ admits exactly 2 coefficients $a \in \mathbf{F}_p \setminus \{\pm 2\}$ for which E is $\mathbf{F}_p$-isomorphic to the curve $E_a^+ : y^2 = x^3 + ax^2 + x$.*

Proof. By Proposition 4, such curves admit a unique Montgomery$^-$ model. Note that, for this model, P^- is positioned at $(0,0)$. The two Montgomery$^+$ models are obtained by translating P_1^+ or P_2^+ to $(0,0)$ and scaling down the resulting b-coefficient (which is a square) to 1, by means of a coordinate change. □

Table 1 summarizes how and with what frequency Montgomery$^\pm$ curves show up as representants of $\mathbf{F}_p$-isomorphism classes of supersingular elliptic curves.

4 2-isogenies between Montgomery$^-$ curves

In this section we assume that $p \equiv 7 \bmod 8$ and we consider the maximal order $\mathbf{Z}[(1+\sqrt{-p})/2]$, in which $(2) = (2,(\sqrt{-p}-1)/2)(2,(\sqrt{-p}+1)/2)$. We describe a fast method for computing the repeated action of one of the factors as a chain of 2-isogenies. This relies on the following remarkably precise statement (recall our convention on square roots!), whose proof can be found in Appendix B.

		$(\lvert S^+_{p,\mathcal{O}}\rvert : \lvert\mathcal{E}\ell\ell_p(\mathcal{O})\rvert)$	$(\lvert S^-_p\rvert : \lvert\mathcal{E}\ell\ell_p(\mathcal{O})\rvert)$
$p \equiv 3 \bmod 8$	$\mathcal{O} = \mathbf{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$	0	$(3:1)$
	$\mathcal{O} = \mathbf{Z}[\sqrt{-p}]$	$(1:1)$	0
$p \equiv 7 \bmod 8$	$\mathcal{O} = \mathbf{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$	$(2:1)$	$(1:1)$
	$\mathcal{O} = \mathbf{Z}[\sqrt{-p}]$	$(1:1)$	0
$p \equiv 1 \bmod 4$		0	0

Table 1. The ratio of the number of Montgomery$\pm$ coefficients to the number of $\mathbf{F}_p$-isomorphism classes of supersingular elliptic curves.

Lemma 4 (Addendum to Lemma 3). *Assume $p \equiv 7 \bmod 8$ and consider an elliptic curve $E : y^2 = x^3 + ax^2 + bx \in \mathcal{E}\ell\ell_p(\mathbf{Z}[(1+\sqrt{-p})/2])$. Let $\delta = \sqrt{a^2 - 4b}$ and $T_1 = ((-a+\delta)/2, 0)$, $T_1 = ((-a-\delta)/2, 0)$. Then:*

1. *if $(0,0) = P^-$ then $T_1 = P_2^+$ and $T_1 = P_1^+$,*
2. *if $(0,0) = P_1^+$ then $T_1 = P_2^+$ and $T_2 = P^-$,*
3. *if $(0,0) = P_2^+$ then $T_1 = P^-$ and $T_2 = P_1^+$.*

This will be combined with the following fact:

Lemma 5. *Assume that $p \equiv 7 \bmod 8$ and let $E \in \mathcal{E}\ell\ell_p(\mathbf{Z}[(1+\sqrt{-p})/2])$. Then*

$$E\left[\left(2, \frac{\sqrt{-p}-1}{2}\right)\right] = \langle P_2^+ \rangle \qquad \text{and} \qquad E\left[\left(2, \frac{\sqrt{-p}+1}{2}\right)\right] = \langle P_1^+ \rangle.$$

Proof. As in the proof of Lemma 2 one checks that P^- takes us down to the floor, so it suffices to prove the first equality. Let $Q \in E(\mathbf{F}_p)$ be such that $2Q = P_2^+$ and let ϕ denote the endomorphism $\frac{\pi_E - 1}{2}$, then $\phi(P_2^+) = \phi(2Q) = 2\phi(Q) = \pi_E(Q) - Q = \infty$, from which the statement follows. □

The formulas to compute 2-isogenies between Montgomery$^-$ curves seem easiest if we perform almost all of them on isomorphic Montgomery$^+$ curves. We formulate the procedure in the form of an algorithm.

Sketch of the proof of Algorithm 1. Note that quadratic twisting swaps the roles of P_1^+ and P_2^+, so with Lemma 5 in mind, we can simply flip the sign of A at the start and the end of the algorithm and focus on P_2^+. Line 4 constitutes a translation $x \leftarrow x + (-a+\delta)/2$, which by Lemma 4 positions $T_1 = P_2^+$ at the origin, followed by the 2-isogeny from (2) and a rescaling to obtain a Montgomery$^+$ curve.

Line 6 is immediate from [18, Proposition 2], where it should be noted that, due to our choice of canonical square root, $x(P_2^+)$ is always a square so that we do not need to consider possible twists. Line 7 is just a translation followed by a rescaling to put everything back in Montgomery$^-$ form. □

Algorithm 1 Computing the action of $(2, (\sqrt{-p}-1)/2)^e$ on $A \in S_p^-$, with $p \equiv 7 \bmod 8$

$A \leftarrow \mathrm{sign}(e) \cdot A$
if $e = 0$ **then return** A
else
    $A \leftarrow 2\frac{A-3\sqrt{A^2+4}}{A+\sqrt{A^2+4}}$
for i from 2 to e **do**
    $A \leftarrow 2(3 + A(\sqrt{A^2-4} - A))$
$A \leftarrow \frac{A+3\sqrt{A^2-4}}{\sqrt{2\sqrt{A^2-4}\left(A+\sqrt{A^2-4}\right)}}$
return $\mathrm{sign}(e) \cdot A$

5 'New' hard homogeneous spaces

For each non-zero entry of Table 1 we obtain a specialization of Theorem 1. For instance, Theorem 2 corresponds to the entry covering Montgomery$^+$ curves, primes $p \equiv 3 \bmod 8$ and endomorphism ring $\mathcal{O} = \mathbf{Z}[\sqrt{-p}]$. The main goal of this section is to prove Theorem 3, which takes care of two further entries, namely those corresponding to Montgomery$^-$ curves, primes $p \equiv 3, 7 \bmod 8$ and endomorphism ring $\mathcal{O} = \mathbf{Z}[(1+\sqrt{-p})/2]$:

Proof of Theorem 3. If $p \equiv 7 \bmod 8$ then this follows immediately from Theorem 1, along with Proposition 2 and the fact that each $\mathbf{F}_p$-isomorphism class on the surface is represented by exactly one Montgomery$^-$ curve.

If $p \equiv 3 \bmod 8$ then consider the bijection τ from Lemma 2, and let ρ^+ be the group action from Theorem 2. We then define

$$\mathcal{C}\ell(\mathbf{Z}[\sqrt{-p}]) \times S_p^- \to S_p^- \ : \ ([\mathfrak{a}], A) \mapsto \tau(\rho^+([\mathfrak{a}], \tau^{-1}(A))),$$

which is clearly a well-defined free and transitive group action, simply because τ is a bijection. So it suffices to show that this matches with ρ^-. For this, consider a Montgomery$^-$ coefficient A and an invertible ideal $\mathfrak{a} \subseteq \mathbf{Z}[\sqrt{-p}]$ having odd norm, along with the subgroup of E_A^- spanned by $E_A^-[\mathfrak{a}]$ and $(0,0)$. We quotient out this subgroup in the following two ways:

- We first quotient out by $E_A^-[\mathfrak{a}]$, using the formulas from Proposition 2, yielding a Montgomery$^-$ curve E_B^-. Let us abusingly denote the corresponding isogeny by ρ^-, and note that it maps $(0,0)$ to $(0,0)$. So we can continue by applying the 2-isogeny from (2), in order to arrive at the Montgomery$^+$ curve $E^+_{\tau^{-1}(B)}$ on the floor.
- Conversely, we apply the 2-isogeny from (2), taking us to the Montgomery$^+$ curve $E^+_{\tau^{-1}(A)}$. Note that this maps $E_A^-[\mathfrak{a}]$ to $E^+_{\tau^{-1}(A)}[\mathfrak{a}]$, which we quotient out in turn, by means of the formulas from [18, Prop. 1]. By the same abuse of notation, we denote the latter isogeny by ρ^+. Because every curve on the floor is represented by a unique Montgomery$^+$ coefficient, this necessarily takes us to $E^+_{\tau^{-1}(B)}$.

Thus we obtain the diagram

$$\begin{array}{ccc} E_A^- & \xrightarrow{\rho^-} & E_B^- \\ \downarrow{\scriptstyle \theta_A} & & \downarrow{\scriptstyle \theta_B} \\ E^+_{\tau^{-1}(A)} & \xrightarrow{\rho^+} & E^+_{\tau^{-1}(B)} \end{array}$$

with θ_A and θ_B denoting the above 2-isogenies, where our reasoning in fact shows that $[\pm 1] \circ \theta_B \circ \rho^- = \rho^+ \circ \theta_A$. This implies that $[\pm 2] \circ \rho^- = \hat{\theta}_B \circ \rho^+ \circ \theta_A$. Multiplication by ± 2 does not change the curve E_B^-, so we are done. □

This leaves us with the two entries corresponding to Montgomery$^+$ curves and primes $p \equiv 7 \bmod 8$. This behaves less uniformly since some curves live on the surface and some live on the floor, and in any case these entries seem of lesser cryptographic interest. We will elaborate on them in Appendix B.

Remark 2. Here are two examples of how the surface can help in understanding the floor. We assume $p \equiv 3 \bmod 8$.

- Let $a, a' \in S_p^+$ be given and let $[\mathfrak{a}] \in \mathcal{C}\ell(\mathbf{Z}[\sqrt{-p}])$ be an unknown ideal class such that $a' = [\mathfrak{a}] \star a$ (action by ρ^+ on the floor). By the foregoing proof this is equivalent with $\tau(a') = [\mathfrak{a}] \star \tau(a)$ (action by ρ^- on the surface), which on the level of $\mathbf{F}_p$-isomorphism classes implies that

  $$E^-_{\tau(a')} \cong [\tilde{\mathfrak{a}}] \star E^-_{\tau(a)},$$

  where $\tilde{\mathfrak{a}}$ is the ideal of $\mathbf{Z}[(1+\sqrt{-p})/2]$ generated by $\mathfrak{a}$. Clearly, in order to find $[\mathfrak{a}]$ it suffices to find $[\tilde{\mathfrak{a}}]$, and then simply try the 3 corresponding possibilities for $\mathfrak{a}$. This confirms that the factor 3 in $|\mathcal{C}\ell(\mathbf{Z}[\sqrt{-p}])|$ offers little extra security to CSIDH.
- If we want a fast evaluation of the action of $[(4, \sqrt{-p}-1)] \in \mathcal{C}\ell(\mathbf{Z}[\sqrt{-p}])$ on S_p^+, this can be done by composing two 2-isogenies, thereby passing through the surface using τ and τ^{-1}. We leave it as an exercise to verify that this leads to the simple formula $[(4, \sqrt{-p}-1)] \star a = 2(a-6)/(a+2)$, which can also be found in [16, §4.2].

6 Implementation

We assume that the reader is familiar with how CSIDH is being set up in practice [7]. In this section we use Theorem 3 and Algorithm 1 to design a variant of CSIDH acting on S_p^- rather than S_p^+. Recall from [7] that CSIDH-512 uses the prime

$$p = 4 \cdot \underbrace{(3 \cdot \ldots \cdot 373)}_{\text{73 first odd primes}} \cdot 587 - 1 \approx 2^{510.668},$$

and then samples exponents from the range $[-5; 5]^{74}$ to represent an element in the class group and let it act on $0 \in S_p^+$, for a conjectured 128 bits of classical

security. Concretely, the exponent vector $(e_1, \ldots, e_{74})$ in this case represents the class group element $(3, \sqrt{-p}-1)^{e_1} \cdots (587, \sqrt{-p}-1)^{e_{74}}$. For the sake of comparison, we propose CSURF-512 which works over $\mathbf{F}_p$ where

$$p = 2^3 \cdot 3 \cdot \underbrace{(3 \cdot \ldots \cdot 389)}_{\substack{74 \text{ consecutive primes,} \\ \text{skip 347 and 359}}} - 1 \approx 2^{512.880}.$$

This prime will speed up the computation of a class group action in multiple ways. First of all, the largest isogeny we need to compute is of degree 389 instead of 587. Secondly, $p+1$ carries an extra factor 3 that can help with sampling points of order 3 to compute 3-isogenies. Indeed, finding an ℓ-torsion point typically amounts to sampling a random point P and multiplying it by $(p+1)/\ell$, which has a $1/\ell$ chance of failure. For CSURF-512 we can multiply a random point P by both $(p+1)/9$ and $(p+1)/3$ to try and find a point of order 3.

The biggest speed-up however stems from the fact that $p \equiv 7 \bmod 8$, so we now have 2 as a 75th prime to use. Furthermore 2-isogenies are very fast due to their simple and explicit formulae, see Algorithm 1, so we can sample the exponent for 2 from a much larger interval. In practice we evaluate these 2-isogenies first, without pushing through points, and then proceed with the other primes as in CSIDH.

We implemented both CSIDH-512 and CSURF-512 in Magma [6] to compare their performance. With the exception of 2-isogenies, both implementations are totally similar, making use of the (projective) Montgomery ladder, the pushing through of points, etc., the only differences being the sign switches discussed in Section 3.1. However, we did not implement any of the constant-time measures since these are orthogonal to the speed-up we described. Based on experiments, a near-optimal set to sample exponent vectors from seems to be

$$I = [-137; 137] \times [-4; 4]^3 \times [-5; 5]^{46} \times [-4; 4]^{25},$$

which results in $275 \cdot 9^{28} \cdot 11^{46} \approx 2^{255.995}$ distinct secret vectors. As in CSIDH-512, we heuristically expect that these vectors represent the elements in the class group quasi-uniformly. Note that for 3-, 5- and 7-isogenies we sample from a smaller interval, since the ease of computing the isogeny is outweighed by the high failure probability of finding the needed torsion points. Sampling from this specific set of exponent vectors gives CSURF-512 a speed-up of about 5.68% compared to CSIDH-512; this estimate is based on an experiment generating 25 000 public keys in both settings. Our source code can be found at `https://github.com/TDecru/CSURF`.

As a final remark, we note that the advantage of working on the surface is expected to diminish when the underlying prime p becomes larger, since the relative contribution of 2-isogenies will decrease. This is especially relevant given the ongoing discussion about the conjectured quantum security of the protocol, see for example [5,17,3]. However, if $p \equiv 7 \bmod 8$ then the surface will always outperform the floor to some extent, due to the availability of horizontal 2-isogenies. This means that setting up these larger instantiations of the CSIDH protocol should preferably be done on the surface, in any case.

References

1. Berre Baelen. Post-quantum key-exchange: Using group actions from supersingular elliptic curve isogenies. Master's thesis, KU Leuven, 2019.
2. Daniel J Bernstein and Tanja Lange. Montgomery curves and the Montgomery ladder. *IACR Cryptology ePrint Archive*, 2017:293, 2017.
3. Daniel J. Bernstein, Tanja Lange, Chloe Martindale, and Lorenz Panny. Quantum circuits for the csidh: optimizing quantum evaluation of isogenies. Cryptology ePrint Archive, Report 2018/1059, 2018.
4. Ward Beullens, Thorsten Kleinjung, and Frederik Vercauteren. CSI-FiSh: Efficient isogeny based signatures through class group computations. In Steven Galbraith and Shiho Moriai, editors, *Advances in Cryptology – ASIACRYPT 2019, Part I*, pages 227–247, 2019.
5. Xavier Bonnetain and André Schrottenloher. Submerging CSIDH. *IACR Cryptology ePrint Archive*, page 537, 2018.
6. 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).
7. Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: An efficient post-quantum commutative group action. In Thomas Peyrin and Steven Galbraith, editors, *Advances in Cryptology – ASIACRYPT 2018, Part III*, pages 395–427, 2018.
8. Wouter Castryck, Lorenz Panny, and Frederik Vercauteren. Rational isogenies from irrational endomorphisms. *IACR Cryptology ePrint Archive*, 2019:1202, 2019.
9. Daniel Cervantes-Vázquez, Mathilde Chenu, Jesús-Javier Chi-Domínguez, Luca De Feo, Francisco Rodríguez-Henríquez, and Benjamin Smith. Stronger and faster side-channel protections for CSIDH. In *International Conference on Cryptology and Information Security in Latin America*, pages 173–193, 2019.
10. Jean-Marc Couveignes. Hard homogeneous spaces. *IACR Cryptology ePrint Archive*, 2006:291, 2006.
11. Luca De Feo, Simon Masson, Christophe Petit, and Antonio Sanso. Verifiable delay functions from supersingular isogenies and pairings. *IACR Cryptology ePrint Archive*, 2019:166, 2019.
12. Luca De Feo and Michael Meyer. Threshold schemes from isogeny assumptions. *IACR Cryptology ePrint Archive*, 2019:1288, 2019.
13. Christina Delfs and Steven D Galbraith. Computing isogenies between supersingular elliptic curves over $\mathbf{F}_p$. *Designs, Codes and Cryptography*, 78(2):425–440, 2016.
14. Aaron Hutchinson, Jason LeGrow, Brian Koziel, and Reza Azarderakhsh. Further optimizations of CSIDH: A systematic approach to efficient strategies, permutations, and bound vectors. *IACR Cryptology ePrint Archive*, 2019:1121, 2019.
15. Greg Kuperberg. Another subexponential-time quantum algorithm for the dihedral hidden subgroup problem. In *8th Conference on the Theory of Quantum Computation, Communication and Cryptography*, volume 22 of *LIPIcs. Leibniz Int. Proc. Inform.*, pages 20–34, 2013.
16. Hiroshi Onuki and Tsuyoshi Takagi. On collisions related to an ideal class of order 3 in CSIDH. *IACR Cryptology ePrint Archive*, 2019:1209, 2019.
17. Chris Peikert. He gives C-sieves on the CSIDH. *IACR Cryptology ePrint Archive*, 2019:725, 2019.

18. Joost Renes. Computing isogenies between Montgomery curves using the action of $(0,0)$. In *International Conference on Post-Quantum Cryptography*, pages 229–247. Springer, 2018.
19. Alexander Rostovtsev and Anton Stolbunov. Public-key cryptosystem based on isogenies. *IACR Cryptology ePrint Archive*, 2006:145, 2006.
20. René Schoof. Nonsingular plane cubic curves over finite fields. *J. Combin. Theory Ser. A*, 46(2):183–211, 1987.
21. Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999.
22. Anton Stolbunov. Public-key encryption based on cycles of isogenous elliptic curves. Master's thesis, Saint-Petersburg State Polytechnical University, 2004. In Russian.
23. Anton Stolbunov. *Cryptographic Schemes Based on Isogenies*. PhD thesis, Norwegian University of Science and Technology, 2011.

Appendix A Proof of Proposition 2

Proof of Proposition 2. Let $i, \theta \in \bar{K}$ be such that $i^2 = -1$ and $\theta^2 = i$, and let $\ell = |G|$. We will construct the isogeny ϕ as the concatenation of $\phi_3 \circ \phi_2 \circ \phi_1$ as illustrated in the following diagram,

$$\begin{array}{ccc} E_A^- & \xrightarrow{\phi} & E_B^- \\ \downarrow{\scriptstyle \phi_1} & & \uparrow{\scriptstyle \phi_3} \\ E_a^+ & \xrightarrow{\phi_2} & E_b^+ \end{array}$$

where $\phi_2 : E_a^+ \to E_b^+$ is the isogeny from [18, Prop. 1], and the elliptic curves are given by the Montgomery$^+$ forms $E_a^+ : y^2 = x^3 + ax^2 + x$ and $E_b^+ : y^2 = x^3 + bx^2 + x$.

The isogenies ϕ_1 and ϕ_3 are in fact isomorphisms (over an extension field) given by

$$\begin{aligned} \phi_1 : E_A^- &\to E_a^+ \\ (x, y) &\mapsto (-ix, \theta y) \end{aligned}$$

and

$$\begin{aligned} \phi_3 : E_b^+ &\to E_B^- \\ (x, y) &\mapsto (ix, -i\theta y). \end{aligned}$$

It is easy to verify that $a = -iA$ and $B = ib$. The rest of the proof is just a straightforward calculation. With the formulas from [18] we can compute the coefficient b as $\tilde{\pi}(a - 3\tilde{\sigma}) = (-i)^\ell \pi(A - 3\sigma)$ where

$$\tilde{\pi} = \prod_{T \in \phi_1(G) \setminus \{\infty\}} x_T = \prod_{T \in G \setminus \{\infty\}} -ix_T = (-i)^{\ell - 1} \pi,$$

$$\tilde{\sigma} = \sum_{T \in \phi_1(G) \setminus \{\infty\}} \left(x_T - \frac{1}{x_T} \right) = \sum_{T \in G \setminus \{\infty\}} \left(-ix_T + \frac{1}{ix_T} \right) = -i\sigma.$$

Similarly if we define

$$\tilde{f} = x \left(\prod_{T \in \phi_1(G) \setminus \{\infty\}} \left(\frac{xx_T - 1}{x - x_T} \right) \right),$$

then with ${\tilde{c}_0}^2 = \tilde{\pi} = (-i)^{\ell-1}\pi$, we have

$$\begin{aligned}
(\phi_2 \circ \phi_1)(x, y) &= \left(\tilde{f}(-ix), \tilde{c}_0 \theta y \tilde{f}'(-ix) \right) \\
&= \left(-ix \prod_{T \in \phi_1(G) \setminus \{\infty\}} \left(\frac{-ixx_T - 1}{-ix - x_T} \right), \tilde{c}_0 \theta y \tilde{f}'(-ix) \right) \\
&= \left(-ix \prod_{T \in G \setminus \{\infty\}} \left(\frac{-xx_T - 1}{-ix + ix_T} \right), \tilde{c}_0 \theta y \tilde{f}'(-ix) \right) \\
&= \left(-i^\ell f(x), \tilde{c}_0 \theta y \tilde{f}'(-ix) \right) \\
&= \left(-i^\ell f(x), \tilde{c}_0 \theta y (-i)^{\ell-1} f'(x) \right).
\end{aligned}$$

If we assume $\ell \equiv 1 \bmod 4$ then $(-i)^{\ell-1} = 1$ such that $\tilde{c}_0$ is just a square root of π. Composing this with $\phi_3(x, y) = (ix, -i\theta y)$ we get that

$$\phi(x, y) = (f(x), \tilde{c}_0 y f'(x)),$$

as well as $B = \pi(A - 3\sigma)$. In this case we let $c_0 = \tilde{c}_0$.

If $\ell \equiv 3 \bmod 4$ then ${\tilde{c}_0}^2 = -\pi$ and the isogeny may not be defined over K. Post-composing it with the isomorphism $\tau : (x, y) \mapsto (-x, iy)$ fixes this if needed. In this case we find

$$\phi(x, y) = (f(x), -i\tilde{c}_0 y f'(x)),$$

and again $B = \pi(A - 3\sigma)$. Defining $c_0 = -i\tilde{c}_0$ finishes the proof. □

Appendix B Further surface statements for $p \equiv 7 \bmod 8$

Proofs of some claims on the points of order 2

Proof of Lemma 3. From the structure of $E(\mathbf{F}_p)[2^\infty]$ one sees that there is indeed a unique point P_2^+ of order 2 whose halves are $\mathbf{F}_p$-rational. If we position P_2^+ at $(0, 0)$ we find a model $y^2 = x^3 + ax^2 + bx$, where necessarily b is a square, as can be seen by mimicking the proof of Lemma 1. When translating the other points of order 2 to the origin we get similar equations, of which the coefficients at x become $\delta(\delta \pm a)/2$ with $\delta = \sqrt{a^2 - 4b}$. The product of these coefficients equals $-b\delta^2$, hence we conclude that one coefficient is a non-square and one coefficient is a square. So, again as in the proof of Lemma 1, we see that the former translated point equals P^-, while the latter translated point equals P_1^+. □

Proof of Lemma 4. The change of coordinates $x \leftarrow x + (-a+\delta)/2$ yields

$$y^2 = x\left(x + \frac{-a+\delta}{2}\right)(x+\delta) = x^3 + \frac{-a+3\delta}{2}x^2 + \frac{\delta(-a+\delta)}{2}x \qquad (4)$$

and positions T_1 at the origin. As in the proof of Lemma 1 we see that $T_1 = P_1^+$ or $T_1 = P_2^+$ if and only if the coefficient $\delta(-a+\delta)/2$ is a square, i.e., if and only if $-a+\delta$ is a square.

In particular, for case *2* it suffices to show that $-a+\delta$ is a square. To this end, note that the 2-isogeny from the proof of Lemma 2 takes our input curve $E : y^2 = x^3 + ax^2 + bx$ to $y^2 = x^3 - 2ax^2 + \delta^2 x$, while mapping P_2^+ to $(0,0)$. But then an $\mathbf{F}_p$-rational half of P_2^+ is mapped to an $\mathbf{F}_p$-rational half of $(0,0)$, which is necessarily of the form $(\pm\delta, \sqrt{2\delta^2(-a\pm\delta)})$. We conclude that at least one of $-a+\delta$ or $-a-\delta$ is a square, but then both elements are squares since their product equals the square $4b$.

Similarly, for case *3* it suffices to prove that $-a+\delta$ is not a square. We can consider the same 2-isogeny, which now maps P_1^+ to $(0,0)$. Using that any point $Q \in E(\mathbf{F}_{p^2} \setminus \mathbf{F}_p)$ doubling to P_1^+ satisfies $\pi_E(Q) = -Q$, which is different from both Q and $Q+(0,0)$, we conclude that the image of P_1^+ cannot be $\mathbf{F}_p$-halvable. From this the desired conclusion follows.

Finally, to settle case *1*, consider the curve (4), whose point $(0,0)$ is either P_1^+ or P_2^+. Also note that the first non-trivial factor in (4) corresponds to P^-. But using the identity

$$\left(\frac{-a+3\delta}{2}\right)^2 - 4\frac{\delta(-a+\delta)}{2} = \left(\frac{a+\delta}{2}\right)^2,$$

we can rewrite (4) as

$$y^2 = x\left(x - \frac{-\frac{-a+3\delta}{2} + \frac{a+\delta}{2}}{2}\right)\left(x - \frac{-\frac{-a+3\delta}{2} - \frac{a+\delta}{2}}{2}\right).$$

Using *2* and the fact that $(a+\delta)/2$ is a square, we see that if $(0,0) = P_1^+$, then the first non-trivial factor of (4) would instead correspond to P_2^+. We conclude that $(0,0) = P_2^+$, from which the lemma follows. □

Hard homogeneous spaces from supersingular Montgomery$^+$ curves

If $p \equiv 7 \bmod 8$ then $|\mathcal{C}\ell(\mathbf{Z}[\sqrt{-p}])| = |\mathcal{C}\ell(\mathbf{Z}[(1+\sqrt{-p})/2])|$. Hence in view of Table 1 there are exactly 3 times as many supersingular Montgomery$^+$ coefficients $a \in \mathbf{F}_p \setminus \{\pm 2\}$ as there are $\mathbf{F}_p$-isomorphism classes of supersingular elliptic curves:

– Under the map $a \mapsto E_a^+$, one third of these are in a 1-to-1 correspondence with $\mathcal{E}\ell\ell_p(\mathbf{Z}[\sqrt{-p}])$. In particular, Theorem 2 remains valid for $p \equiv 7 \bmod 8$, provided that we replace S_p^+ with $S_{p,\mathbf{Z}[\sqrt{-p}]}^+$.

– According to the proof of Corollary 1, the other two thirds split into

$$S^+_{p,\mathbf{Z}[(1+\sqrt{-p})/2],1} = \{\, a \in S^+_{p,\mathbf{Z}[(1+\sqrt{-p})/2]} \mid (0,0) \notin 2E^+_a(\mathbf{F}_p) \,\}$$

and

$$S^+_{p,\mathbf{Z}[(1+\sqrt{-p})/2],2} = \{\, a \in S^+_{p,\mathbf{Z}[(1+\sqrt{-p})/2]} \mid (0,0) \in 2E^+_a(\mathbf{F}_p) \,\},$$

and both sets are in a 1-to-1 correspondence with $\mathcal{E}\ell\ell_p(\mathbf{Z}[(1+\sqrt{-p})/2])$. Since the instantiated versions of Vélu's formulae map $(0,0)$ to $(0,0)$, in the statement of Theorem 2 we are equally allowed to replace $\mathbf{Z}[\sqrt{-p}]$ with $\mathbf{Z}[(1+\sqrt{-p})/2]$ and S^+_p with $S^+_{p,\mathbf{Z}[(1+\sqrt{-p})/2],i}$, for any choice of $i = 1, 2$.

Remark 3. The latter setting again allows for horizontal 2-isogenies, therefore it should give rise to very similar timings as those reported upon in Section 6. One minor drawback is that Alice and Bob should agree on the value of i and validate each other's public keys as such; moreover 0 can no longer be used as a starting coefficient.

Remark 4. Alternatively, it is natural to view

$$S^+_{p,\mathbf{Z}[(1+\sqrt{-p})/2],1} \qquad \text{and} \qquad S^+_{p,\mathbf{Z}[(1+\sqrt{-p})/2],2}$$

as two orbits under the free but *non-transitive* action

$$\rho^+ : \mathcal{C}\ell(\mathbf{Z}[(1+\sqrt{-p})]) \times S^+_{p,\mathbf{Z}[(1+\sqrt{-p})/2]} \to S^+_{p,\mathbf{Z}[(1+\sqrt{-p})/2]}$$

described by the same formulae. Using that the quadratic twisting map $E^+_a \mapsto E^+_{-a}$ jumps back and forth between the two orbits, along with the fact that $[\mathfrak{a}] \star E^t \cong ([\mathfrak{a}]^{-1} \star E)^t$ (see e.g. [8, Lem. 5]), the two orbits can be glued together into a single orbit under an action by the dihedral group $\operatorname{Dih} \mathcal{C}\ell(\mathbf{Z}[(1+\sqrt{-p})])$.