J. Math. Cryptol. ? (????), 1–23
DOI 10.1515/jmc-????-???

Orienting supersingular isogeny graphs

Leonardo Colò and David Kohel

Communicated by ???

Abstract. We introduce a category of $\mathcal{O}$-oriented supersingular elliptic curves and derive properties of the associated oriented and nonoriented ℓ-isogeny supersingular isogeny graphs. As an application we introduce an oriented supersingular isogeny Diffie-Hellman protocol (OSIDH), analogous to the supersingular isogeny Diffie-Hellman (SIDH) protocol and generalizing the commutative supersingular isogeny Diffie-Hellman (CSIDH) protocol.

Keywords. Supersingular elliptic curves, isogeny graphs.

1 Introduction

We introduce a category of supersingular elliptic curves oriented by an imaginary quadratic order $\mathcal{O}$, and derive properties of the associated oriented and nonoriented supersingular ℓ-isogeny graphs. This permits one to derive a group action on a set of oriented supersingular points, mapping to the set of nonoriented supersingular points. As an application we introduce an oriented supersingular isogeny Diffie-Hellman protocol (OSIDH), analogous to the supersingular isogeny Diffie-Hellman (SIDH) of DeFeo and Jao [18] and generalizing the commutative supersingular isogeny Diffie-Hellman (CSIDH) of Castryck, Lange, Martindale, Panny and Renes [4], the latter based on the idea of group actions on sets by Couveignes [8] and Rostovtsev-Stolbunov [26].

The idea of SIDH is to fix a large prime number p of the form $p = \ell_A^{e_A}\ell_B^{e_B} f \pm 1$ for a small cofactor f and to let the two parties Alice and Bob take random walks (i.e., isogenies chains) of length e_A (or e_B) in the ℓ_A-isogeny graph (or the ℓ_B-isogeny graph, respectively) on the set of supersingular j-invariants defined over $\mathbb{F}_{p^2}$. In order to have the two key spaces of similar size $\ell_A^{e_A} \approx \ell_B^{e_B}$, we need to take $\ell_A^{e_A} \approx \ell_B^{e_B} \approx \sqrt{p}$. Since the total number of supersingular j-invariants is around $p/12$, this implies that, for each party, the space of choices for the secret key is limited to a fraction of the whole set of supersingular j-invariants over $\mathbb{F}_{p^2}$. In other words, in choosing their secrets, Alice and Bob can go only "halfway" around the graph from the starting vertex j_0.

Recently, Castryck, Lange, Martindale, Panny and Rennes proposed another key exchange protocol based on supersingular isogeny graphs over the prime field $\mathbb{F}_p$. We fix a prime of the form $p = 4\ell_1 \cdot \ldots \cdot \ell_t - 1$ and an elliptic curve $E/\mathbb{F}_p$ defined by the equation $E : y^2 = x^3 + ax^2 + x$. The peculiarity of CSIDH is that it works with curves defined over $\mathbb{F}_p$ and restricts the endomorphism rings of such curves to the commutative subring consisting of $\mathbb{F}_p$-rational endomorphisms. Starting from this setup, the scheme is an adaptation of the Couveignes and Rostovtsev-Stolbunov idea.

A feature shared by SIDH and CSIDH is that the isogenies are constructed as quotients of rational torsion subgroups: the secret path of length e_A in the ℓ_A-isogeny graph corresponds to a secret cyclic subgroup $\langle A \rangle \subseteq E\left[\ell^{e_A}\right]$ where A is a rational $\ell_A^{e_A}$-torsion point on E. The need for rational points limits the choice of the prime p and, thus, of the finite field we work on.

In this paper we want to describe a new cryptographic protocol, the OSIDH, defined over an arbitrarily large subset of oriented supersingular elliptic curves over $\mathbb{F}_{p^2}$, which permits us to cover essentially all isomorphism classes of supersingular elliptic curves and avoid conditions on the rational torsion subgroups.

2 Orientations, isogeny chains, and ladders

Let E be a supersingular elliptic curve over a finite field k of characteristic p, and denote by $\mathrm{End}(E)$ the full endomorphism ring. We denote by $\mathrm{End}^0(E)$ the $\mathbb{Q}$-algebra $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$. We suppose that k contains $\mathbb{F}_{p^2}$ and E is in an isogeny class such that $\mathrm{End}_k(E) = \mathrm{End}(E)$. In particular we may suppose that $k = \mathbb{F}_{p^2}$ and that E is in the isogeny class of an elliptic curve $E_0/\mathbb{F}_p$.

Orientations

Let $\mathfrak{B}$ be a quaternion algebra over $\mathbb{Q}$ ramified at p and ∞, K a quadratic imaginary field of discriminant Δ_K, $\mathcal{O}_K$ its maximal order and $\mathcal{O}$ an arbitrary order in $\mathcal{O}_K$. We recall that $\mathfrak{B}$ is unique up to isomorphism and if p is ramified or inert in $\mathcal{O}_K$ then K embeds in $\mathfrak{B}$. By hypothesis on E, there exists an isomorphism $\mathrm{End}^0(E) \cong \mathfrak{B}$.

Definition 2.1. A *K-orientation* on a supersingular elliptic curve E/k is a homomorphism $\iota : K \hookrightarrow \mathrm{End}^0(E)$. An *$\mathcal{O}$-orientation* on E is a K-orientation such that the image of the restriction of ι to $\mathcal{O}$ is contained in $\mathrm{End}(E)$. An $\mathcal{O}$-orientation is *primitive* if this restriction is an isomorphism with $\mathrm{End}(E) \cap \iota(K)$.

Let $\phi : E \to F$ be an isogeny of degree ℓ. A K-orientation $\iota : K \hookrightarrow \mathrm{End}^0(E)$ determines a K-orientation $\phi_*(\iota) : K \hookrightarrow \mathrm{End}^0(F)$ on F, defined by

$$\phi_*(\iota)(\alpha) = \frac{1}{\ell}\,\phi \circ \iota(\alpha) \circ \hat{\phi}.$$

Conversely, given K-oriented elliptic curves (E, ι_E) and (F, ι_F) we say that an isogeny $\phi : E \to F$ is K-oriented if $\phi_*(\iota_E) = \iota_F$, i.e. if the orientation on F is induced by ϕ.

If E admits a primitive $\mathcal{O}$-orientation by an order $\mathcal{O}$ in K, $\phi : E \to F$ is an isogeny then F admits an induced primitive $\mathcal{O}'$-orientation for an order $\mathcal{O}'$ satisfying

$$\mathbb{Z} + \ell\mathcal{O} \subseteq \mathcal{O}' \text{ and } \mathbb{Z} + \ell\mathcal{O}' \subseteq \mathcal{O}.$$

We say that an isogeny $\phi : E \to F$ is an $\mathcal{O}$-oriented isogeny if $\mathcal{O} = \mathcal{O}'$.

If ℓ is prime, as direct analogue of Proposition 4.2.3 of [19], one of the following holds:

- $\mathcal{O} = \mathcal{O}'$ and we say that φ is *horizontal*,
- $\mathcal{O} \subset \mathcal{O}'$ with index ℓ and we say that φ is *ascending*,
- $\mathcal{O}' \subset \mathcal{O}$ with index ℓ and we say that φ is *descending*.

Moreover if the discriminant of $\mathcal{O}$ is Δ, then there are exactly $\ell - \left(\frac{\Delta}{\ell}\right)$ descending isogenies. If $\mathcal{O}$ is maximal at ℓ, then there are $\left(\frac{\Delta}{\ell}\right) + 1$ horizontal isogenies, and if $\mathcal{O}$ is nonmaximal at ℓ, then there is exactly one ascending ℓ-isogeny and no horizontal isogenies.

Isogeny chains and ladders

Let E_0/k be a fixed supersingular elliptic curve, equipped with an $\mathcal{O}_K$-orientation, and let $\ell \neq p$ be a prime.

Definition 2.2. We define an *ℓ-isogeny chain* of length n from E_0 to E to be a sequence of isogenies of degree ℓ:

$$E_0 \xrightarrow{\phi_0} E_1 \xrightarrow{\phi_1} E_2 \xrightarrow{\phi_2} \dots \xrightarrow{\phi_{n-1}} E_n = E.$$

We say that the ℓ-isogeny chain is *without backtracking* if $\ker(\phi_{i+1} \circ \phi_i) \neq E_i[\ell]$ for each $i = 0, \dots, n-1$, and say that the isogeny chain is *descending* (or *ascending*, or *horizontal*) if each ϕ_i is descending (or ascending, or horizontal, respectively).

Remark. Since the dual isogeny of ϕ_i, up to isomorphism, is the only isogeny ϕ_{i+1} satisfying $\ker(\phi_{i+1} \circ \phi_i) = E_i[\ell]$, an isogeny chain is without backtracking if and only if the composition of two consecutive isogenies is cyclic. Moreover, we can extend this characterization in terms of cyclicity to the entire ℓ-isogeny chain.

Lemma 2.3. *The composition of the isogenies in an ℓ-isogeny chain is cyclic if and only if the ℓ-isogeny chain is without backtracking.*

Remark. If an isogeny ϕ is descending, then the unique ascending isogeny from $\phi(E)$, up to isomorphism, is the dual isogeny $\hat{\phi}$, satisfying $\hat{\phi}\phi = [\ell]$. As an immediate consequence, a descending ℓ-isogeny chain is automatically without backtracking, and an ℓ-isogeny chain without backtracking is descending if and only if ϕ_0 is descending.

Suppose that (E_i, ϕ_i) is an ℓ-isogeny chain, with E_0 equipped with an $\mathcal{O}_K$-orientation $\iota_0 : \mathcal{O}_K \to \mathrm{End}(E_0)$. For each i, let $\iota_i : K \to \mathrm{End}^0(E_i)$ be the induced K-orientation on E_i, and we note $\mathcal{O}_i = \mathrm{End}(E_i) \cap \iota_i(K)$ with $\mathcal{O}_0 = \mathcal{O}_K$. In particular, if (E_i, ϕ_i) is a descending ℓ-chain, then ι_i induces an isomorphism

$$\iota_i : \mathbb{Z} + \ell^i \mathcal{O}_K \longrightarrow \mathcal{O}_i.$$

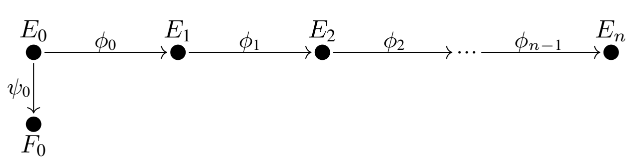
Let q be a prime different from p and ℓ that splits in $\mathcal{O}_K$, let $\mathfrak{q}$ be a fixed prime over q. For each i we set $\mathfrak{q}_i = \iota_i(\mathfrak{q}) \cap \mathcal{O}_i$, and define

$$C_i = E_i[\mathfrak{q}_i] = \{P \in E_i[q] \mid \psi(P) = 0 \text{ for all } \psi \in \mathfrak{q}_i\}.$$

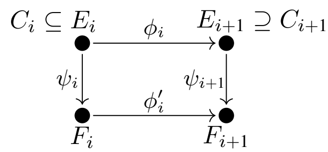
We define $F_i = E_i/C_i$, and let $\psi_i : E_i \to F_i$, an isogeny of degree q. By construction, it follows that $\phi_i(C_i) = C_{i+1}$ for all $i = 0, \dots, n-1$. In particular, if (E_i, ϕ_i) is a descending ℓ-ladder, then ι_i induces an isomorphism

$$\iota_i : \mathbb{Z} + \ell^i \mathcal{O}_K \longrightarrow \mathcal{O}_i.$$

The isogeny $\psi_0 : E_0 \to F_0 = E/C_0$ gives the following diagram of isogenies:

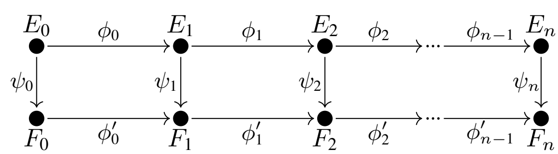


and for each $i = 0, \dots, n-1$ there exists a unique $\phi_i' : F_i \to F_{i+1}$ with kernel $\psi_i(\ker(\phi_i))$ such that the following diagram commutes:



This construction motivates the following definition.

Definition 2.4. An *ℓ-ladder* of length n and degree q is a commutative diagram of ℓ-isogeny chains (E_i, ϕ_i) and (F_i, ϕ'_i) of length n connected by q-isogenies $(\psi_i : E_i \to F_i)$:



We also refer to an ℓ-ladder of degree q as a *q-isogeny* of ℓ-isogeny chains, which we express as $\psi : (E_i, \phi_i) \to (F_i, \phi'_i)$.

We say that an ℓ-ladder is ascending (or descending, or horizontal) if the ℓ-isogeny chain (E_i, ϕ_i) is ascending (or descending, or horizontal, respectively). We say that the ℓ-ladder is *level* if ψ_0 is a horizontal q-isogeny. If the ℓ-ladder is descending (or ascending), then we refer to the length of the ladder as its *depth* (or, respectively, as its *height*).

Lemma 2.5. *An ℓ-ladder is level if and only if* $\mathrm{End}(E_i) = \mathrm{End}(F_i)$ *for all* $0 \le i \le n$*. In particular, if an ℓ-ladder $\psi : (E_i, \phi) \to (F_i, \phi'_i)$ is level, then (E_i, ϕ_i) is descending if and only if (F_i, ϕ'_i) is descending.*

3 Action of the class group

Let $\mathrm{SS}(p)$ denote the set of supersingular elliptic curves over $\overline{\mathbb{F}}_p$ up to isomorphism, and let $\mathrm{SS}_{\mathcal{O}}(p)$ the set of $\mathcal{O}$-oriented supersingular elliptic curves up to K-isomorphism over $\overline{\mathbb{F}}_p$, and denote the subset of primitive $\mathcal{O}$-oriented curves by $\mathrm{SS}^{pr}_{\mathcal{O}}(p)$. The set $\mathrm{SS}_{\mathcal{O}}(p)$ admits a transitive group action:

$$\begin{array}{rcl} \mathcal{C}\ell(\mathcal{O}) \times \mathrm{SS}_{\mathcal{O}}(p) & \longrightarrow & \mathrm{SS}_{\mathcal{O}}(p) \\ ([\mathfrak{a}], E) & \longmapsto & [\mathfrak{a}] \cdot E = E/E[\mathfrak{a}] \end{array}$$

where $\mathfrak{a}$ is any representative ideal coprime to the index $[\mathcal{O}_K : \mathcal{O}]$ so that the isogeny $E \to E/E[\mathfrak{a}]$ is horizontal. When restricted to primitive $\mathcal{O}$-oriented curves, we obtain the following classical result, extending the standard result for CM elliptic curves.

Proposition 3.1. *The class group $\mathcal{C}\ell(\mathcal{O})$ acts faithfully and transitively on the set of $\mathcal{O}$-isomorphism classes of primitive $\mathcal{O}$-oriented elliptic curves.*

In particular, for fixed primitive $\mathcal{O}$-oriented E, we hence obtain a bijection of sets:

$$\begin{array}{ccc} \mathcal{C}\ell(\mathcal{O}) & \longrightarrow & \mathrm{SS}_{\mathcal{O}}^{pr}(p) \\ [\mathfrak{a}] & \longmapsto & [\mathfrak{a}] \cdot E \end{array}$$

For any ideal class $[\mathfrak{a}]$ and generating set $\{\mathfrak{q}_1, \dots, \mathfrak{q}_r\}$ of small primes, coprime to $[\mathcal{O}_K : \mathcal{O}]$, we can find an identity $[\mathfrak{a}] = [\mathfrak{q}_1^{e_1} \cdot \ldots \cdot \mathfrak{q}_r^{e_r}]$, in order to compute the action via a sequence of low-degree isogenies.

Definition 3.2. We define a *vortex* to be an ℓ-isogeny subgraph whose vertices are isomorphism classes of $\mathcal{O}$-oriented elliptic curves with ℓ-maximal endomorphism ring, equipped with the action of $\mathcal{C}\ell(\mathcal{O})$.

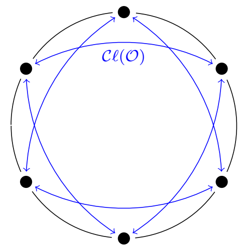


Figure 1. A *vortex* is an isogeny circle acted on and shuffled by $\mathcal{C}\ell(\mathcal{O})$.

Instead of considering the union of different isogeny graphs as in Couveignes [8] and Rostovtsev-Stolbunov [26], we focus on one single prime ℓ and we think of all the others as acting on the surface of the ℓ-isogeny graph: the resulting object is the union of ℓ-isogeny craters mixing under the action of $\mathcal{C}\ell(\mathcal{O})$.

We define a *whirlpool* to be a complete ℓ-isogeny graph of $\mathcal{O}$-oriented elliptic curves acted on by the class group.

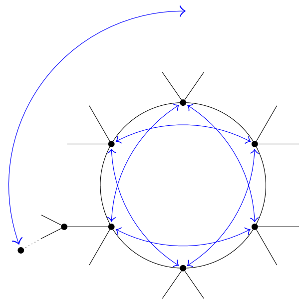


Figure 2. A *whirlphool* is an isogeny graph spinning under the action of $\mathcal{C}\ell(\mathcal{O})$.

The underlying graph of a whirlpool may be composed of several ℓ-isogeny orbits (craters), although the class group is transitive in any given isogeny class (Fig. 5). The existence of multiple ℓ-volcanoes is studied in [21] and [13] and the set of all these ℓ-volcanoes is called ℓ-cordillera. As an example, we can consider the set of elliptic curves $E/\mathbb{F}_{353}$ with 344 $\mathbb{F}_{353}$-rational points. We obtain two different 2-volcanoes.

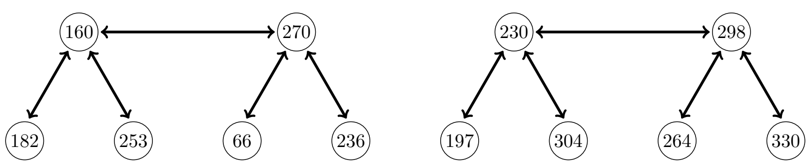


Figure 3. A 2-cordillera.

A whirlpool is the union of the two shuffled by the class group of $\mathbb{Z}[2\sqrt{-82}]$. In the following picture the blue lines indicate 7-isogenies while red lines correspond to 13-isogenies.

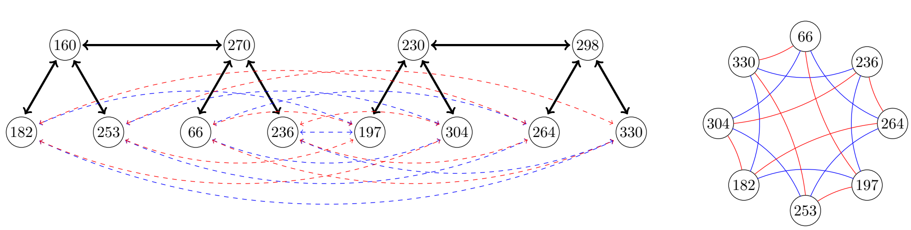


Figure 4. A whirlpool.

In conclusion, we define a whirlpool to be an ℓ-cordillera (black lines) acted on by the class group (represented by colored lines).

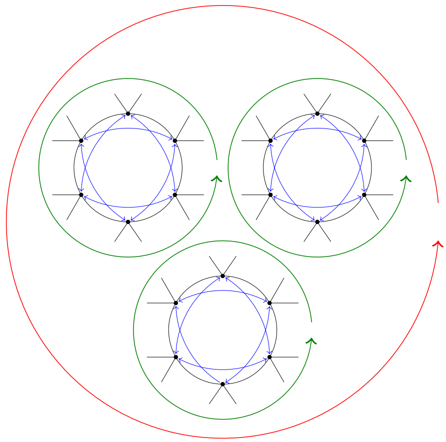


Figure 5. The isogeny graph may consists of different orbits.

4 Modular isogenies

In this section we consider the way in which we effectively represent and compute isogenies. With the view to oriented isogenies, we focus on horizontal isogenies with kernel $E[\mathfrak{q}]$, where E is a primitive $\mathcal{O}$-oriented elliptic curve and $\mathfrak{q}$ a prime ideal of $\iota(\mathcal{O})$. In what follows we suppress ι and identify $\mathcal{O}$ with $\iota(\mathcal{O})$.

Effective endomorphism rings and isogenies

We say a subring of $\mathrm{End}(E)$ is effective if we have explicit polynomial or rational functions which represent its generators. The subring $\mathbb{Z}$ in $\mathrm{End}(E)$ is thus effective. Examples of effective imaginary quadratic subrings $\mathcal{O} \subset \mathrm{End}(E)$, are the subring $\mathcal{O} = \mathbb{Z}[\pi]$ generated by Frobenius, for either an ordinary elliptic curve, or a supersingular elliptic curve defined over $\mathbb{F}_p$, or an elliptic curve obtained by CM construction for an order $\mathcal{O}$ of small discriminant (in absolute value).

In the Couveignes [8] or the Rostovtsev–Stolbunov [26] constructions, or in the CSIDH protocol [4], one works with the ring $\mathcal{O} = \mathbb{Z}[\pi]$. The disadvantage is that for large finite fields, the class group of $\mathcal{O}$ is large and the primes $\mathfrak{q}$ in $\mathcal{O}$ have no small generators. For large p (and small q), the smallest generator of a prime $\mathfrak{q}$ of norm q is the endomorphism $[q]$, of degree q^2. The division polynomial $\psi_q(x)$ which cuts out the torsion module $E[q]$ is of degree $(q^2-1)/2$, and factoring $\psi_q(x)$ to find the kernel polynomial (see Kohel [19, Chapter 2]) of degree $(q-1)/2$ for $E[\mathfrak{q}]$ is relatively expensive. As a consequence, in the SIDH protocol [18], the ordinary protocol of De Feo, Smith, and Kieffer [10], or the CSIDH protocol [4], the curves are chosen such that the points of $E[\mathfrak{q}]$ are defined over a small degree extension κ/k, particularly $[\kappa/k] \in \{1,2\}$, and working with rational points in $E(\kappa)$.

In the OSIDH protocol outlined below, we propose the use of an effective CM order $\mathcal{O}_K$ of class number 1. In particular every prime $\mathfrak{q}$ of norm q is generated by an endomorphism of the minimal degree q. For example we may take $\mathcal{O}_K$ to be the Eisenstein or Gaussian integers of discriminant -3 or -4, generated by an automorphism. The kernel polynomial of degree $(q-1)/2$ can be computed directly without need for a splitting field for $E[\mathfrak{q}]$, and the computation of a generator isogeny is a one-time precomputation.

Push forward isogenies

The extension of an endomorphism of E_0 to an ℓ-isogeny chain (E_i, ϕ_i) reduces to the construction of a ladder. At each step we are given $\phi_i : E_i \to E_{i+1}$ and $\psi_i : E_i \to F_i$ of coprime degrees, and need to compute

$$\psi_{i+1} : E_{i+1} \to F_{i+1} \text{ and } \phi_i' : F_i \to F_{i+1}.$$

Rather than working with elliptic curves and isogenies, we construct the oriented graphs directly as points on a modular curve linked by modular correspondences defined by modular polynomials.

Modular curves and isogenies

The use of modular curves for efficient computation of isogenies has an established history (see Elkies [12]). For this purpose we represent isogeny chains and ladders as finite sequences of points on the modular curve $\mathcal{X} = X(1)$ preserving the relations given by a modular equation.

We recall that the modular curve $X(1) \cong \mathbb{P}^1$ classifies elliptic curves up to isomorphism, and the function j generates its function field. The family of elliptic curves

$$E : y^2 + xy = x^3 - \frac{36}{(j-1728)}x - \frac{1}{(j-1728)}$$

covers all isomorphism classes $j \neq 0, 12^3$ or ∞, such that the fiber over $j_0 \in k$ is an elliptic curve of j-invariant j_0. The curves $y^2 + y = x^3$ and $y^2 = x^3 + x$ deal with the cases $j = 0$ and $j = 1728$.

The modular polynomial $\Phi_m(X, Y)$ defines a correspondence in $X(1) \times X(1)$ such that $\Phi_m(j(E), j(E')) = 0$ if and only if there exists a cyclic m-isogeny ϕ

from E to E', possibly over some extension field. The curve in $X(1) \times X(1)$ cut out by $\Phi_m(X,Y) = 0$ is a singular image of the modular curve $X_0(m)$ parametrizing such pairs (E, ϕ).

Remark. The modular curve $X(1)$ can be replaced by any genus 0 modular curve $\mathcal{X}$ parametrizing elliptic curves with level structure. Lifting the modular polynomials back to $\mathcal{X}$ of higher level (but still genus 0) has an advantage of reducing the size of the corresponding modular polynomials $\Phi_m(X,Y)$.

In the case of CSIDH, the authors use $\mathcal{X} = X_0(4)$, with a modular function $a \in k(X_0(4))$ to parametrize the family of curves

$$E : y^2 = x(x^2 + ax + 1),$$

together with a cyclic subgroup $C \subset E$ of order 4, whose generators are cut out by $x = 1$. The map $\mathcal{X} \to X(1)$ is given by

$$j = \frac{2^8(a^2-3)^3}{(a-2)(a+2)}.$$

The approach via modular isogenies methods of this section can be adapted as well to the CSIDH protocol.

Definition 4.1. A *modular ℓ-isogeny chain* of length n over k is a finite sequence $(j_0, j_1, \dots, j_n)$ in k such that $\Phi_\ell(j_i, j_{i+1}) = 0$ for $0 \le i < n$. A *modular ℓ-ladder* of length n and degree q over k is a pair of modular ℓ-isogeny chains

$$(j_0, j_1, \dots, j_n) \text{ and } (j'_0, j'_1, \dots, j'_n),$$

such that $\Phi_q(j_i, j'_i) = 0$.

Clearly an ℓ-isogeny chain (E_i, ϕ_i) determines the modular ℓ-isogeny chain $(j_i = j(E_i))$, but the converse is equally true.

Proposition 4.2. *If $(j_0, \dots, j_n)$ is a modular ℓ-isogeny chain over k, and E_0/k is an elliptic curve with $j(E_0) = j_0$, then there exists an ℓ-isogeny chain (E_i, ϕ_i) such that $j_i = j(E_i)$ for all $0 \le i \le n$.*

Given any modular ℓ-isogeny chain (j_i), elliptic curve E_0 with $j(E_0) = j_0$, and isogeny $\psi_0 : E_0 \to F_0$, it follows that we can construct an ℓ-ladder $\psi : (E_i, \phi_i) \to (F_i, \phi'_i)$ and hence a modular ℓ-isogeny ladder. In fact the ℓ-ladder can be efficiently constructed recursively from the modular ℓ-isogeny chain $(j_0, \dots, j_n)$ and $(j'_0, \dots, j'_i)$, by solving the system of equations

$$\Phi_\ell(j'_i, Y) = \Phi_q(j_{i+1}, Y) = 0,$$

for $Y = j'_{i+1}$. A computation of the polynomial gcd yields the generically unique solution.

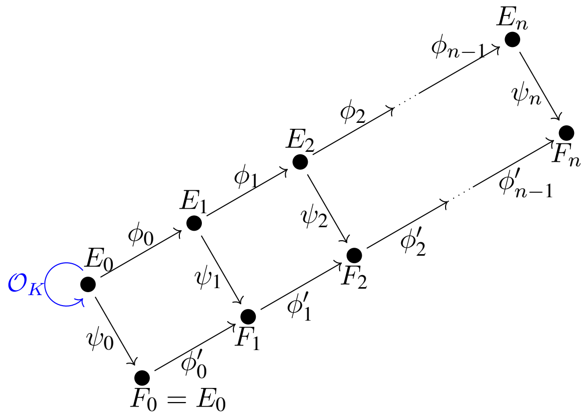
5 OSIDH

We consider an elliptic curve E_0/k ($k = \mathbb{F}_{p^2}$) with an $\mathcal{O}_K$-orientation by an effective ring $\mathcal{O}_K$ of class number 1, e.g. $j = 0$ or $j = 12^3$ (for which $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ or $\mathbb{Z}[i]$), small prime ℓ, and a descending ℓ-isogeny chain from E_0 to $E = E_n$. The $\mathcal{O}_K$-orientation on E_0 and ℓ-isogeny chain induces isomorphisms

$$\iota_i : \mathbb{Z} + \ell^i \mathcal{O}_K \to \mathcal{O}_i \subset \mathrm{End}(E_i),$$

and we set $\mathcal{O} = \mathcal{O}_n$. By hypothesis on E_0/k (the class number of $\mathcal{O}_K$ is 1), any horizontal isogeny $\psi_0 : E_0 \to F_0$ is, up to isomorphism $F_0 \cong E_0$, an endomorphism.

For a small prime q, we push forward a q-endomorphism $\phi_0 \in \mathrm{End}(E_0)$, to a q-isogeny $\psi : (E_i, \phi_i) \to (F_i, \phi_i')$.



By sending $\mathfrak{q} \subset \mathcal{O}_K$ to $\psi_0 : E_0 \to F_0 = E_0/E_0[\mathfrak{q}] \cong E_0$, and pushing forward to $\psi_n : E_n \to F_n$, we obtain the effective action of $\mathcal{C}\ell(\mathcal{O})$ on ℓ-isogeny chains of length n from E_0. In order to have the action of $\mathcal{C}\ell(\mathcal{O})$ cover a large portion of the supersingular elliptic curves, we require $\ell^n \sim p$, i.e., $n \sim \log_\ell(p)$.

Recall. The previous estimates are based on two very important results. Observe that the number of oriented elliptic curves that we can reach after n steps equals the class number $h(\mathcal{O}_n)$ of $\mathcal{O}_n = \mathbb{Z} + \ell^n \mathcal{O}_K$. It is well known [9, §7.D] that:

$$h(m\mathcal{O}_K) = \frac{h(\mathcal{O}_K)m}{[\mathcal{O}_K^\times : \mathcal{O}^\times]} \prod_{p \mid m} \left(1 - \left(\frac{\Delta_K}{p}\right)\frac{1}{p}\right) \tag{5.1}$$

where [7, VI.3]

$$\mathcal{O}_K^\times = \begin{cases} \{\pm 1\} & \text{if } \Delta_K < -4 \\ \{\pm 1, \pm i\} & \text{if } \Delta_K = -4 \\ \{\pm 1, \pm\zeta_3, \pm\zeta_3^2\} & \text{if } \Delta_K = -3 \end{cases} \Rightarrow \left[\mathcal{O}_K^\times : \mathcal{O}^\times\right] = \begin{cases} 1 & \text{if } \Delta_K < -4 \\ 2 & \text{if } \Delta_K = -4 \\ 3 & \text{if } \Delta_K = -3 \end{cases}$$

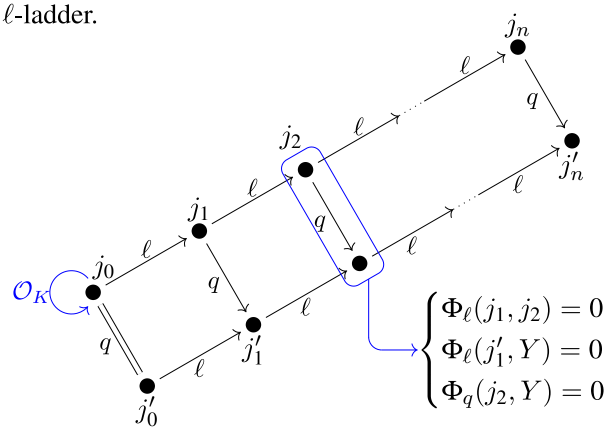
On the other hand, we know that the number of supersingular elliptic curves over $\mathbb{F}_{p^2}$ is given by the following formula [28, V.4]:

$$\#\mathrm{SS}(p) = \left\lfloor \frac{p}{12} \right\rfloor + \begin{cases} 0 & \text{if } p \equiv 1 \bmod 12 \\ 1 & \text{if } p \equiv 5, 7 \bmod 12 \\ 2 & \text{if } p \equiv 11 \bmod 12 \end{cases}$$

Therefore, in our case

$$h(\ell^n \mathcal{O}_K) = \frac{1 \cdot \ell^n}{2 \text{ or } 3}\left(1 - \left(\frac{\Delta_K}{\ell}\right)\frac{1}{\ell}\right) = \left\lfloor \frac{p}{12} \right\rfloor + \epsilon \implies p \sim \ell^n$$

To realise the class group action, it suffices to replace the above ℓ-ladder with its modular ℓ-ladder.

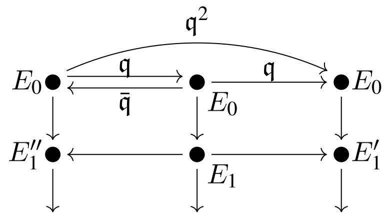


At the first index for which $j_i' = j(E_i/E_i[\mathfrak{q}_i])$ is distinguished from $j_i'' = j(E_i/E_i[\bar{\mathfrak{q}}_i])$, that is, $[\mathfrak{q}_i] \neq [\bar{\mathfrak{q}}_i]$ in $\mathcal{C}\ell(\mathcal{O}_i)$, we can solve iteratively for j_{i+1}' from j_i' and j_{i+1} using the equations:

$$\Phi_\ell(j_i', Y) = \Phi_q(j_{i+1}, Y) = 0.$$

The action of primes $\mathfrak{q}$ through $\mathcal{C}\ell(\mathcal{O})$ can be precomputed by its action on these initial segments which permits us to separate the action of $\mathfrak{q}$ and $\bar{\mathfrak{q}}$, hence assures a unique solution to the above system.

Remark. How many steps one can expect before $\mathfrak{q}$ and $\bar{\mathfrak{q}}$ act differently?



Thus, $E_i' \neq E_i''$ if and only if $\mathfrak{q}^2 \cap \mathcal{O}_i$ is not principal and the probability that a random ideal in $\mathcal{O}_i$ is principal is $1/h(\mathcal{O}_i)$. In fact, we can do better; we write $\mathcal{O}_K = \mathbb{Z}[\omega]$ and we observe that if $\mathfrak{q}^2$ was principal, then

$$q^2 = \mathrm{N}(\mathfrak{q}^2) = \mathrm{N}(a + b\ell^i\omega)$$

since it would be generated by an element of $\mathcal{O}_i = \mathbb{Z} + \ell^i\mathcal{O}_K$. Now

$$\mathrm{N}(a + b\ell^i) = a^2 \pm abt\ell^i + b^2 s\ell^{2i} \quad \text{where} \quad \omega^2 + t\omega + s = 0$$

Thus, as soon as $\ell^{2i} > q^2$ we are guaranteed that $\mathfrak{q}^2$ is not principal.

5.1 A first naive protocol

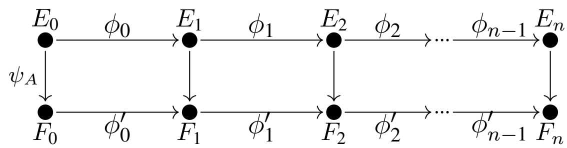
We now present the OSIDH cryptographic protocol based on this construction. We first describe a simplified version as intermediate step. The reason for doing that is twofold. On one hand it permits us to observe how the notions introduced so far lead to a cryptographic protocol, and on the other hand it highlights the critical security considerations and identifies the computationally hard problems on which the security is based.

As described at the beginning of the section, we fix a maximal order $\mathcal{O}_K$ in a quadratic imaginary field K of small discriminant Δ_K and a large prime p such that $\left(\frac{\Delta_K}{p}\right) \neq 1$. Further, the two parties agree on an elliptic curve E_0 with effective maximal order $\mathcal{O}_K$ embedded in the endomorphism ring and a descending ℓ-isogeny chain:

$$E_0 \longrightarrow E_1 \longrightarrow E_2 \longrightarrow \cdots \longrightarrow E_n.$$

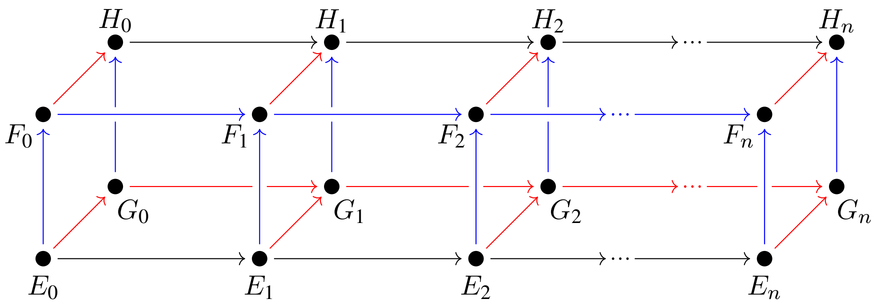
Recall. In practice, we will fix $\mathcal{O}_K$ to be either $\mathbb{Z}[i]$ or $\mathbb{Z}[\zeta_3]$.

Alice privately chooses a horizontal endomorphism $\psi_A = \psi_0 : E_0 \to F_0 = E_0$, and pushes it forward to an ℓ-ladder of length n:



The ℓ-isogeny chain (F_i) is sent to Bob, who choses an endomorphism ψ_B, and sends the resulting ℓ-isogeny chain (G_i) to Alice. Each applies the private endomorphism to obtain $(H_i) = \psi_B \cdot (F_i) = \psi_A \cdot (G_i)$, and $H = H_n$ is the shared secret.

In the following picture the blue arrows correspond to the orientation chosen throughout by Alice while the red ones represent the choice made by Bob.



PUBLIC DATA: A chain of ℓ-isogenies $E_0 \to E_1 \to \cdots \to E_n$		
	ALICE	**BOB**
Choose a smooth endomorphism of E_0 in $\mathcal{O}_K$	E_0 — F_0	E_0 — G_0
Push it forward to depth n	$\underbrace{F_0 \to F_1 \to \cdots \to F_n}_{\psi_A}$	$\underbrace{G_0 \to G_1 \to \cdots \to G_n}_{\psi_B}$
Exchange data	(G_i)	(F_i)
Compute shared secret	Compute $\psi_A \cdot (G_i)$	Compute $\psi_B \cdot (F_i)$
In the end, Alice and Bob share a new chain $E_0 \to H_1 \to \cdots \to H_n$		

This naive protocol presents a weak point: since E_0 is choosen in a very peculiar way, we know $\text{End}(E_0)$ and, at each step, we can also deduce

$$\mathbb{Z} + \ell\text{End}(E_i) \subset \text{End}(E_{i+1}) = \text{End}(F_{i+1})$$

Thus knowing $\mathbb{Z} + \ell^n\text{End}(E_0) \subset \text{End}(F_n)$, we can construct $\text{End}(F_n)$ and this gives us enough information to construct Alice's private key ψ_A.

Theorem 5.1 ([15, Theorem 4.1]). *Let E and E_A be supersingular elliptic curves over $\mathbb{F}_{p^2}$ such that $E[\ell^n] \subseteq E(\mathbb{F}_{p^2})$ and there is an isogeny $\psi_A : E \to E_A$ of* *degree ℓ^n. Suppose there is no isogeny $\phi : E \to E_A$ of degree strictly less than ℓ^n. Then, given an explicit description of* $\mathrm{End}(E)$ *and* $\mathrm{End}(E_A)$*, there is an efficient algorithm to compute ψ_A.*

We observe that there is another approach to this problem which uses only properties of the ideal class group. Suppose we have a K-descending ℓ-isogeny chain

$$E_0 \longrightarrow E_1 \longrightarrow \ldots \longrightarrow E_n$$

with

$$\mathrm{End}(E_0) \supsetneq \mathcal{O}_K = \mathcal{O}_0 \supseteq \mathcal{O}_1 \supseteq \ldots \supseteq \mathcal{O}_n \simeq \mathbb{Z} + \ell^n \mathcal{O}_K$$

This induces a sequence at the level of class groups

$$\begin{array}{ccccccccc} \mathcal{C}\ell(\mathcal{O}_n) & \longrightarrow & \cdots & \longrightarrow & \mathcal{C}\ell(\mathcal{O}_i) & \longrightarrow & \cdots & \longrightarrow & \mathcal{C}\ell(\mathcal{O}_K) \\ \wr\| & & & & \wr\| & & & & \wr\| \\ \frac{(\mathcal{O}_K/\ell^n\mathcal{O}_K)^\times}{\bar{\mathcal{O}}_K^\times(\mathbb{Z}/\ell^n\mathbb{Z})^\times} & \longrightarrow & \cdots & \longrightarrow & \frac{(\mathcal{O}_K/\ell^i\mathcal{O}_K)^\times}{\bar{\mathcal{O}}_K^\times(\mathbb{Z}/\ell^i\mathbb{Z})^\times} & \longrightarrow & \cdots & \longrightarrow & \{1\} \end{array}$$

In particular, there exists a surjection

$$\mathcal{C}\ell(\mathcal{O}_{i+1}) \simeq \frac{\left(\mathcal{O}_K/\ell^{i+1}\mathcal{O}_K\right)^\times}{\bar{\mathcal{O}}_K^\times\left(\mathbb{Z}/\ell^{i+1}\mathbb{Z}\right)^\times} \longrightarrow\!\!\!\!\!\!\rightarrow \frac{\left(\mathcal{O}_K/\ell^{i}\mathcal{O}_K\right)^\times}{\bar{\mathcal{O}}_K^\times\left(\mathbb{Z}/\ell^{i}\mathbb{Z}\right)^\times} \simeq \mathcal{C}\ell(\mathcal{O}_i)$$

whose kernel has an easy description. First of all we have to distinguish two different situations: the map $\psi : \mathcal{C}\ell(\mathcal{O}_1) \to \mathcal{C}\ell(\mathcal{O}_K)$ has kernel

$$\begin{cases} \mathbb{F}_{\ell^2}^\times/\mathbb{F}_\ell^\times & \text{of order } \ell+1 \quad \text{if } \ell \text{ is inert} \\ \left(\mathbb{F}_\ell^\times \times \mathbb{F}_\ell^\times\right)/\mathbb{F}_\ell^\times & \text{of order } \ell-1 \quad \text{if } \ell \text{ splits} \\ \left(\mathbb{F}_\ell\left[\xi\right]\right)^\times/\mathbb{F}_\ell^\times & \text{of order } \ell \quad \text{if } \ell \text{ is ramified} \end{cases}$$

where $\xi^2 = 0$. Roughly speaking, ψ is an intersection composed with a normalization; it is studied in [9, §7.D] and [22, §12]. Its kernel is the basis for a public key cryptosystem proposed in 1999 [16] [23] - NICE - and a signature scheme [17], both using non-maximal imaginary quadratic orders.

For $i > 1$, the surjection described above has cyclic kernel of order ℓ by virtue of the class number formula (5.1).

We notice that, at every step, our group is then growing by a factor ℓ; indeed, it is possible to prove that

$$\mathcal{C}\ell(\mathcal{O}_{i+1}) \simeq \mathcal{C}\ell(\mathcal{O}_i) \oplus \ker\left(\mathcal{C}\ell(\mathcal{O}_{i+1}) \twoheadrightarrow \mathcal{C}\ell(\mathcal{O}_i)\right)$$

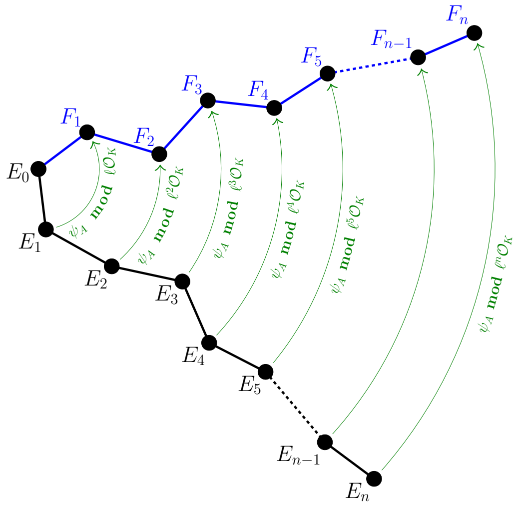


Figure 6. Construction of Alice's secret key

This means that if we have already constructed some representative for ψ_A modulo $\ell^i\mathcal{O}_K$, we can easily lift it and find ψ_A mod $\ell^{i+1}\mathcal{O}_K$.

In the end, it turns out that we only need to solve multiple instaces of the discrete logarithm problem in a group of order ℓ as in Pohlig-Hellman algorithm [24] and in the generalization of Teske [29].

Once a representative for ψ_A mod $\ell^n\mathcal{O}_K$ is known, we can search for an efficient (smooth) representative for ψ_A

$$\psi_A \equiv \psi_1^{n_1}\psi_2^{n_2} \cdot \ldots \cdot \psi_t^{n_t} \bmod \ell^n\mathcal{O}_K$$

with $\deg \psi_i = q_i$ small.

In conclusion, this first naïve protocol was found to be insecure. The problem is that we make the two parties share the knowledge of the entire chains (F_i) and (G_i). The question becomes: how can we avoid this while still giving the other party enough information?

5.2 The OSIDH protocol

We now detail how to send enough public data to compute the isogenies ψ_A and ψ_B on $G = G_n$ and $F = F_n$, respectively, without revealing the ℓ-isogeny chains (F_i) and (G_i). The setup remains the same with a public choice of $\mathcal{O}_K$-oriented elliptic curve E_0 and ℓ-isogeny chain

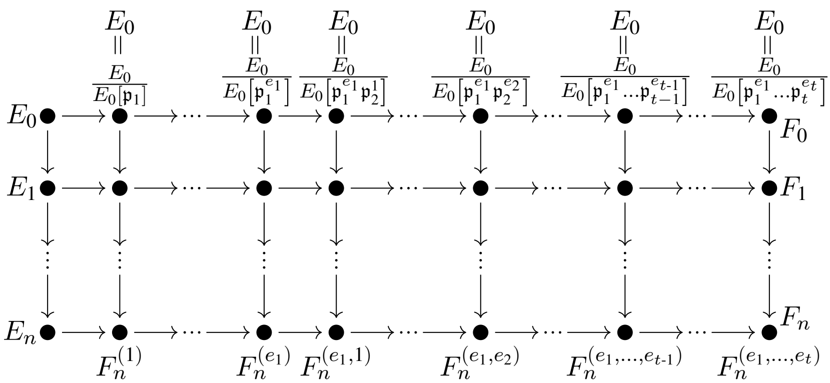
$$E_0 \to E_1 \to \cdots \to E_n.$$

Moreover, a set of primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ splitting in $\mathcal{O}_K$ is fixed.

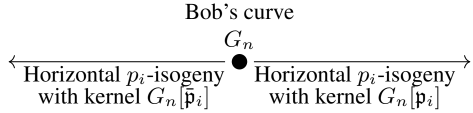
The first step consists of choosing the secret keys; these are represented by a sequence of integers $(e_1, \ldots, e_t)$ such that $|e_i| \leq r$. The bound r is taken so that the number $(2r+1)^t$ of curves that can be reached is sufficiently large. This choice of integers enables Alice to compute a new elliptic curve

$$F_n = \frac{E_n}{E_n\left[\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_t^{e_t}\right]}$$

by means of constructing the following commutative diagram



At this point the idea is to exchange curves F_n and G_n and to apply the same process again starting from the elliptic curve received from the other party. Unfortunately, this is not enough to get to the same final elliptic curve. Once Alice receives the unoriented curve G_n computed by Bob she also needs additional information for each prime $\mathfrak{p}_i$:



but she has no information as to which directions — out of $p_i + 1$ total p_i-isogenies — to take as $\mathfrak{p}_i$ and $\bar{\mathfrak{p}}_i$. For this reason, once that they have constructed their elliptic curves F_n and G_n, they precompute, for each prime $\mathfrak{p}_i$, the p_i-isogeny chains coming from $\bar{\mathfrak{p}}_i^j$ (denoted by the class $\mathfrak{p}_i^{-j}$) and $\mathfrak{p}_i^j$:

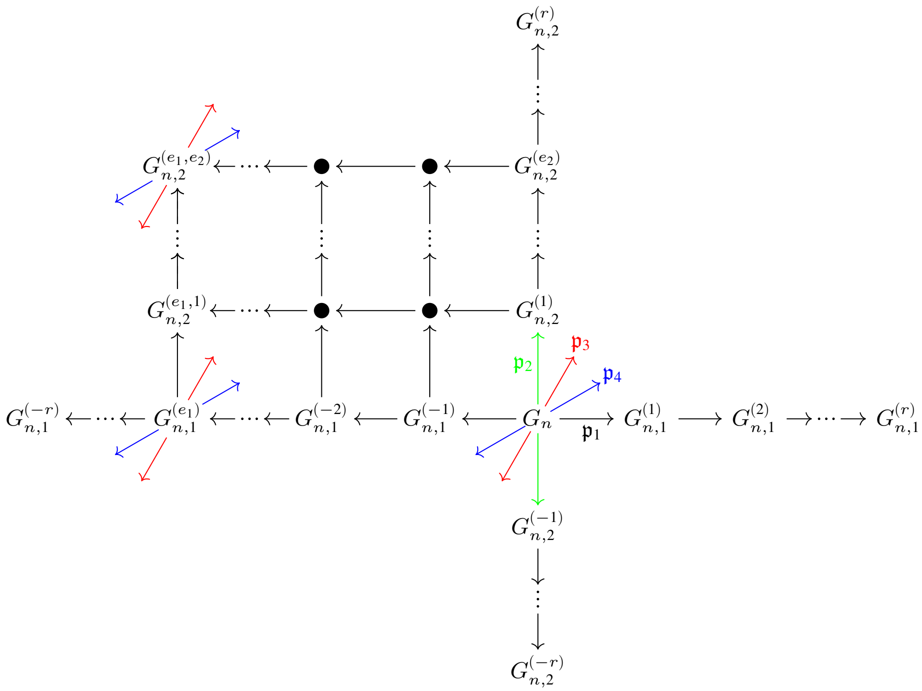
$$F_{n,i}^{(-r)} \leftarrow \cdots \leftarrow F_{n,i}^{(-1)} \leftarrow F_n \rightarrow F_{n,i}^{(1)} \rightarrow \cdots \rightarrow F_{n,i}^{(r-1)} \rightarrow F_{n,i}^{(r)},$$

and

$$G_{n,i}^{(-r)} \leftarrow \cdots \leftarrow G_{n,i}^{(-1)} \leftarrow G_n \rightarrow G_{n,i}^{(1)} \rightarrow \cdots \rightarrow G_{n,i}^{(r-1)} \rightarrow G_{n,i}^{(r)}.$$

Now Alice obtains from Bob the curve G_n and, for each i, the horizontal p_i-isogeny chains determined by the isogenies with kernels $G_n[\mathfrak{p}_i^j]$. With this information Alice can take e_1 steps in the $\mathfrak{p}_1$-isogeny chain and push forward all the $\mathfrak{p}_i$-isogeny chains for $i > 1$.

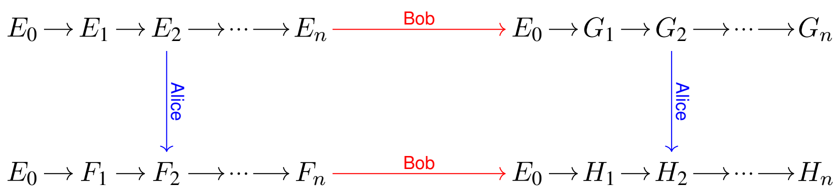
Remark. We recall that pushing forward means constructing a ladder which transmits all the information about the commutative action of $\mathfrak{p}_i^{e_i}$ in the class group.



Alice repeats the process for all the $\mathfrak{p}_i$'s every time pushing forward the isogenies for the primes with index strictly bigger than i. Finally, she obtains a new elliptic curve

$$H_n = \frac{E_n}{E_n\left[\mathfrak{p}_1^{e_1+d_1} \cdots \mathfrak{p}_t^{e_t+d_t}\right]}$$

Bob follows the same process with the public data received from Alice, in order to compute the same curve H_n. Recall that, in the naive protocol, Alice and Bob compute the group action on the full ℓ-isogeny chains:



In the refined OSIDH protocol, Alice and Bob share sufficient information to determine the curve H_n without knowledge of the other party's ℓ-isogeny chain (G_i) and (F_i), nor the full ℓ-isogeny chain (H_i) from the base curve E_0.

PUBLIC DATA: A chain of ℓ-isogenies $E_0 \to E_1 \to \cdots \to E_n$ and a set of splitting primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_t \subseteq \mathcal{O} = \mathrm{End}(E_n) \cap K \hookrightarrow \mathcal{O}_K$

	ALICE	**BOB**
Choose integers in an interval $[-r, r]$	$(e_1, \ldots, e_t)$	$(d_1, \ldots, d_t)$
Construct an isogenous curve	$F_n = \dfrac{E_n}{E_n[\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_t^{e_t}]}$	$G_n = \dfrac{E_n}{E_n[\mathfrak{p}_1^{d_1} \cdots \mathfrak{p}_t^{d_t}]}$
Precompute all directions $\forall\, i$	$F_n \to F_{n,i}^{(1)} \to \cdots \to F_{n,1}^{(r)}$	$G_n \to G_{n,i}^{(1)} \to \cdots \to G_{n,1}^{(r)}$
... and their conjugates	$F_{n,i}^{(-r)} \leftarrow \cdots \leftarrow F_{n,i}^{(-1)} \leftarrow F_n$	$G_{n,i}^{(-r)} \leftarrow \cdots \leftarrow G_{n,i}^{(-1)} \leftarrow G_n$
Exchange data	G_n+directions	F_n+directions
Compute shared data	Takes e_i steps in $\mathfrak{p}_i$-isogeny chain & push forward information for all $j > i$.	Takes d_i steps in $\mathfrak{p}_i$-isogeny chain & push forward information for all $j > i$.

In the end, both Alice and Bob share the same elliptic curve

$$H_n = \frac{F_n}{F_n[\mathfrak{p}_1^{d_1} \cdots \mathfrak{p}_t^{d_t}]} = \frac{G_n}{G_n[\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_t^{e_t}]} = \frac{E_n}{E_n[\mathfrak{p}_1^{e_1+d_1} \cdots \mathfrak{p}_t^{e_t+d_t}]}.$$

Remark. We can read this scheme using the terminology of section 3.

After the choice of the secret key, we observe a vortex: Alice (respectively Bob) acts on an isogeny crater (that in the case of $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ or $\mathbb{Z}[i]$ consists of a single points) with the primes $\mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_t^{e_t}$ (respectively $\mathfrak{q}_1^{d_1} \cdot \ldots \cdot \mathfrak{q}_t^{d_t}$).

This action is eventually transmitted along the ℓ-isogeny chain and we get a whirlphool. We can think of the isogeny volcano as rotating under the action

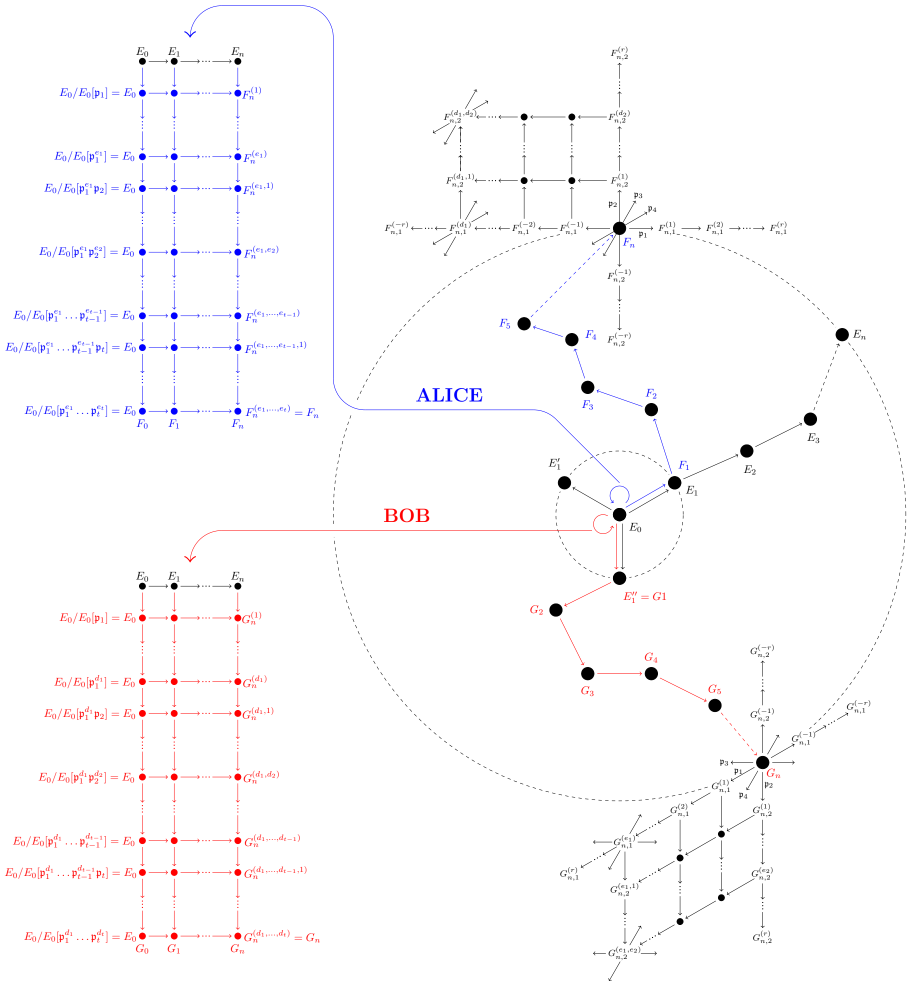


Figure 7. Graphic representation of OSIDH

of the secret keys and the initial ℓ-isogeny path transforming into the two secret isogeny chains.

6 Conclusion

By imposing the data of an orientation by an imaginary quadratic ring $\mathcal{O}$, we obtain an augmented category of supersingular curves on which the class group $\mathcal{C}\ell(\mathcal{O})$ acts faithfully and transitively. This idea is already implicit in the CSIDH protocol, in which supersingular curves over $\mathbb{F}_p$ are oriented by the Frobenius subring $\mathbb{Z}[\pi] \cong \mathbb{Z}[\sqrt{-p}]$. In contrast we consider an elliptic curve E_0 oriented by a CM order $\mathcal{O}_K$ of class number one. To obtain a nontrivial group action, we consider ℓ-isogeny chains, on which the class group of an order $\mathcal{O}$ of large index ℓ^n in $\mathcal{O}_K$ acts, a structure we call a whirlpool. The map from ℓ-isogeny chains to its terminus forgets the structure of the orientation, and the original base curve E_0, giving rise to a generic supersingular elliptic curve. Within this general framework we define a new oriented supersingular isogeny Diffie-Hellman (OSIDH) protocol, which has fewer restrictions on the proportion of supersingular curves covered and on the torsion group structure of the underlying curves. Moreover, the group action can be carried out effectively solely on the sequences of moduli points (such as j-invariants) on a modular curve, thereby avoiding expensive isogeny computations, and is further amenable to speedup by precomputations of endomorphisms on the base curve E_0.

Bibliography

[1] J.F. Biasse, D. Jao and A. Sankar. A quantum algorithm for computing isogenies between supersingular elliptic curves, In *International Conference in Cryptology in India*, Springer, 428-442, 2014.

[2] A. Bostan, F. Morain, B. Salvy and É. Schost. Fast algorithms for computing isogenies between elliptic curves, In *Mathematics of Computation*, vol. **77**, 1755-1778, 2008.

[3] R. Bröker, D. Charles and K. Lauter. Evaluating Large Degree Isogenies and Applications to Pairing Based Cryptography, In *Galbraith, S.D., Paterson, K.G. (eds.) Pairing 2008. LNCS*, vol. **5209**, 100âĂŞ112. Springer, Heidelberg, 2008.

[4] W. Castryck, T. Lange, C. Martindale, L. Panny, and J. Renes. CSIDH: an efficient post-quantum commutative group action, In *Advances in Cryptology - ASIACRYPT 2018.*, Lecture Notes in Computer Science, vol **11274** Springer, 2018.

[5] D. Charles, E. Goren, and C. Lauter. Cryptographic hash functions from expander graphs, *J. Cryptography* **22** (1), 93–113, 2009.

[6] A. Childs, D. Jao, and V. Soukharev. Constructing elliptic curve isogenies in quantum subexponential time, In *Journal of Mathematical Cryptology*, vol **8**(1), 1–29, 2014.

[7] H. Cohn. Advanced Number Theory, Courier Corporation, 1980.

[8] J.M. Couveignes. Hard Homogeneous Spaces, In *IACR Cryptology ePrint Archive 2006/291*, 2006. `https://eprint.iacr.org/2006/291`.

[9] D.A. Cox. Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication, In *Pure and applied mathematics*, Wiley, 1997.

[10] L. De Feo, J. Kieffer, and B. Smith. Towards practical key exchange from ordinary isogeny graphs, In *Advances in Cryptology - ASIACRYPT 2018.*, Lecture Notes in Computer Science, vol **11274** Springer, 2018.

[11] K. Eisenträger, S. Hallgren, K. Lauter, T. Morrison, and C. Petit. Supersingular Isogeny Graphs and Endomorphism Rings: Reductions and Solutions, In *Advances in Cryptology - EUROCRYPT 2018*. Ed. by Jesper Buus Nielsen and Vincent Rijmen. Springer International Publishing, 2018, 329-368.

[12] N.D. Elkies. Elliptic and modular curves over finite fields and related computational issues, In *Computational Perspectives in Number Theory: Conference in Honor of A. O. L. Atkin*, D. A. Buell and J. T. Teitelbaum, eds., American Mathematical Society (1998), 21–76.

[13] M. Fouquet and F. Morain. Isogeny Volcanoes and the SEA Algorithm, In *C. Fieker and D.R. Kohel (eds) Algorithmic Number Theory. ANTS 2002*, Lecture Notes in Computer Science, vol **2369** (2002). Springer, Berlin, Heidelberg.

[14] S.D. Galbraith. Constructing isogenies between elliptic curves over finite fields, *LMS Journal of Computation and Mathematics*, vol. **2** (1999), 118-138.

[15] S.D. Galbraith, C. Petit, B. Shani and Y.B. Ti. On the Security of Supersingular Isogeny Cryptosystems, In *ASIACRYPT (1)*, Springer, 63-91, 2016. `https://eprint.iacr.org/2016/859`.

[16] M. Hartmann, S. Paulus, T. Takagi. NICE - New Ideal Coset Encryption. In *CHES 1999*. Springer, 1999.

[17] D. Hühnlein, J. Merkle. An efficient NICE-Schnorr-type signature scheme. In *PKC 2000*, LNCS **1751**, 14–27, Springer, 2000.

[18] D. Jao and L. De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies, In *Post-Quantum Cryptography*, LNCS **7071**, 19–34, Springer, 2011. `https://eprint.iacr.org/2011/506`.

[19] D. Kohel. *Endomorphism rings of elliptic curves over finite fields*, Ph.D. thesis, U.C. Berkeley, 1996.

[20] G. Kuperberg. A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. In *SIAM Journal of Computing*, vol. **35**(1), 170âĂŞ-188 (2005).

[21] J. Miret, D. Sadornil, J. Tena, R. Tomàs and M. Valls Isogeny cordillera algorithm to obtain cryptographically good elliptic curves, In *ACSW Frontiers 2007*, Conferences in Research and Practice in Information Technology **68**, pp. 127–131, 2007.

[22] J. Neukirch. Algebraische Zahlentheorie, In *Masterclass*, Springer Berlin Heidelberg, 1992.

[23] S. Paulus, T. Takagi. A New Public-Key Cryptosystem over a Quadratic Order with Quadratic Decryption Time, In *Journal of Cryptology* vol. **13**, 263–272, Springer, 2000. `http://dx.doi.org/10.1007/s001459910010`.

[24] S.C. Pohlig, M.E. Hellman. An improved algorithm for computing logarithms over GF(p) and its cryptographic significance, In *IEEE-Transactions on Information Theory* vol. **24**, 106–110, 1978.

[25] O. Regev. A subexponential time algorithm for the dihedral hidden subgroup problem with polynomial space. arXiv:quant-ph/0406151, June 2004. `http://arxiv.org/abs/quant-ph/0406151`.

[26] A. Rostovtsev and A. Stolbunov. Public-key cryptosystem based on isogenies, In *IACR Cryptology ePrint Archive 2006/145*, 2006. `https://eprint.iacr.org/2006/145`.

[27] R. Schoof. Quadratic fields and factorization, In *Computation Methods in Number Theory*, Math. Centrum Tract 154, 235–286, Amsterdam, 1982.

[28] J.H. Silverman. The Arithmetic of Elliptic Curves, Springer-Verlag, 1986.

[29] E. Teske. The Pohlig-Hellman method generalized for group structure computation, In *Journal of symbolic computation*, vol. **11**, 1–14, 1999.

Received **???**.

Author information

Leonardo Colò, Aix Marseille Univ, CNRS, Centrale Marseille, I2M, Marseille, France.
E-mail: `leonardo.colo@univ-amu.fr`

David Kohel, Aix Marseille Univ, CNRS, Centrale Marseille, I2M, Marseille, France.
E-mail: `david.kohel@univ-amu.fr`