

TOULON, 09 MARCH 2021

ORIENTING SUPERSINGULAR ISOGENY GRAPHS

LEONARDO COLÒ & DAVID KOHEL

Institut de Mathématiques de Marseille

Definition

Let k be a field of characteristic $\neq 2, 3$. An elliptic curve E defined over k is a smooth projective curve of genus 1 defined by a Weierstrass equation

$$E : Y^2 Z = X^3 + aXZ^2 + bZ^3$$

where $a, b \in k$ are such that $4a^3 + 27b^2 \neq 0$.

In general we work with the affine equation of E , i.e., $E : y^2 = x^3 + ax + b$.

We distinguish the point $O = (0 : 1 : 0)$ (called *point at infinity*).

There is a way of adding points on E based on Bezout's theorem (we fix the point O and we define the sum of three co-linear points to be O). This law endows the set of k -rational points with a group structure where O plays the role of identity element. We write $E(k)$.

Isomorphisms

An isomorphism of elliptic curves is an invertible morphism of algebraic curves (*admissible linear change of variables*). They are of the form

$$(x, y) \rightarrow (u^2x, u^3y) \quad \text{for some } u \in \bar{k}.$$

Isomorphisms between elliptic curves are group isomorphisms.

Isomorphism classes are described by an invariant:

j -invariant

The j -invariant of an elliptic curve $E : y^2 = x^3 + ax + b$ is

$$j(E) = 1728 \frac{4a^3}{4a^3 + 27b^2}$$

Two elliptic curves E, E' are isomorphic over \bar{k} if and only if $j(E) = j(E')$.

Let E be an elliptic curve defined over a field k and m an integer. The m -torsion subgroup of E is

$$E[m] = \{P \in E(\bar{k}) \mid mP = O\}$$

Torsion structure

Let E be an elliptic curve defined over an algebraic closed field \bar{k} of characteristic p . If p does not divide m or $p = 0$, then

$$E[m] \simeq \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}$$

If the $p > 0$, then

$$E[p^r] \simeq \begin{cases} \frac{\mathbb{Z}}{p^r\mathbb{Z}} & \text{Ordinary case} \\ \{O\} & \text{Supersingular case} \end{cases}$$

They are relationships between isomorphisms classes of elliptic curves.

Isogenies

An isogeny $\phi : E \rightarrow E'$ between two elliptic curves is

- ▶ A map $E \rightarrow E'$ such that $\phi(P + Q) = \phi(P) + \phi(Q)$.
- ▶ A surjective group morphisms (in the algebraic closure).
- ▶ A group morphism with finite kernel.
- ▶ A non-constant algebraic map of projective varieties such that $\phi(O_E) = O_{E'}$.
- ▶ An algebraic morphism given by rational maps

$$\phi(x, y) = \left(\frac{f_1(x, y)}{g_1(x, y)}, \frac{f_2(x, y)}{g_2(x, y)} \right)$$

The first example of isogeny is the multiplication by n map: $[n] : E \rightarrow E$.
If $k = \mathbb{F}_q$ we also have the Frobenius morphism $\pi : (x, y) \rightarrow (x^q, y^q)$.

Let $\phi : E \rightarrow E'$ be an isogeny defined over a field k , $\text{char}(k) = p$.

Definitions

- ▶ The degree of ϕ is defined to be $\mathbf{deg} \phi = [k(E) : \phi^*k(E')]$.
- ▶ ϕ is said separable, inseparable or purely inseparable if the corresponding extension of function fields is.
- ▶ If ϕ is separable then $\mathbf{deg} \phi = \#\ker \phi$.
- ▶ Given any isogeny $\phi : E \rightarrow E'$ there always exists a unique isogeny $\hat{\phi} : E' \rightarrow E$, called the *dual isogeny*, such that

$$\phi \circ \hat{\phi} = [\mathbf{deg} \phi]_{E'} \quad \hat{\phi} \circ \phi = [\mathbf{deg} \phi]_E$$

Theorem

For every finite subgroup $G \subset E(\bar{k})$, there exist a unique (up to isomorphism) elliptic curve $E' = E/G$ and a unique separable isogeny $E \rightarrow E'$ of degree $\#G$. Further, any separable isogeny arises in this way.

Given G , Velu's formulæ enables one to find explicit description for ϕ .

Theorem (Tate)

Two elliptic curves E and E' defined over a finite field k are isogenous over k if and only if $\#E(k) = \#E'(k)$.

Observe that there exists an algorithm (Schoof - 1985) which, using isogenies, compute the cardinality of E in polynomial time.

An endomorphism of an elliptic curve E is an isogeny from E to itself.

Endomorphism ring

The endomorphism ring $\mathbf{End}(E) = \mathbf{End}_{\bar{k}}(E)$ of an elliptic curve E/k is the set of all endomorphisms of E (together with the 0-map) endowed with sum and multiplication

The endomorphism ring always contains a copy of \mathbb{Z} in the form of the multiplication by m maps.

If k is a finite field we also have the Frobenius endomorphism.

Let E be an elliptic curve defined over a finite field k . $\text{End}(E)$ has dimension either 2 or 4 as a \mathbb{Z} -module.

Theorem (Deuring)

Let E/k be an elliptic curve over a finite field k of characteristic $p > 0$. $\text{End}(E)$ is isomorphic to one of the following:

- ▶ An order \mathcal{O} in a quadratic imaginary field; we say that E is ordinary.
- ▶ A maximal order in a quaternion algebra; we say that E is supersingular.

Isogenous curves are always either both ordinary, or both supersingular.

Theorem (Serre-Tate)

Two elliptic curves E_0 and E_1 defined over a finite field k are isogenous if and only if $\text{End}(E_0) \otimes_{\mathbb{Z}} \mathbb{Q} \simeq \text{End}(E_1) \otimes_{\mathbb{Z}} \mathbb{Q}$.

Definition

Given an elliptic curve E over k , and a finite set of primes S , we can associate an isogeny graph $\Gamma = (E, S)$

- ▶ whose vertices are elliptic curves isogenous to E over \bar{k} , and
- ▶ whose edges are isogenies of degree $\ell \in S$.

The vertices are defined up to \bar{k} -isomorphism (therefore represented by j -invariants), and the edges from a given vertex are defined up to a \bar{k} -isomorphism of the codomain.

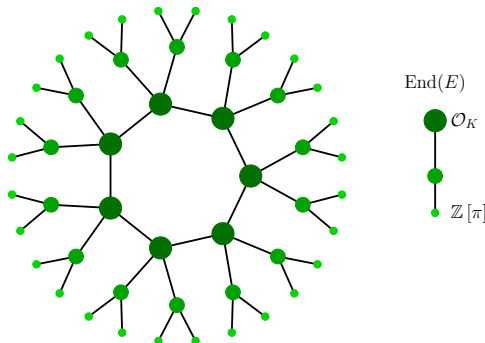
If $S = \{\ell\}$, then we call Γ an ℓ -isogeny graph.

The ℓ -isogeny graph of E is $(\ell + 1)$ -regular (as a directed multigraph). In characteristic 0, if $\text{End}(E) = \mathbb{Z}$, then this graph is a tree.

Let $\text{End}(E) = \mathcal{O} \subseteq K$. The class group $\text{Cl}(\mathcal{O})$ acts faithfully and transitively on the set of elliptic curves with endomorphism ring \mathcal{O} :

$$E \longrightarrow E/E[\mathfrak{a}] \quad E[\mathfrak{a}] = \{P \in E \mid \alpha(P) = 0 \ \forall \alpha \in \mathfrak{a}\}$$

Thus, the CM isogeny graphs can be modelled by an equivalent category of fractional ideals of K .

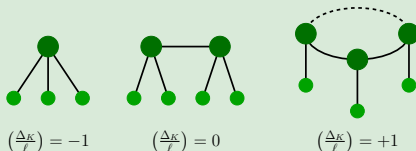


Let E and E' be two elliptic curves with endomorphism rings \mathcal{O} and \mathcal{O}' respectively and let $\phi : E \rightarrow E'$ be an ℓ isogeny.

- ▶ If $\mathcal{O} = \mathcal{O}'$ we say that ϕ is horizontal;
- ▶ If $[\mathcal{O}' : \mathcal{O}] = \ell$ we say that ϕ is ascending;
- ▶ If $[\mathcal{O} : \mathcal{O}'] = \ell$ we say that ϕ is descending.

Crater

The crater consists of $h(\mathcal{O}_K) = \#\mathcal{C}(\mathcal{O}_K)$ Elliptic curves. Depending on the behavior of ℓ in \mathcal{O}_K we can have one or multiple craters:



The height of the volcano is $\nu_\ell([\mathcal{O}_K : \mathbb{Z}[\pi]])$.

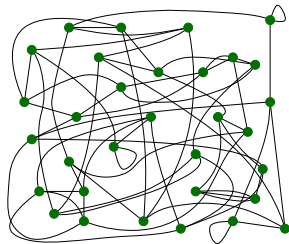
The supersingular isogeny graphs are remarkable because the vertex sets are finite : there are $(p + 1)/12 + \epsilon_p$ curves. Moreover

- ▶ every supersingular elliptic curve can be defined over \mathbb{F}_{p^2} ;
- ▶ all ℓ -isogenies are defined over \mathbb{F}_{p^2} ;
- ▶ every endomorphism of E is defined over \mathbb{F}_{p^2} .

The lack of a commutative group acting on the set of supersingular elliptic curves/ \mathbb{F}_{p^2} makes the isogeny graph more complicated.

For this reason, supersingular isogeny graphs have been proposed for

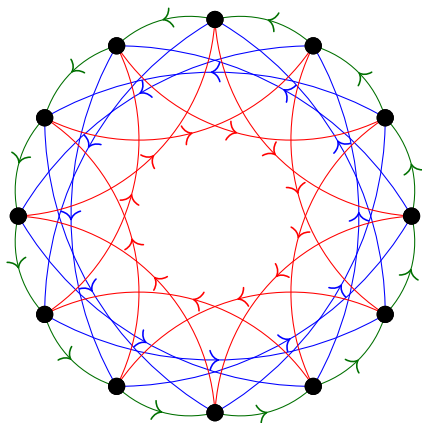
- ▶ cryptographic hash functions (Goren–Lauter),
- ▶ post-quantum SIDH key exchange protocol.



Fix a large enough finite field \mathbb{F}_q of large characteristic p and an ordinary elliptic curve E_0/\mathbb{F}_q such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

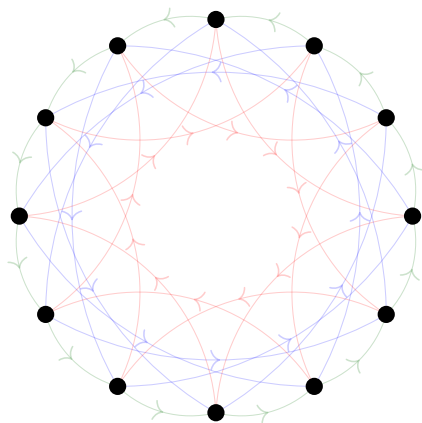
$$\mathcal{L} = \{\ell_1, \ell_2, \ell_3\}$$



Fix a large enough finite field \mathbb{F}_q of large characteristic p and an ordinary elliptic curve E_0/\mathbb{F}_q such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

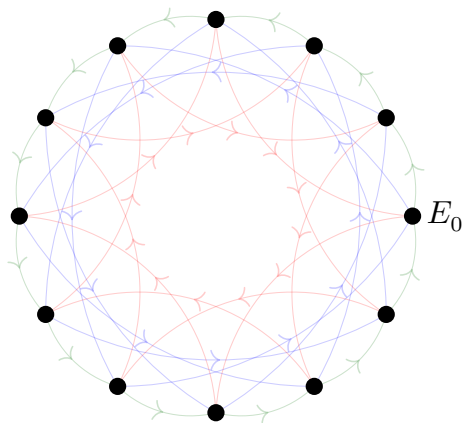
$$\mathcal{L} = \{\ell_1, \ell_2, \ell_3\}$$



Fix a large enough finite field \mathbb{F}_q of large characteristic p and an ordinary elliptic curve E_0/\mathbb{F}_q such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$$\mathcal{L} = \{\ell_1, \ell_2, \ell_3\}$$



Fix a large enough finite field \mathbb{F}_q of large characteristic p and an ordinary elliptic curve E_0/\mathbb{F}_q such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

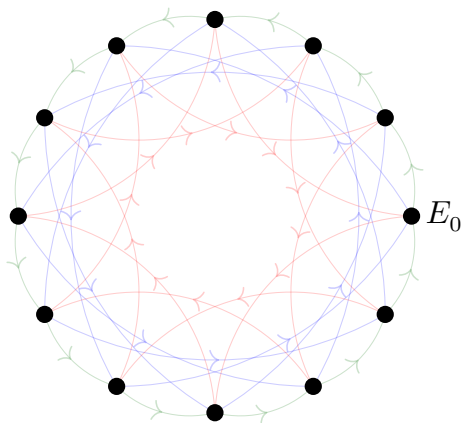
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$$\mathcal{L} = \{\ell_1, \ell_2, \ell_3\}$$

Alice

$$\rho_A = (2, 1, -1)$$

$$\mathfrak{a} = \ell_1^2 \ell_2 \ell_3^{-1}$$



Fix a large enough finite field \mathbb{F}_q of large characteristic p and an ordinary elliptic curve E_0/\mathbb{F}_q such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

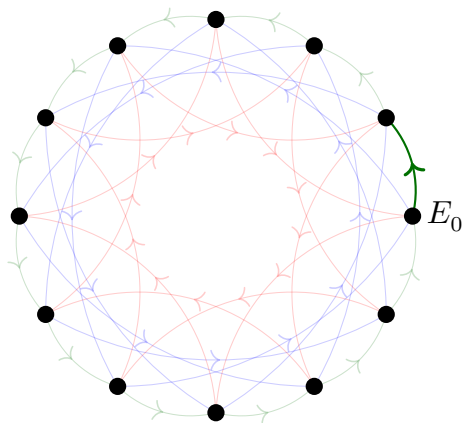
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$$\mathcal{L} = \{\ell_1, \ell_2, \ell_3\}$$

Alice

$$\rho_A = (2, 1, -1)$$

$$\mathfrak{a} = \ell_1^2 \ell_2 \ell_3^{-1}$$



Fix a large enough finite field \mathbb{F}_q of large characteristic p and an ordinary elliptic curve E_0/\mathbb{F}_q such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

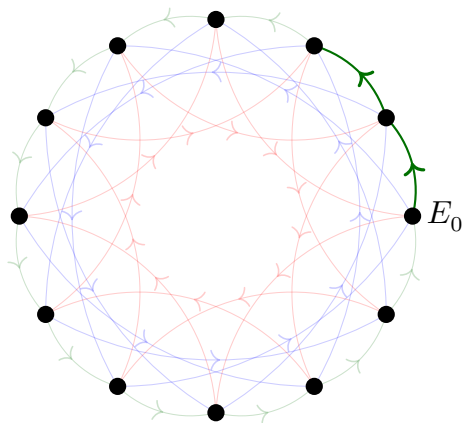
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$$\mathcal{L} = \{\ell_1, \ell_2, \ell_3\}$$

Alice

$$\rho_A = (2, 1, -1)$$

$$\mathfrak{a} = \ell_1^2 \ell_2 \ell_3^{-1}$$



Fix a large enough finite field \mathbb{F}_q of large characteristic p and an ordinary elliptic curve E_0/\mathbb{F}_q such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

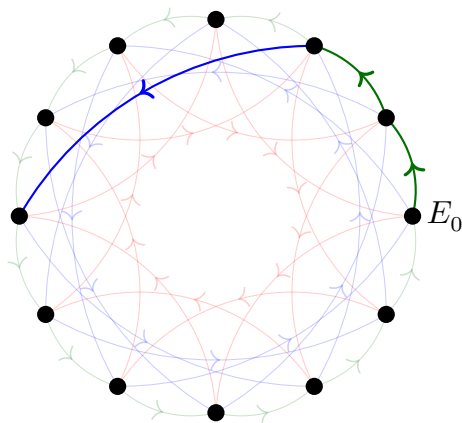
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$$\mathcal{L} = \{\ell_1, \ell_2, \ell_3\}$$

Alice

$$\rho_A = (2, 1, -1)$$

$$\mathfrak{a} = \ell_1^2 \ell_2 \ell_3^{-1}$$



Fix a large enough finite field \mathbb{F}_q of large characteristic p and an ordinary elliptic curve E_0/\mathbb{F}_q such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

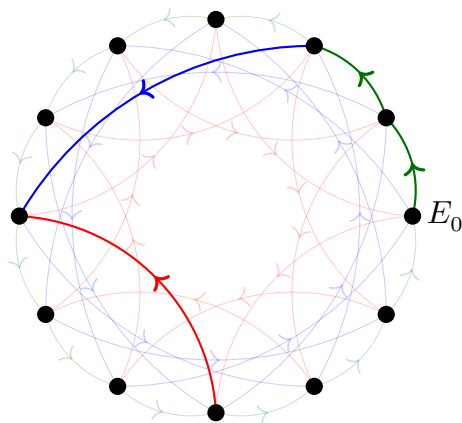
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$$\mathcal{L} = \{\ell_1, \ell_2, \ell_3\}$$

Alice

$$\rho_A = (2, 1, -1)$$

$$\mathfrak{a} = \ell_1^2 \ell_2 \ell_3^{-1}$$



Fix a large enough finite field \mathbb{F}_q of large characteristic p and an ordinary elliptic curve E_0/\mathbb{F}_q such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

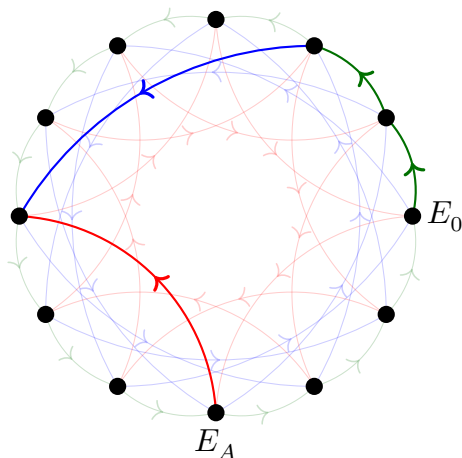
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$$\mathcal{L} = \{\ell_1, \ell_2, \ell_3\}$$

Alice

$$\rho_A = (2, 1, -1)$$

$$\mathfrak{a} = \ell_1^2 \ell_2 \ell_3^{-1}$$



Fix a large enough finite field \mathbb{F}_q of large characteristic p and an ordinary elliptic curve E_0/\mathbb{F}_q such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

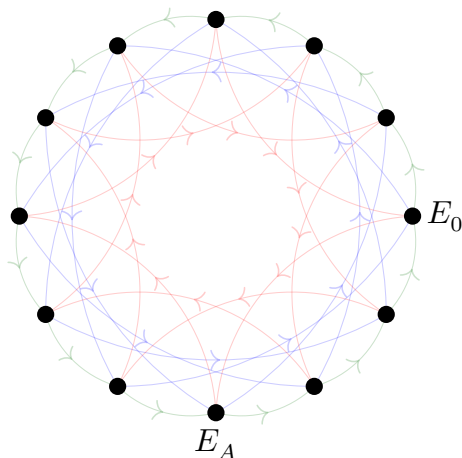
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$$\mathcal{L} = \{\ell_1, \ell_2, \ell_3\}$$

Alice

$$\rho_A = (2, 1, -1)$$

$$\mathfrak{a} = \ell_1^2 \ell_2 \ell_3^{-1}$$



Bob

$$\rho_B = (-2, 0, 1)$$

$$\mathfrak{a} = \ell_1^{-2} \ell_3$$

Fix a large enough finite field \mathbb{F}_q of large characteristic p and an ordinary elliptic curve E_0/\mathbb{F}_q such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

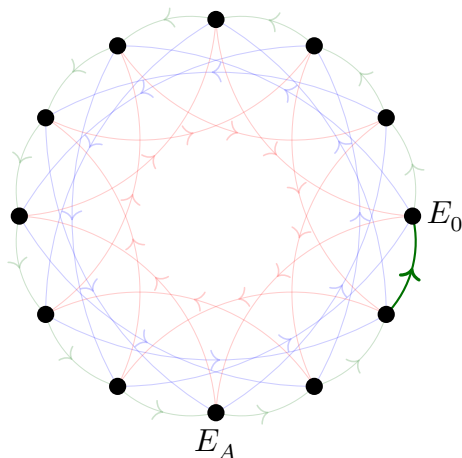
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$$\mathcal{L} = \{\ell_1, \ell_2, \ell_3\}$$

Alice

$$\rho_A = (2, 1, -1)$$

$$\mathfrak{a} = \ell_1^2 \ell_2 \ell_3^{-1}$$



Bob

$$\rho_B = (-2, 0, 1)$$

$$\mathfrak{a} = \ell_1^{-2} \ell_3$$

Fix a large enough finite field \mathbb{F}_q of large characteristic p and an ordinary elliptic curve E_0/\mathbb{F}_q such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

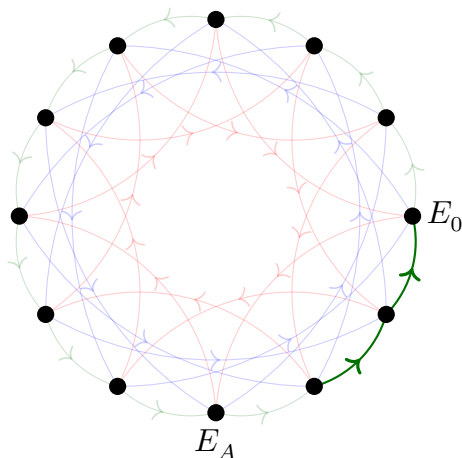
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$$\mathcal{L} = \{\ell_1, \ell_2, \ell_3\}$$

Alice

$$\rho_A = (2, 1, -1)$$

$$\mathfrak{a} = \ell_1^2 \ell_2 \ell_3^{-1}$$



Bob

$$\rho_B = (-2, 0, 1)$$

$$\mathfrak{a} = \ell_1^{-2} \ell_3$$

Fix a large enough finite field \mathbb{F}_q of large characteristic p and an ordinary elliptic curve E_0/\mathbb{F}_q such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

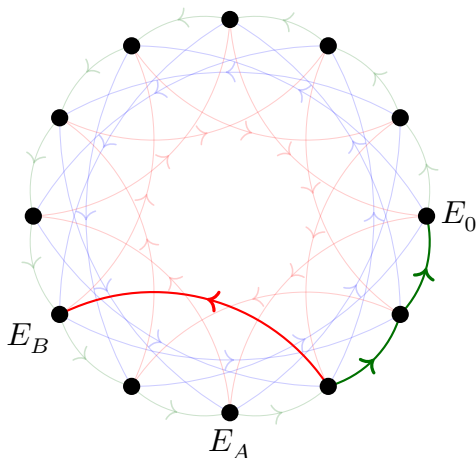
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$$\mathcal{L} = \{\ell_1, \ell_2, \ell_3\}$$

Alice

$$\rho_A = (2, 1, -1)$$

$$\mathfrak{a} = \ell_1^2 \ell_2 \ell_3^{-1}$$



Bob

$$\rho_B = (-2, 0, 1)$$

$$\mathfrak{a} = \ell_1^{-2} \ell_3$$

Fix a large enough finite field \mathbb{F}_q of large characteristic p and an ordinary elliptic curve E_0/\mathbb{F}_q such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

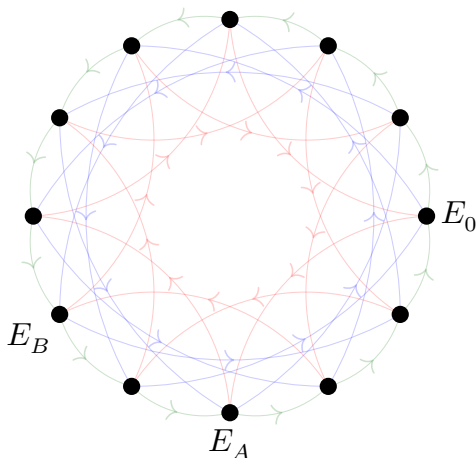
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$$\mathcal{L} = \{\ell_1, \ell_2, \ell_3\}$$

Alice

$$\rho_A = (2, 1, -1)$$

$$\mathfrak{a} = \ell_1^2 \ell_2 \ell_3^{-1}$$



Bob

$$\rho_B = (-2, 0, 1)$$

$$\mathfrak{a} = \ell_1^{-2} \ell_3$$

Fix a large enough finite field \mathbb{F}_q of large characteristic p and an ordinary elliptic curve E_0/\mathbb{F}_q such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

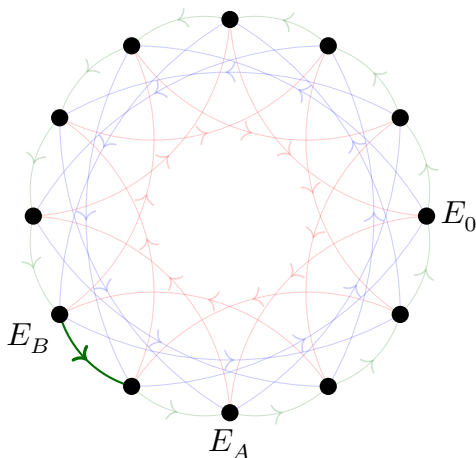
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$$\mathcal{L} = \{\ell_1, \ell_2, \ell_3\}$$

Alice

$$\rho_A = (2, 1, -1)$$

$$\mathfrak{a} = \ell_1^2 \ell_2 \ell_3^{-1}$$



Bob

$$\rho_B = (-2, 0, 1)$$

$$\mathfrak{a} = \ell_1^{-2} \ell_3$$

Fix a large enough finite field \mathbb{F}_q of large characteristic p and an ordinary elliptic curve E_0/\mathbb{F}_q such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

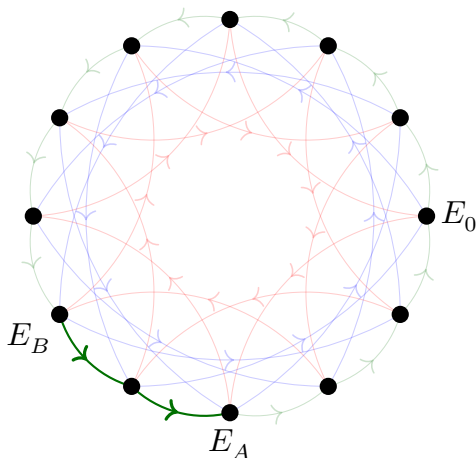
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$$\mathcal{L} = \{\ell_1, \ell_2, \ell_3\}$$

Alice

$$\rho_A = (2, 1, -1)$$

$$\mathfrak{a} = \ell_1^2 \ell_2 \ell_3^{-1}$$



Bob

$$\rho_B = (-2, 0, 1)$$

$$\mathfrak{a} = \ell_1^{-2} \ell_3$$

Fix a large enough finite field \mathbb{F}_q of large characteristic p and an ordinary elliptic curve E_0/\mathbb{F}_q such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

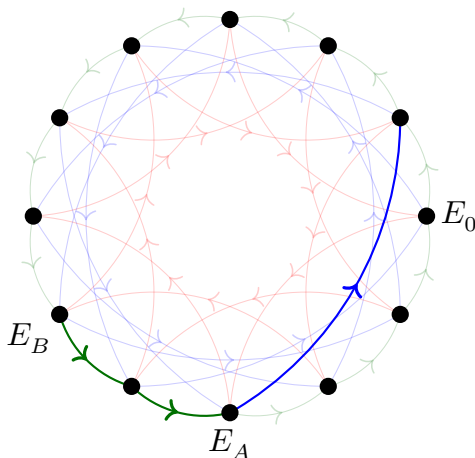
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$$\mathcal{L} = \{\ell_1, \ell_2, \ell_3\}$$

Alice

$$\rho_A = (2, 1, -1)$$

$$\mathfrak{a} = \ell_1^2 \ell_2 \ell_3^{-1}$$



Bob

$$\rho_B = (-2, 0, 1)$$

$$\mathfrak{a} = \ell_1^{-2} \ell_3$$

Fix a large enough finite field \mathbb{F}_q of large characteristic p and an ordinary elliptic curve E_0/\mathbb{F}_q such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

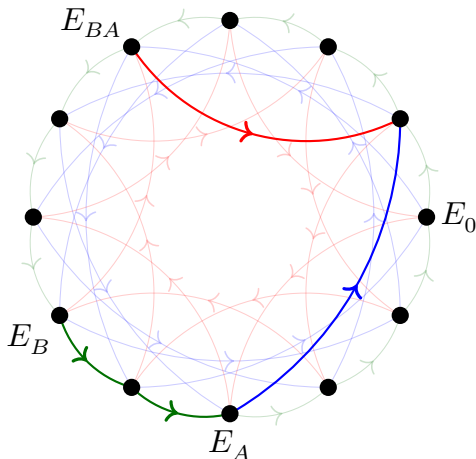
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$$\mathcal{L} = \{\ell_1, \ell_2, \ell_3\}$$

Alice

$$\rho_A = (2, 1, -1)$$

$$\mathfrak{a} = \ell_1^2 \ell_2 \ell_3^{-1}$$



Bob

$$\rho_B = (-2, 0, 1)$$

$$\mathfrak{a} = \ell_1^{-2} \ell_3$$

Fix a large enough finite field \mathbb{F}_q of large characteristic p and an ordinary elliptic curve E_0/\mathbb{F}_q such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

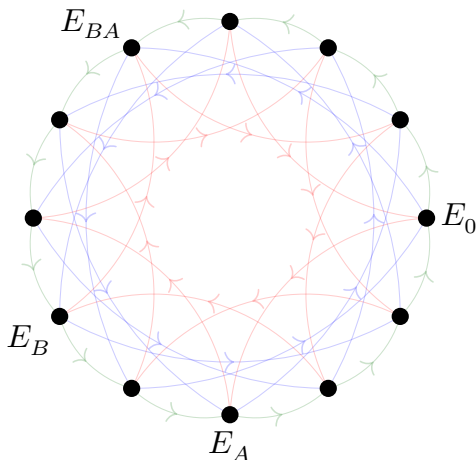
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$$\mathcal{L} = \{\ell_1, \ell_2, \ell_3\}$$

Alice

$$\rho_A = (2, 1, -1)$$

$$\mathfrak{a} = \ell_1^2 \ell_2 \ell_3^{-1}$$



Bob

$$\rho_B = (-2, 0, 1)$$

$$\mathfrak{a} = \ell_1^{-2} \ell_3$$

Fix a large enough finite field \mathbb{F}_q of large characteristic p and an ordinary elliptic curve E_0/\mathbb{F}_q such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

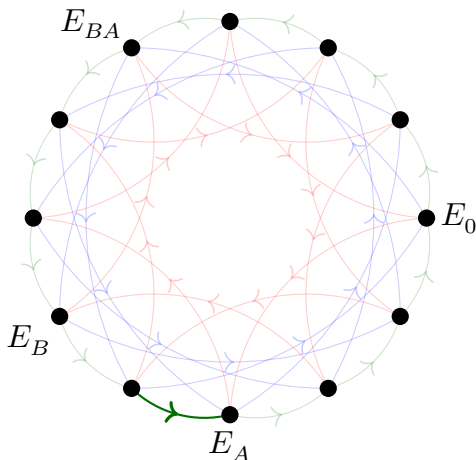
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$$\mathcal{L} = \{\ell_1, \ell_2, \ell_3\}$$

Alice

$$\rho_A = (2, 1, -1)$$

$$\mathfrak{a} = \ell_1^2 \ell_2 \ell_3^{-1}$$



Bob

$$\rho_B = (-2, 0, 1)$$

$$\mathfrak{a} = \ell_1^{-2} \ell_3$$

Fix a large enough finite field \mathbb{F}_q of large characteristic p and an ordinary elliptic curve E_0/\mathbb{F}_q such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

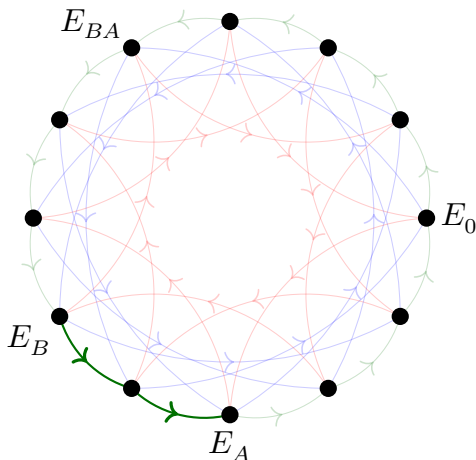
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$$\mathcal{L} = \{\ell_1, \ell_2, \ell_3\}$$

Alice

$$\rho_A = (2, 1, -1)$$

$$\mathfrak{a} = \ell_1^2 \ell_2 \ell_3^{-1}$$



Bob

$$\rho_B = (-2, 0, 1)$$

$$\mathfrak{a} = \ell_1^{-2} \ell_3$$

Fix a large enough finite field \mathbb{F}_q of large characteristic p and an ordinary elliptic curve E_0/\mathbb{F}_q such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

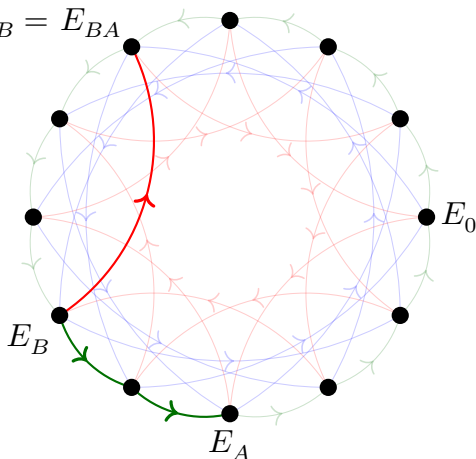
$$E_{AB} = E_{BA}$$

$$\mathcal{L} = \{\ell_1, \ell_2, \ell_3\}$$

Alice

$$\rho_A = (2, 1, -1)$$

$$\mathfrak{a} = \ell_1^2 \ell_2 \ell_3^{-1}$$



Bob

$$\rho_B = (-2, 0, 1)$$

$$\mathfrak{a} = \ell_1^{-2} \ell_3$$

Fix a large enough finite field \mathbb{F}_q of large characteristic p and an ordinary elliptic curve E_0/\mathbb{F}_q such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

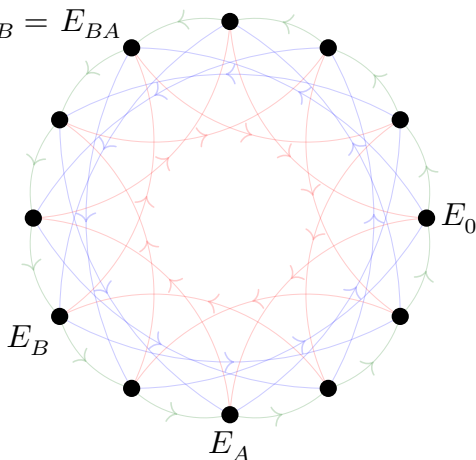
$$E_{AB} = E_{BA}$$

$$\mathcal{L} = \{\ell_1, \ell_2, \ell_3\}$$

Alice

$$\rho_A = (2, 1, -1)$$

$$\mathfrak{a} = \ell_1^2 \ell_2 \ell_3^{-1}$$



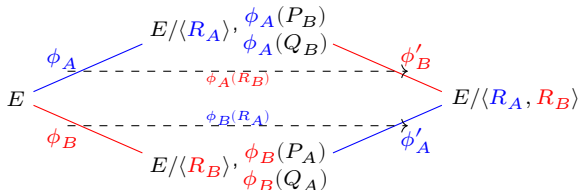
Bob

$$\rho_B = (-2, 0, 1)$$

$$\mathfrak{a} = \ell_1^{-2} \ell_3$$

Supersingular isogeny Diffie-Hellman

- ▶ Fix two small primes ℓ_A and ℓ_B ;
- ▶ Choose a prime p such that $p + 1 = \ell_A^a \ell_B^b f$ for a small correction term f ;
- ▶ Pick a random supersingular elliptic curve E/\mathbb{F}_{p^2} : $E(\mathbb{F}_{p^2}) \simeq \left(\frac{\mathbb{Z}}{(p+1)\mathbb{Z}}\right)^2$
- ▶ Alice consider $E[\ell_A^a] = \langle P_A, Q_A \rangle$ while Bob takes $E[\ell_B^b] = \langle P_B, Q_B \rangle$.
- ▶ **Secret Data:** $R_A = m_A P_A + n_A Q_A$ and $R_B = m_B P_B + n_B Q_B$.
- ▶ **Private Key:** isogenies $\phi_A : E \rightarrow E_A = E/E\langle R_A \rangle$ and $\phi_B : E \rightarrow E_B = E/E\langle R_B \rangle$.
- ▶ **Shared Data:** $E_A, \phi_A(P_B), \phi_A(Q_B)$ and $E_B, \phi_B(P_A), \phi_B(Q_A)$.
- ▶ **Shared Key:** $E/E\langle R_A, R_B \rangle = E_B/\langle \phi_B(R_A) \rangle = E_A/\langle \phi_A(R_B) \rangle$.



It is an adaptation of the Couveignes–Rostovtsev–Stolbunov scheme to supersingular elliptic curves.

Commutative Supersingular isogeny Diffie-Hellman

- ▶ Fix a prime $p = 4 \cdot \ell_1 \cdot \dots \cdot \ell_t - 1$ for small distinct odd primes ℓ_i .
- ▶ The elliptic curve $E_0 : y^2 = x^3 + x/\mathbb{F}_p$ is supersingular and its endomorphism ring restricted to \mathbb{F}_p is $\mathcal{O} = \mathbb{Z}[\pi]$ (commutative).
- ▶ All Montgomery curves $E_A : y^2 = x^3 + Ax^2 + x/\mathbb{F}_p$ that are supersingular, appear in the $\mathcal{C}(\mathcal{O})$ -orbit of E_0 (easy to store data).
- ▶ **Private Key:** it is an n -tuple of integers (e_1, \dots, e_t) sampled in a range $\{-m, \dots, m\}$ representing an ideal class $[\mathfrak{a}] = [\mathfrak{l}_1^{e_1} \cdot \dots \cdot \mathfrak{l}_t^{e_t}] \in \mathcal{C}(\mathcal{O})$ where $\mathfrak{l}_i = (\ell_i, \pi - 1)$.
- ▶ **Public Key:** The Montgomery coefficients A of the elliptic curve $E_A = [\mathfrak{a}] \cdot E_0 : y^2 = x^3 + Ax^2 + x$.
- ▶ **Shared Key:** If Alice and Bob have private key (\mathfrak{a}, A) and (\mathfrak{b}, B) then they can compute the shared key $E_{AB} = [\mathfrak{a}][\mathfrak{b}] \cdot E_0 = [\mathfrak{b}][\mathfrak{a}] \cdot E_0$.

The constraint to \mathbb{F}_p -rational isogenies can be interpreted as an orientation of the supersingular graph by the subring $\mathbb{Z}[\pi]$ of $\text{End}(E)$ generated by the Frobenius endomorphism π .

We introduce a general notion of orienting supersingular elliptic curves and their isogenies, and use this as the basis to construct a general oriented supersingular isogeny Diffie-Hellman (OSIDH) protocol.

Motivation

- ▶ Generalize CSIDH.
- ▶ Key space of SIDH: in order to have the two key spaces of similar size, we need to take $\ell_A^a \approx \ell_B^b \approx \sqrt{p}$. This implies that 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} .
- ▶ A feature shared by SIDH and CSIDH is that the isogenies are constructed as quotients of rational torsion subgroups. The need for rational points limits the choice of the prime p

Let \mathcal{O} be an order in an imaginary quadratic field K . An \mathcal{O} -orientation on a supersingular elliptic curve E is an inclusion $\iota : \mathcal{O} \hookrightarrow \mathbf{End}(E)$, and a K -orientation is an inclusion $\iota : K \hookrightarrow \mathbf{End}^0(E) = \mathbf{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$. An \mathcal{O} -orientation is *primitive* if $\mathcal{O} \simeq \mathbf{End}(E) \cap \iota(K)$.

Theorem

The category of K -oriented supersingular elliptic curves (E, ι) , whose morphisms are isogenies commuting with the K -orientations, is equivalent to the category of elliptic curves with CM by K .

Let $\phi : E \rightarrow F$ be an isogeny of degree ℓ . A K -orientation $\iota : K \hookrightarrow \mathbf{End}^0(E)$ determines a K -orientation $\phi_*(\iota) : K \hookrightarrow \mathbf{End}^0(F)$ 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 $\phi : E \rightarrow F$ is K -oriented if $\phi_*(\iota_E) = \iota_F$, i.e., if the orientation on F is induced by ϕ .

- ▶ $\mathbf{SS}(p) = \{\text{supersingular elliptic curves over } \overline{\mathbb{F}}_p \text{ up to isomorphism}\}.$
- ▶ $\mathbf{SS}_{\mathcal{O}}(p) = \{\mathcal{O}\text{-oriented s.s. elliptic curves over } \overline{\mathbb{F}}_p \text{ up to } K\text{-isomorphism}\}.$
- ▶ $\mathbf{SS}_{\mathcal{O}}^{pr}(p) = \text{subset of primitive } \mathcal{O}\text{-oriented curves}.$

The set $\mathbf{SS}_{\mathcal{O}}(p)$ admits a transitive group action:

$$\mathcal{C}l(\mathcal{O}) \times \mathbf{SS}_{\mathcal{O}}(p) \longrightarrow \mathbf{SS}_{\mathcal{O}}(p) \quad ([\mathfrak{a}], E) \longmapsto [\mathfrak{a}] \cdot E = E/E[\mathfrak{a}]$$

Proposition

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

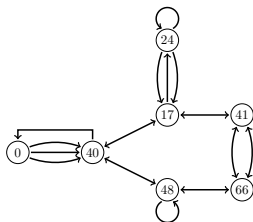
In particular, for fixed primitive \mathcal{O} -oriented E , we obtain a bijection of sets:

$$\mathcal{C}l(\mathcal{O}) \longrightarrow \mathbf{SS}_{\mathcal{O}}^{pr}(p) \quad [\mathfrak{a}] \longmapsto [\mathfrak{a}] \cdot E$$

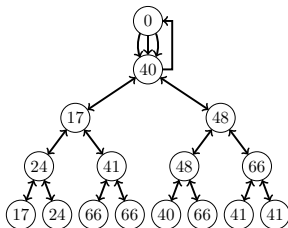
For any ideal class $[\mathfrak{a}]$ and generating set $\{\mathfrak{q}_1, \dots, \mathfrak{q}_r\}$ of small primes, coprime to $[\mathcal{O}_K : \mathcal{O}]$, we can find an identity $[\mathfrak{a}] = [\mathfrak{q}_1^{e_1} \cdot \dots \cdot \mathfrak{q}_r^{e_r}]$, in order to compute the action via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

ORIENTATION- AN EXAMPLE

Example. $p = 71, \ell = 2$, elliptic curves with $j = 0$ oriented by $\mathcal{O}_K = \mathbb{Z}[\omega]$,
 $\omega^2 + \omega + 1 = 0$.



The orientation by $K = \mathbb{Q}(\omega)$ differentiates vertices in the descending paths from E_0 , determining an infinite graph:



We have a bijection (isomorphism of sets with $\mathcal{C}(\mathcal{O})$ -action):

$$\mathcal{C}(\mathcal{O}) \cong \mathbf{SS}_{\mathcal{O}}^{pr}(\mathcal{O}) \subseteq \mathbf{SS}_{\mathcal{O}}(p)$$

On the other hand, the inclusion $\mathcal{O}_{i+1} \subset \mathcal{O}_i$ determines an inclusion

$$\begin{aligned} \mathbf{SS}_{\mathcal{O}_i}(p) \subset \mathbf{SS}_{\mathcal{O}_{i+1}}(p) &= \mathbf{SS}_{\mathcal{O}_i}(p) \cup \mathbf{SS}_{\mathcal{O}_{i+1}}^{pr}(p) \\ &\Downarrow \\ \mathbf{SS}_{\mathcal{O}_K}(p) \subset \mathbf{SS}_{\mathcal{O}_1}(p) &\subset \dots \subset \mathbf{SS}_{\mathcal{O}_i}(p) \subset \dots \end{aligned}$$

equipped with forgetful maps

$$\begin{aligned} \mathbf{SS}_{\mathcal{O}_i}(p) &\rightarrow \mathbf{SS}(p) \\ [(E, \mathcal{O}_i)] &\rightarrow j(E) \end{aligned}$$

Question

When the map $\mathbf{SS}_{\mathcal{O}_i}(p) \rightarrow \mathbf{SS}(p)$ and its restriction to $\mathbf{SS}_{\mathcal{O}_i}^{pr}(p)$ are injective?
When are they surjective?

Proposition

Let \mathcal{O} be an imaginary quadratic order of discriminant Δ and p a prime which is inert in \mathcal{O} . If $|\Delta| < p$, then the map $\mathbf{SS}_{\mathcal{O}}(p) \rightarrow \mathbf{SS}(p)$ is injective.

$p = 1013$					
i	$h(O_i)$	$ Y_i $	$ X_i $	$H(p)$	λ_i
1	1	1	1	85	0.3590
2	2	2	3	85	0.5593
3	4	4	7	85	0.7596
4	8	8	15	85	0.9599
5	16	16	29	85	1.1603
6	32	26	47	85	1.3606
7	64	43	66	85	1.5609
8	128	70	82	85	1.7612
9	256	79	85	85	1.9615
10	512	83	85	85	2.1618

$p = 1019$					
i	$h(O_i)$	$ Y_i $	$ X_i $	$H(p)$	λ_i
1	1	1	1	86	0.3587
2	2	2	3	86	0.5588
3	4	4	7	86	0.7590
4	8	8	15	86	0.9591
5	16	15	30	86	1.1593
6	32	29	49	86	1.3594
7	64	46	69	86	1.5595
8	128	64	81	86	1.7597
9	256	83	84	86	1.9598
10	512	86	86	86	2.1600

Definition

An ℓ -isogeny chain of length n from E_0 to E is a sequence of isogenies of degree ℓ :

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

The ℓ -isogeny chain is without backtracking if $\ker(\phi_{i+1} \circ \phi_i) \neq E_i[\ell]$, $\forall i$.
The isogeny chain is descending (or ascending, or horizontal) if each ϕ_i is descending (or ascending, or horizontal, respectively).

The dual isogeny of ϕ_i is the only isogeny ϕ_{i+1} satisfying $\ker(\phi_{i+1} \circ \phi_i) = E_i[\ell]$. Thus, an isogeny chain is without backtracking if and only if the composition of two consecutive isogenies is cyclic.

Lemma

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

PUSHING ISOGENIES ALONG A CHAIN

Suppose that (E_i, ϕ_i) is an ℓ -isogeny chain, with E_0 equipped with an \mathcal{O}_K -orientation $\iota_0 : \mathcal{O}_K \rightarrow \mathbf{End}(E_0)$.

For each i , $\iota_i : K \rightarrow \mathbf{End}^0(E_i)$ is the induced K -orientation on E_i . Write $\mathcal{O}_i = \mathbf{End}(E_i) \cap \iota_i(K)$ with $\mathcal{O}_0 = \mathcal{O}_K$.

If \mathfrak{q} is a split prime in \mathcal{O}_K over $q \neq \ell, p$, then the isogeny

$$\psi_0 : E_0 \rightarrow F_0 = E_0 / E_0[\mathfrak{q}]$$

can be extended to the ℓ -isogeny chain by pushing forward $C_0 = E_0[\mathfrak{q}]$:

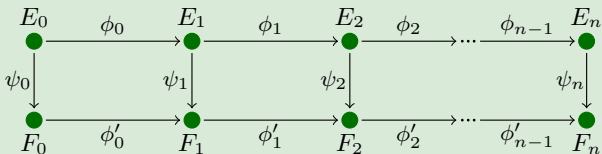
$$C_0 = E_0[\mathfrak{q}], C_1 = \phi_0(C_0), \dots, C_n = \phi_{n-1}(C_{n-1})$$

and defining $F_i = E_i / C_i$.

$$\begin{array}{ccc}
 E_{i-1}/C_{i-1} = F_{i-1} & \xrightarrow{\ell} & F_i = E_i/C_i \\
 \uparrow \psi_{i-1} \mathfrak{q} & & \uparrow \psi_i \mathfrak{q} \\
 C_{i-1} \subseteq E_{i-1} & \xrightarrow[\ell]{} & E_i \supseteq C_i
 \end{array}$$

Definition

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

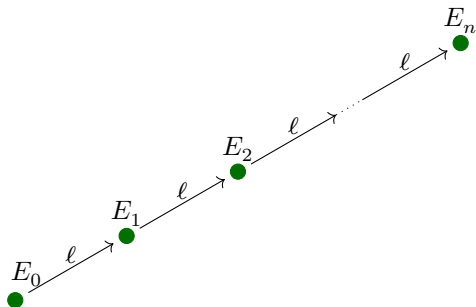


We also refer to an ℓ -ladder of degree q as a q -isogeny of ℓ -isogeny chains.

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).

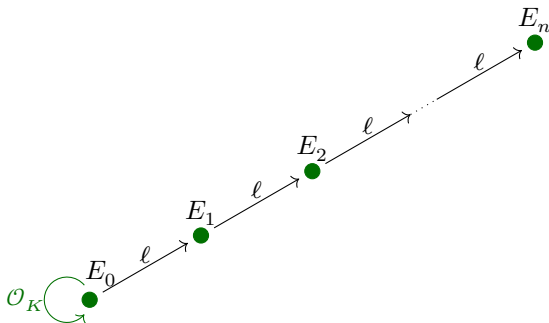
We say that the ℓ -ladder is level if ψ_0 is a horizontal q -isogeny. If the ℓ -ladder is descending (or ascending), then we refer to the length of the ladder as its depth (or, respectively, as its height).

We consider an elliptic curve E_0 with an effective endomorphism ring (eg. $j_0 = 0, 1728$) and a chain of ℓ -isogenies.



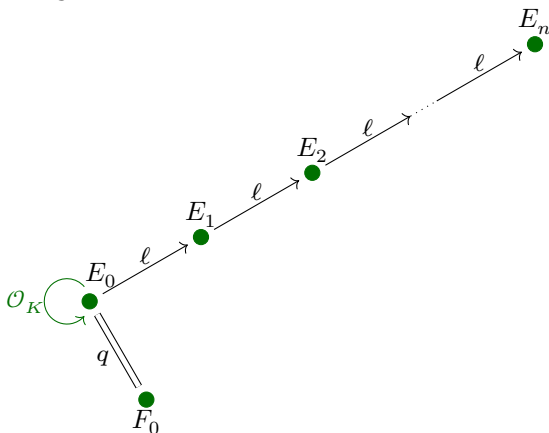
We consider an elliptic curve E_0 with an effective endomorphism ring (eg. $j_0 = 0, 1728$) and a chain of ℓ -isogenies.

- ▶ For $\ell = 2$ (or 3) a suitable candidate for \mathcal{O}_K could be the Gaussian integers $\mathbb{Z}[i]$ or the Eisenstein integers $\mathbb{Z}[\omega]$.



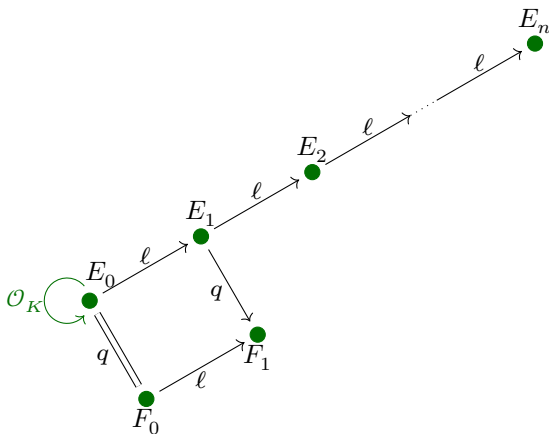
We consider an elliptic curve E_0 with an effective endomorphism ring (eg. $j_0 = 0, 1728$) and a chain of ℓ -isogenies.

- Horizontal isogenies must be endomorphisms



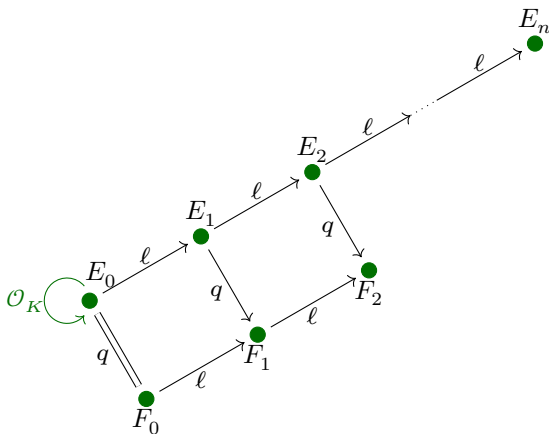
We consider an elliptic curve E_0 with an effective endomorphism ring (eg. $j_0 = 0, 1728$) and a chain of ℓ -isogenies.

- We push forward our q -orientation obtaining F_1 .



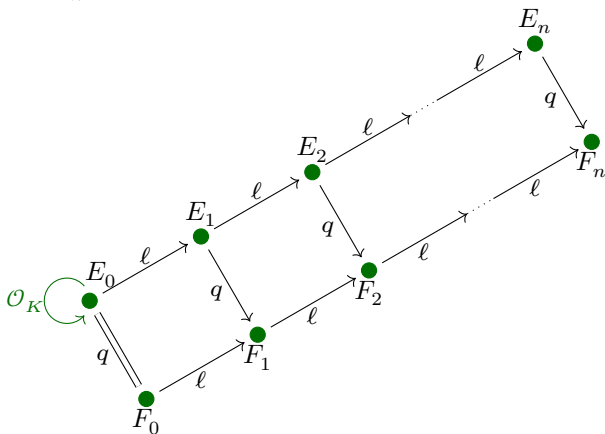
We consider an elliptic curve E_0 with an effective endomorphism ring (eg. $j_0 = 0, 1728$) and a chain of ℓ -isogenies.

- We repeat the process for F_2 .

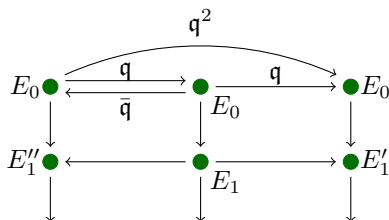


We consider an elliptic curve E_0 with an effective endomorphism ring (eg. $j_0 = 0, 1728$) and a chain of ℓ -isogenies.

- And again till F_n .



HOW MANY STEPS BEFORE THE IDEALS ACT DIFFERENTLY?



$E'_i \neq E''_i$ 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

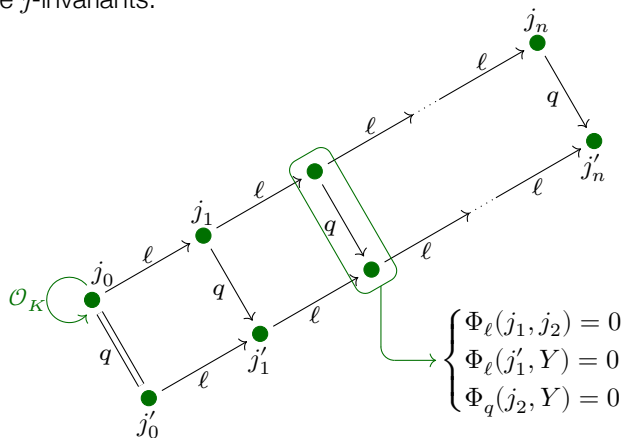
$$\mathfrak{q}^2 = \mathbf{N}(\mathfrak{q}^2) = \mathbf{N}(a + b\ell^i\omega)$$

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

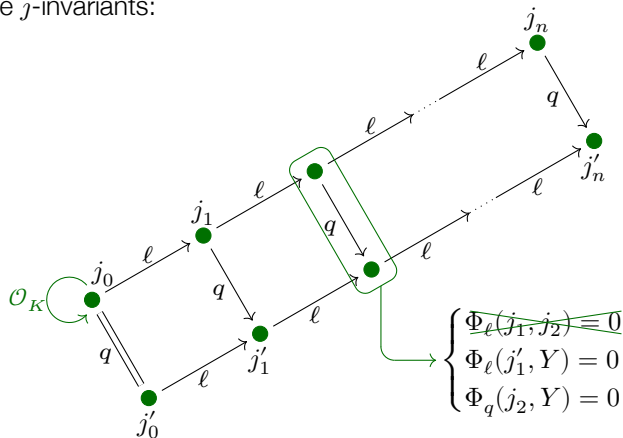
$$\mathbf{N}(a + b\ell^i) = a^2 \pm abt\ell^i + b^2s\ell^{2i} \quad \text{where} \quad \omega^2 + t\omega + s = 0$$

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

If we look at modular polynomials $\Phi_\ell(X, Y)$ and $\Phi_q(X, Y)$ we realize that all we need are the j -invariants:



If we look at modular polynomials $\Phi_\ell(X, Y)$ and $\Phi_q(X, Y)$ we realize that all we need are the j -invariants:



Since j_2 is given (the initial chain is known) and supposing that j'_1 has already been constructed, j'_2 is determined by a system of two equations

PUBLIC DATA: A chain of ℓ -isogenies $E_0 \rightarrow E_1 \rightarrow \dots \rightarrow E_n$

ALICE

BOB

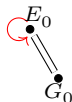
PUBLIC DATA: A chain of ℓ -isogenies $E_0 \rightarrow E_1 \rightarrow \dots \rightarrow E_n$

Choose a primitive
 \mathcal{O}_K -orientation of
 E_0

ALICE



BOB



PUBLIC DATA: A chain of ℓ -isogenies $E_0 \rightarrow E_1 \rightarrow \dots \rightarrow E_n$

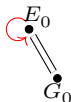
Choose a primitive \mathcal{O}_K -orientation of E_0

Push it forward to depth n

ALICE



BOB



$$\underbrace{E_0 = F_0 \rightarrow F_1 \rightarrow \dots \rightarrow F_n}_{\phi_A}$$

$$\underbrace{E_0 = G_0 \rightarrow G_1 \rightarrow \dots \rightarrow G_n}_{\phi_B}$$

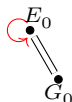
PUBLIC DATA: A chain of ℓ -isogenies $E_0 \rightarrow E_1 \rightarrow \dots \rightarrow E_n$

Choose a primitive \mathcal{O}_K -orientation of E_0

ALICE



BOB



Push it forward to depth n

$$\underbrace{E_0 = F_0 \rightarrow F_1 \rightarrow \dots \rightarrow F_n}_{\phi_A}$$

$$\underbrace{E_0 = G_0 \rightarrow G_1 \rightarrow \dots \rightarrow G_n}_{\phi_B}$$

Exchange data

$$\{G_i\}_{i=1}^n \leftarrow \phi_A \quad \phi_B \rightarrow \{F_i\}_{i=1}^n$$

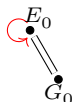
PUBLIC DATA: A chain of ℓ -isogenies $E_0 \rightarrow E_1 \rightarrow \dots \rightarrow E_n$

Choose a primitive \mathcal{O}_K -orientation of E_0

ALICE



BOB



Push it forward to depth n

$$\underbrace{E_0 = F_0 \rightarrow F_1 \rightarrow \dots \rightarrow F_n}_{\phi_A}$$

$$\underbrace{E_0 = G_0 \rightarrow G_1 \rightarrow \dots \rightarrow G_n}_{\phi_B}$$

Exchange data

$$\{G_i\}_{i=1}^n$$

$$\{F_i\}_{i=1}^n$$

Compute shared secret

Compute $\phi_A \cdot \{G_i\}$

Compute $\phi_B \cdot \{F_i\}$

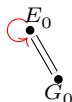
PUBLIC DATA: A chain of ℓ -isogenies $E_0 \rightarrow E_1 \rightarrow \dots \rightarrow E_n$

Choose a primitive \mathcal{O}_K -orientation of E_0

ALICE



BOB



Push it forward to depth n

$$\underbrace{E_0 = F_0 \rightarrow F_1 \rightarrow \dots \rightarrow F_n}_{\phi_A}$$

$$\underbrace{E_0 = G_0 \rightarrow G_1 \rightarrow \dots \rightarrow G_n}_{\phi_B}$$

Exchange data

$$\{G_i\}_{i=1}^n$$

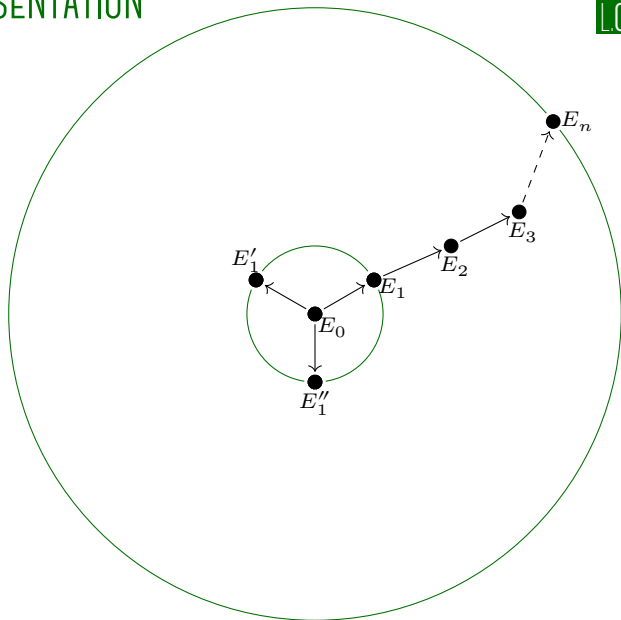
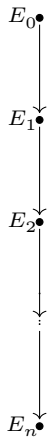
$$\{F_i\}_{i=1}^n$$

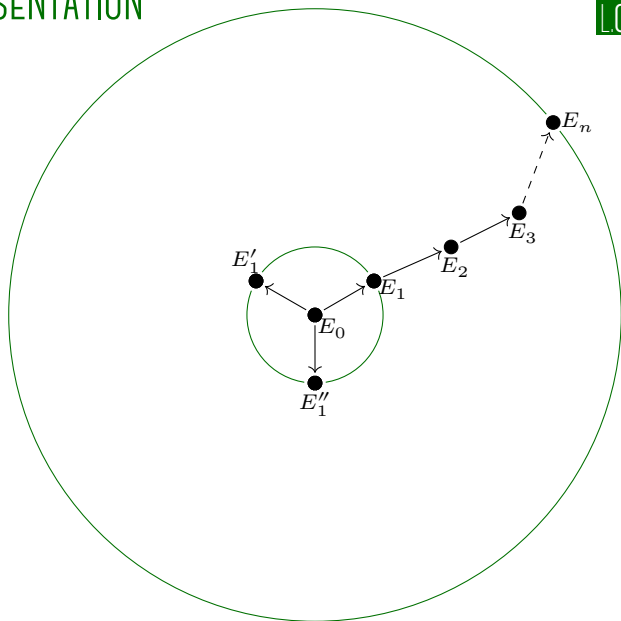
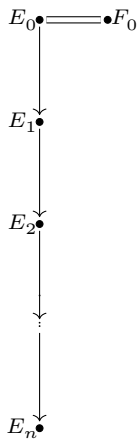
Compute shared secret

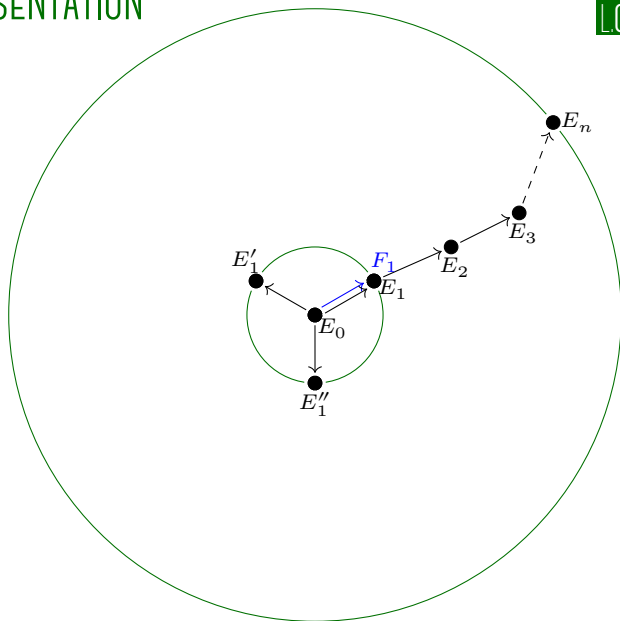
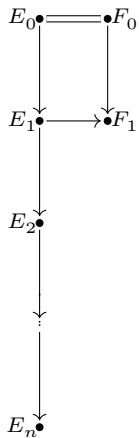
$$\text{Compute } \phi_A \cdot \{G_i\}$$

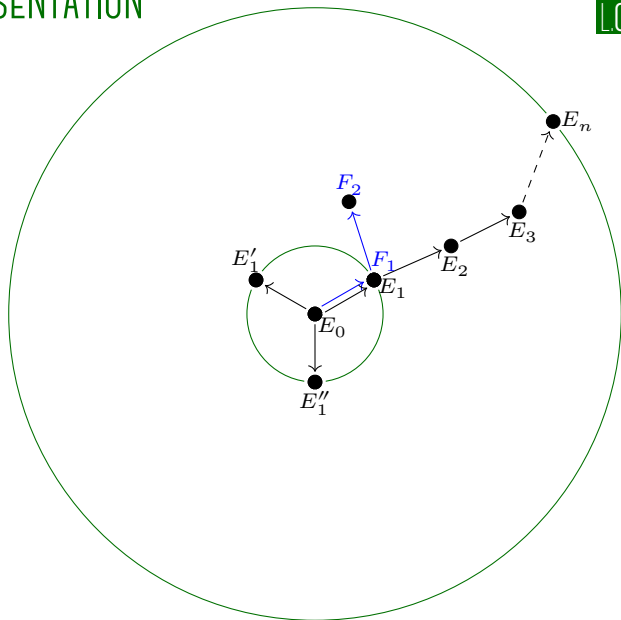
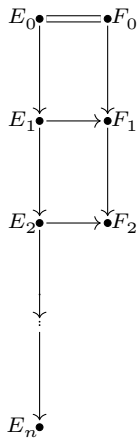
$$\text{Compute } \phi_B \cdot \{F_i\}$$

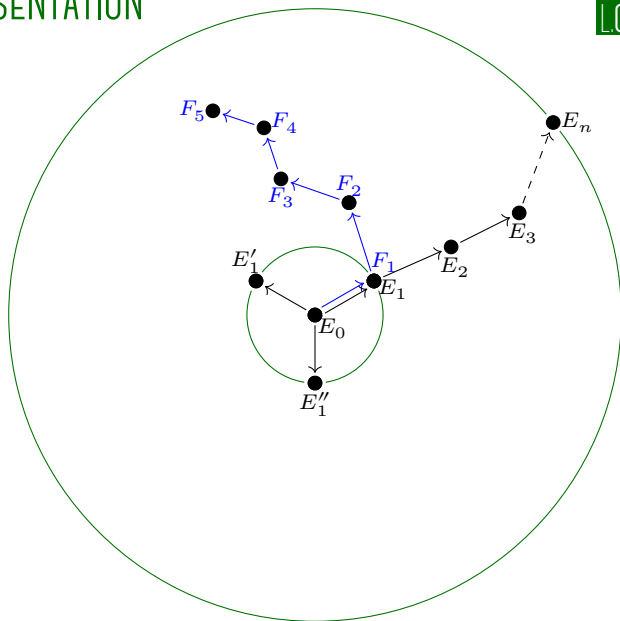
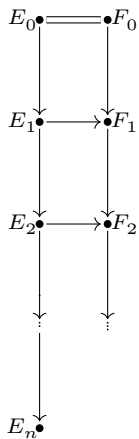
In the end, Alice and Bob will share a new chain $E_0 \rightarrow H_1 \rightarrow \dots \rightarrow H_n$

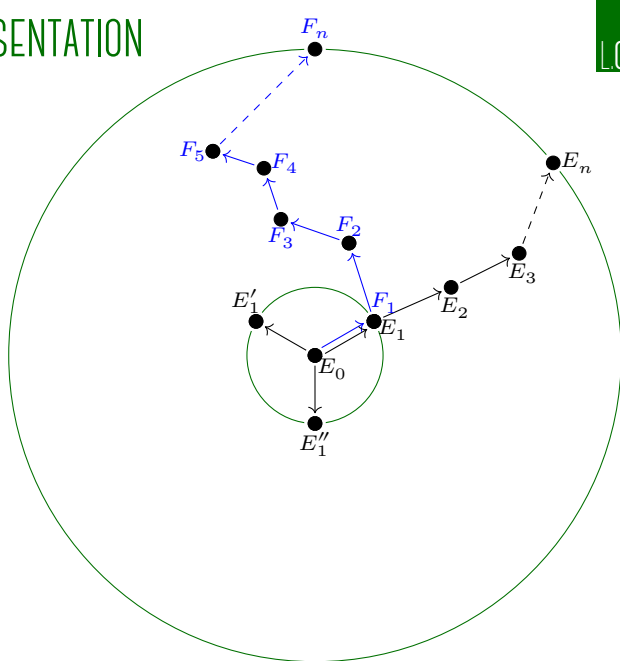
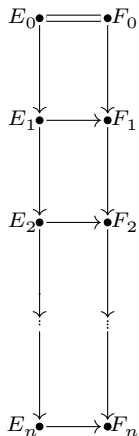


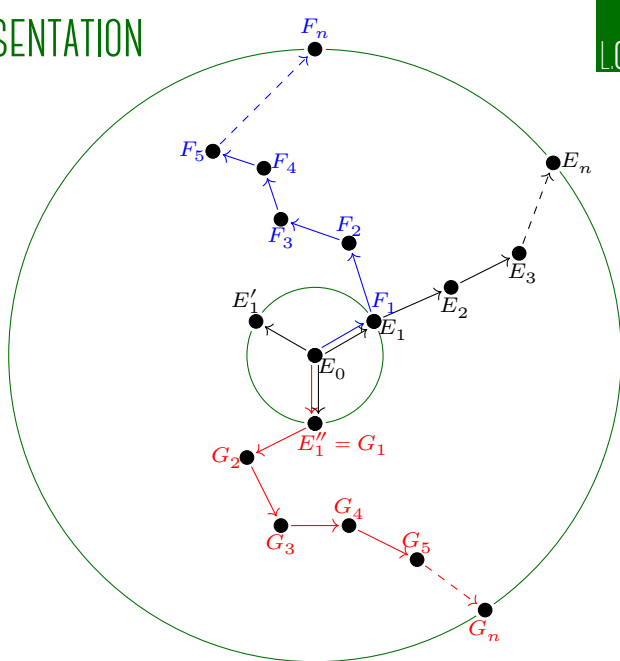
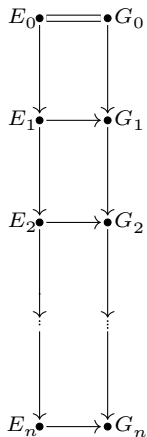


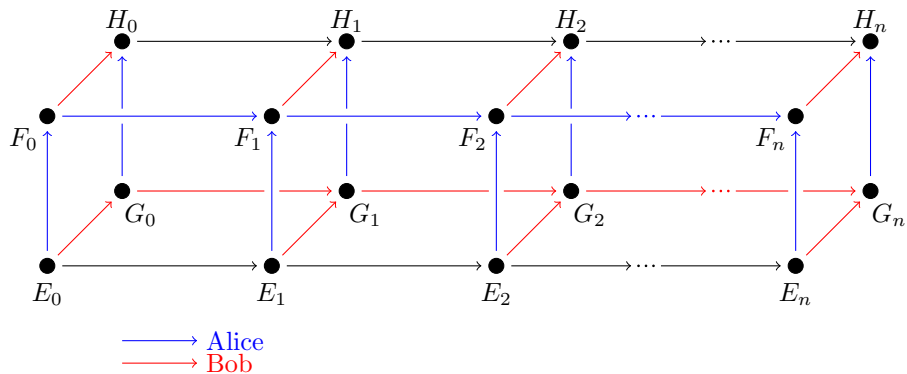












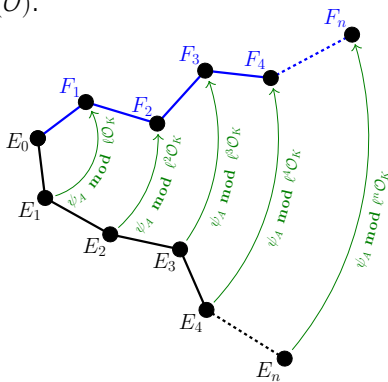
A FIRST NAIVE PROTOCOL - WEAKNESS

In reality, sharing (F_i) and (G_i) reveals too much of the private data.

From the short exact sequence of class groups:

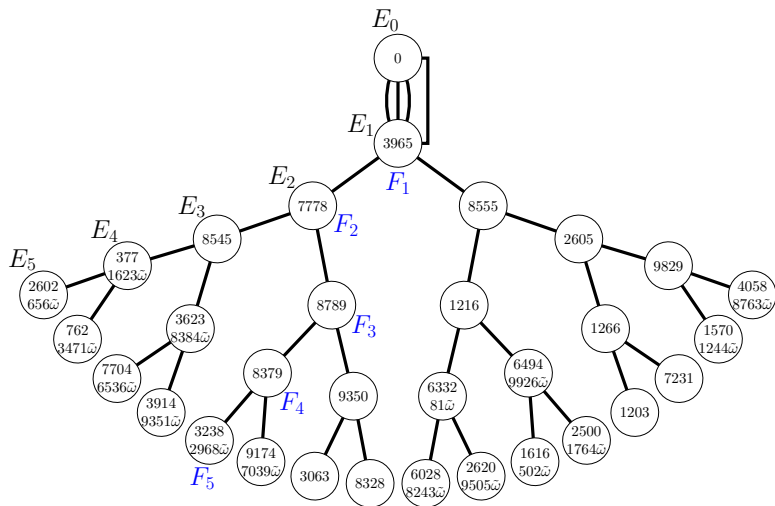
$$1 \rightarrow \frac{(\mathcal{O}_K/\ell^n \mathcal{O}_K)^\times}{\mathcal{O}_K^\times (\mathbb{Z}/\ell^n \mathbb{Z})^\times} \rightarrow \mathcal{Cl}(\mathcal{O}) \rightarrow \mathcal{Cl}(\mathcal{O}_K) \rightarrow 1$$

an adversary can compute successive approximations (mod ℓ^i) to ϕ_A and ϕ_B modulo ℓ^n hence in $\mathcal{Cl}(\mathcal{O})$.



AN EXAMPLE: COMPUTE SUCCESSIVE APPROXIMATIONS

Take $q = p^2 = 10007^2$. $E_0 : y^2 = x^3 + 1$ of j -invariant 0 is supersingular over \mathbb{F}_q . We orient E_0 by $\mathcal{O}_K = \mathbb{Z}[\omega] \hookrightarrow \text{End}(E_0)$ where $w^2 + w + 1$.



Algorithm. Action of an ideal $[(q, a + b\ell^i w)] \in \mathcal{C}l(\mathbb{Z} + \ell^i \mathcal{O}_K)$ lying over q on the set of primitive \mathcal{O} -oriented elliptic curves $\mathbf{SS}_{\mathcal{O}}^{pr}(p)$.

Input: The j -invariants of two elliptic curves E and E' over \mathbb{F}_{p^2} known to be q -isogenous.

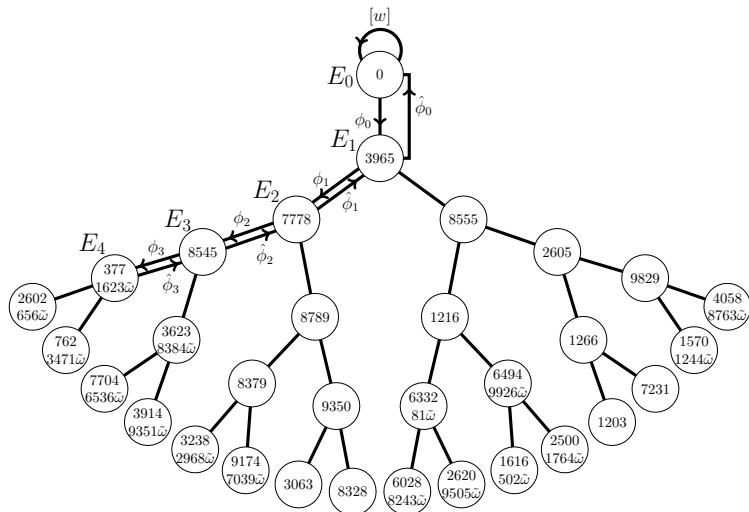
Output: The ideal $[a] \in \{[q], [\bar{q}]\}$ such that $[a] * j(E) = j(E')$.

1. Compute q -division polynomial $\psi_q(x)$.
2. Factor $\psi_q(x)$ and find the factor $f(x)$ corresponding to the desired isogeny $\phi : E \rightarrow E'$.
3. Pick a root of f , i.e., a q -torsion point P lying in the kernel of ϕ .
4. Set $m\mathcal{O} = q\bar{q} = (q, a + b\ell^i w)(q, a' + b'\ell^i w)$.
5. **If** $[a]P + [b] \cdot [\ell^i w]P = O_E$
 Return q .
 Else
 Return \bar{q} .

AN EXAMPLE: COMPUTE SUCCESSIVE APPROXIMATIONS

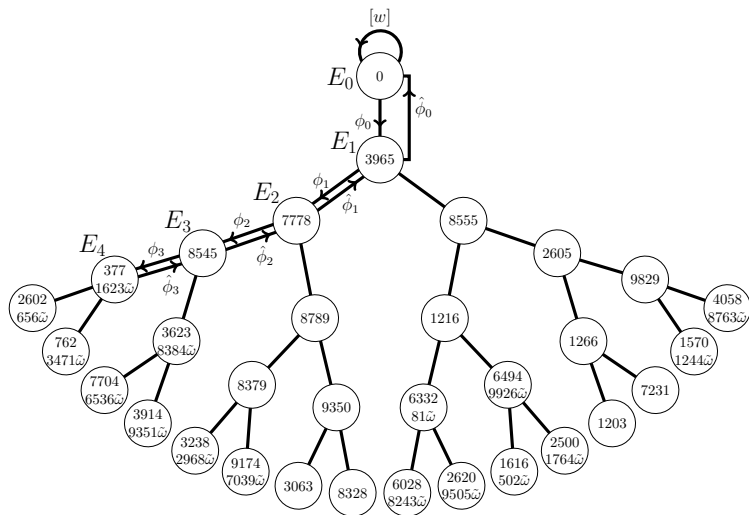
The action of $\ell^i \omega$ on E_i will be given by the composition

$$\phi_{i-1} \circ \cdots \circ \phi_2 \circ \phi_1 \circ \phi_0 \circ [\omega] \circ \hat{\phi}_0 \circ \hat{\phi}_1 \circ \hat{\phi}_2 \circ \cdots \circ \hat{\phi}_{i-1}$$



AN EXAMPLE: COMPUTE SUCCESSIVE APPROXIMATIONS

Observe that this is exactly the definition of orientation by \mathcal{O}_i transmitted to E_i along the isogeny $E_0 \rightarrow E_1 \rightarrow E_2 \rightarrow \dots \rightarrow E_i$.



Computing successive approximations

We are given two sequences $\{E_i\}_{i=0}^n$ and $\{F_i\}_{i=0}^n$. Suppose that $E_i = F_i$ for all $i \leq m$; there are l possibilities for F_{m+1} , and we need to find $\beta \in \mathbf{End}(\mathcal{O}_K)$ such that

1. $\beta \equiv 1 \pmod{\ell^m}$ so that $\beta_* E_i = F_i = E_i$ for all $i \leq m$;
2. $\beta_* E_{m+1} = F_{m+1}$;
3. β is smooth with small exponents (in order to determine the action of β modulo ℓ^{m+1} effectively).

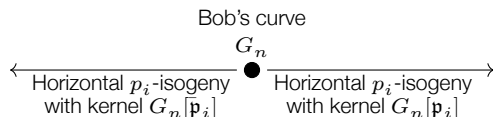
Once that we have constructed α such that $\alpha_* E_i = F_i$ for all $m < i \leq k$, then we can substitute **1** with

- 1'. $\beta \equiv \alpha \pmod{\ell^k}$ so that $\beta_* E_{k+1} = F_{k+1}$.

How can we avoid this while still giving the other enough information?

Instead Alice and Bob can send only $F = F_n$ and $G = G_n$.

Problem Once Alice receives the unoriented curve G_n computed by Bob she also needs additional information for each prime \mathfrak{p}_i :



In fact, she has no information as to which directions — out of $p_i + 1$ total p_i -isogenies — to take as \mathfrak{p}_i and $\bar{\mathfrak{p}}_i$.

Solution They share a collection of local isogeny data $(F_n[\mathfrak{q}_j])$ and $(G_n[\mathfrak{q}_j])$ which identifies the isogeny directions (out of $q_i + 1$) for a system of small split primes (\mathfrak{q}_i) in \mathcal{O}_K .

PUBLIC DATA: A chain of ℓ -isogenies $E_0 \rightarrow E_1 \rightarrow \dots \rightarrow E_n$ and a set of splitting primes $\mathfrak{p}_1, \dots, \mathfrak{p}_t \subseteq \mathcal{O} \subseteq \text{End}E_n \cap K \subseteq \mathcal{O}_K$

ALICE

BOB

PUBLIC DATA: A chain of ℓ -isogenies $E_0 \rightarrow E_1 \rightarrow \dots \rightarrow E_n$ and a set of splitting primes $\mathfrak{p}_1, \dots, \mathfrak{p}_t \subseteq \mathcal{O} \subseteq \text{End}E_n \cap K \subseteq \mathcal{O}_K$

	ALICE	BOB
Choose integers in a bound $[-r, r]$	(e_1, \dots, e_t)	(d_1, \dots, d_t)

PUBLIC DATA: A chain of ℓ -isogenies $E_0 \rightarrow E_1 \rightarrow \dots \rightarrow E_n$ and a set of splitting primes $\mathfrak{p}_1, \dots, \mathfrak{p}_t \subseteq \mathcal{O} \subseteq \text{End}E_n \cap K \subseteq \mathcal{O}_K$

	ALICE	BOB
Choose integers in a bound $[-r, r]$	(e_1, \dots, e_t)	(d_1, \dots, d_t)
Construct an isogenous curve	$F_n = E_n / E_n [\mathfrak{p}_1^{e_1} \dots \mathfrak{p}_t^{e_t}]$	$G_n = E_n / E_n [\mathfrak{p}_1^{d_1} \dots \mathfrak{p}_t^{d_t}]$

PUBLIC DATA: A chain of ℓ -isogenies $E_0 \rightarrow E_1 \rightarrow \dots \rightarrow E_n$ and a set of splitting primes $\mathfrak{p}_1, \dots, \mathfrak{p}_t \subseteq \mathcal{O} \subseteq \text{End}E_n \cap K \subseteq \mathcal{O}_K$

	ALICE	BOB
Choose integers in a bound $[-r, r]$	(e_1, \dots, e_t)	(d_1, \dots, d_t)
Construct an isogenous curve	$F_n = E_n / E_n [\mathfrak{p}_1^{e_1} \dots \mathfrak{p}_t^{e_t}]$	$G_n = E_n / E_n [\mathfrak{p}_1^{d_1} \dots \mathfrak{p}_t^{d_t}]$
Precompute all directions $\forall i$	$F_{n,i}^{(-r)} \leftarrow F_{n,i}^{(-r+1)} \leftarrow \dots \leftarrow F_{n,i}^{(1)} \leftarrow F_n$	$G_{n,i}^{(-r)} \leftarrow G_{n,i}^{(-r+1)} \leftarrow \dots \leftarrow G_{n,i}^{(1)} \leftarrow G_n$

PUBLIC DATA: A chain of ℓ -isogenies $E_0 \rightarrow E_1 \rightarrow \dots \rightarrow E_n$ and a set of splitting primes $\mathfrak{p}_1, \dots, \mathfrak{p}_t \subseteq \mathcal{O} \subseteq \text{End}E_n \cap K \subseteq \mathcal{O}_K$

Choose integers
in a bound $[-r, r]$
Construct an
isogenous curve
Precompute all
directions $\forall i$
... and their
conjugates

ALICE

$$(e_1, \dots, e_t)$$

$$F_n = E_n / E_n [\mathfrak{p}_1^{e_1} \dots \mathfrak{p}_t^{e_t}]$$

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

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

BOB

$$(d_1, \dots, d_t)$$

$$G_n = E_n / E_n [\mathfrak{p}_1^{d_1} \dots \mathfrak{p}_t^{d_t}]$$

$$G_{n,i}^{(-r)} \leftarrow G_{n,i}^{(-r+1)} \leftarrow \dots \leftarrow G_{n,i}^{(1)} \leftarrow G_n$$

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

PUBLIC DATA: A chain of ℓ -isogenies $E_0 \rightarrow E_1 \rightarrow \dots \rightarrow E_n$ and a set of splitting primes $\mathfrak{p}_1, \dots, \mathfrak{p}_t \subseteq \mathcal{O} \subseteq \text{End}E_n \cap K \subseteq \mathcal{O}_K$

Choose integers in a bound $[-r, r]$
 Construct an isogenous curve
 Precompute all directions $\forall i$
 ... and their conjugates
 Exchange data

ALICE

$$(e_1, \dots, e_t)$$

$$F_n = E_n / E_n [\mathfrak{p}_1^{e_1} \dots \mathfrak{p}_t^{e_t}]$$

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

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

BOB

$$(d_1, \dots, d_t)$$

$$G_n = E_n / E_n [\mathfrak{p}_1^{d_1} \dots \mathfrak{p}_t^{d_t}]$$

$$G_{n,i}^{(-r)} \leftarrow G_{n,i}^{(-r+1)} \leftarrow \dots \leftarrow G_{n,i}^{(1)} \leftarrow G_n$$

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

G_n + directions

F_n + directions



PUBLIC DATA: A chain of ℓ -isogenies $E_0 \rightarrow E_1 \rightarrow \dots \rightarrow E_n$ and a set of splitting primes $\mathfrak{p}_1, \dots, \mathfrak{p}_t \subseteq \mathcal{O} \subseteq \text{End}E_n \cap K \subseteq \mathcal{O}_K$

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

PUBLIC DATA: A chain of ℓ -isogenies $E_0 \rightarrow E_1 \rightarrow \dots \rightarrow E_n$ and a set of splitting primes $\mathfrak{p}_1, \dots, \mathfrak{p}_t \subseteq \mathcal{O} \subseteq \text{End}E_n \cap K \subseteq \mathcal{O}_K$

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

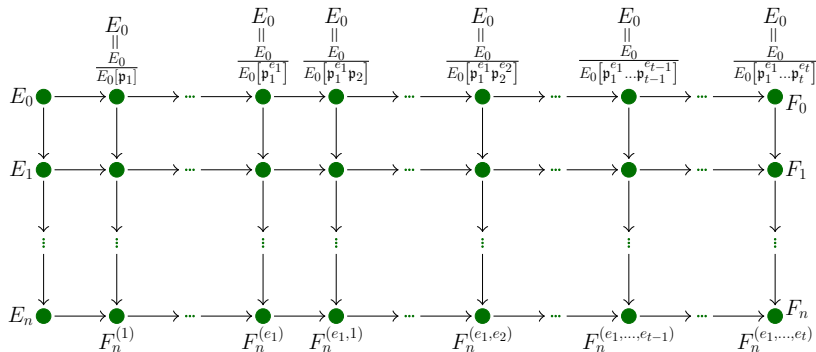
In the end, they share $H_n = E_n / E_n [\mathfrak{p}_1^{e_1+d_1} \cdot \dots \cdot \mathfrak{p}_t^{e_t+d_t}]$

OSIDH PROTOCOL - GRAPHIC REPRESENTATION I

The first step consists of choosing the secret keys; these are represented by a sequence of integers (e_1, \dots, 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

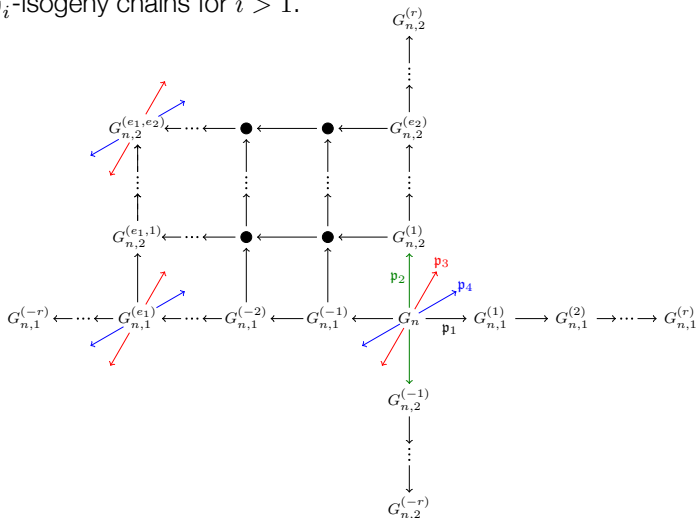
$$F_n = \frac{E_n}{E_n[\mathbf{p}_1^{e_1} \dots \mathbf{p}_t^{e_t}]}$$

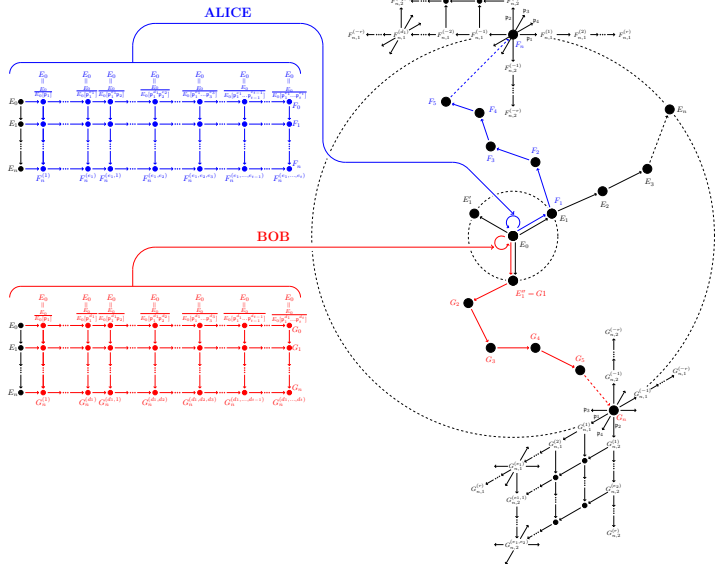
by means of constructing the following commutative diagram



OSIDH PROTOCOL - GRAPHIC REPRESENTATION II

Once that Alice obtain from Bob the curve G_n together with the collection of data encoding the directions, she takes e_1 steps in the \mathfrak{p}_1 -isogeny chain and push forward all the \mathfrak{p}_i -isogeny chains for $i > 1$.





OSIDH PROTOCOL - AN EXAMPLE

$$p = 10007$$

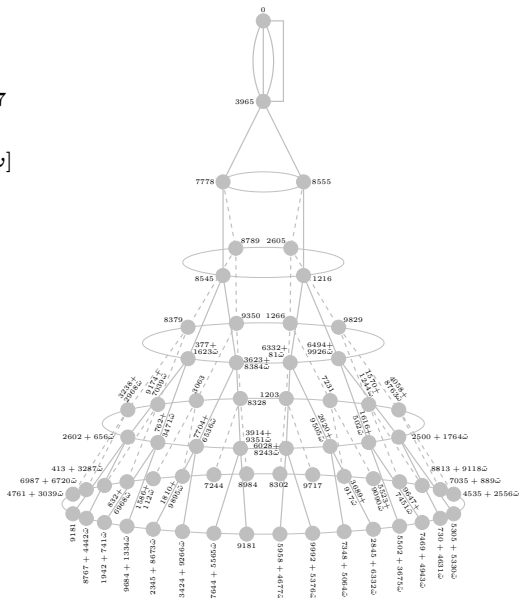
$$\ell = 2$$

$$\mathcal{O}_K = \mathbb{Z}[\omega]$$

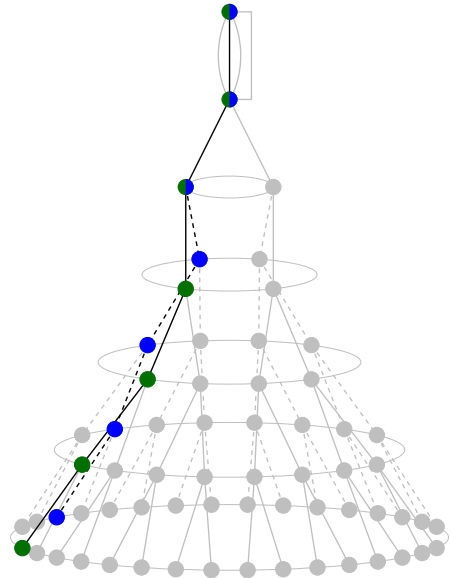
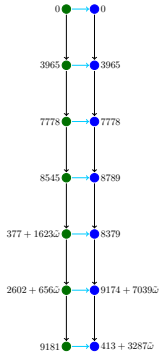
$$l_1 = 13$$

$$l_2 = 31$$

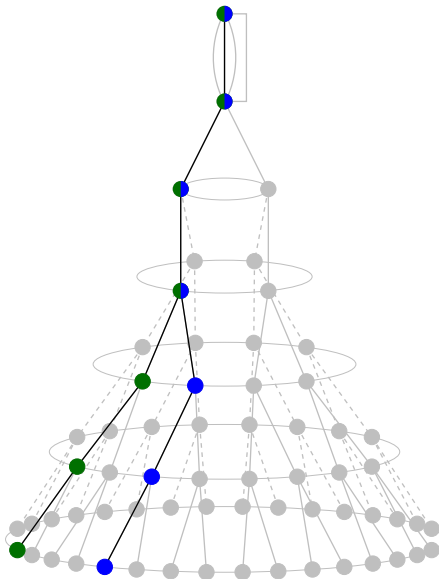
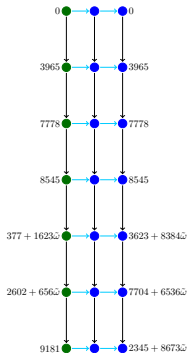
$$l_3 = 43$$



Alice secret key: $(\alpha_1^5, \alpha_2^3, \alpha_3^2)$

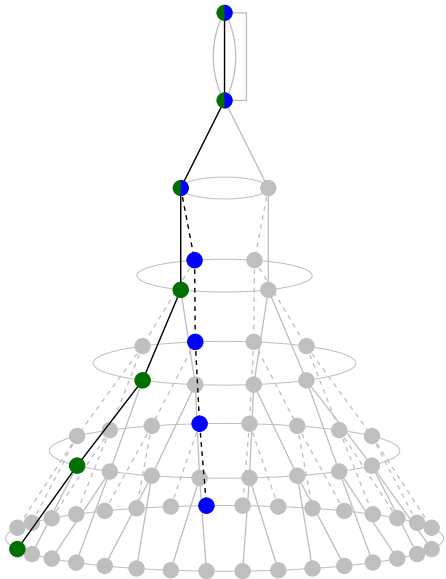
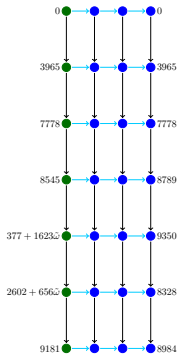


Alice secret key: (r_1^5, r_2^3, r_3^2)

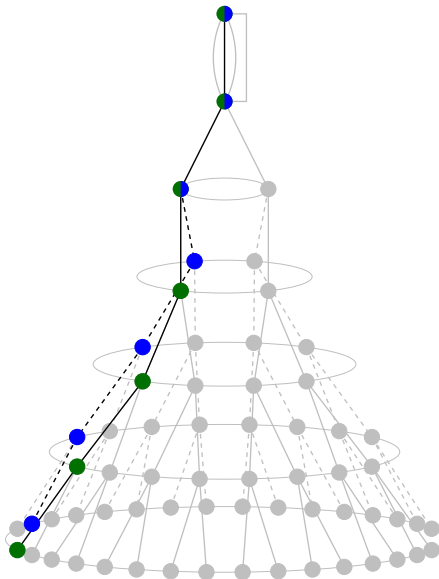
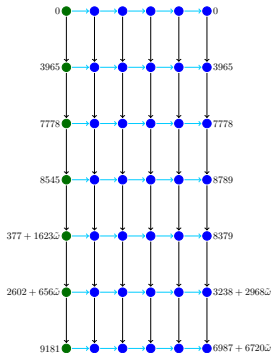


OSIDH PROTOCOL - AN EXAMPLE

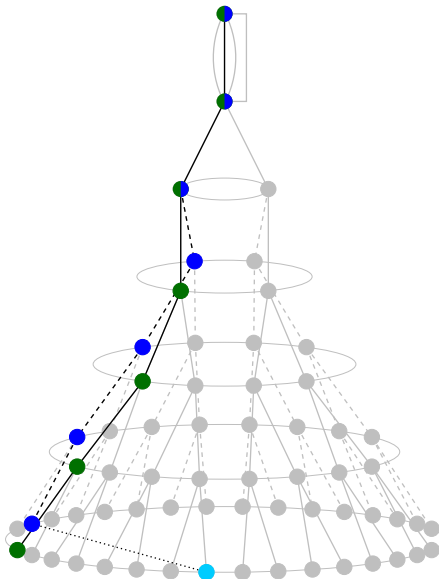
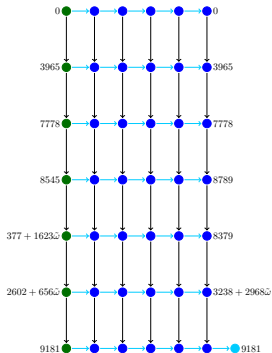
Alice secret key: $\{r_1^5, r_2^3, r_3^2\}$



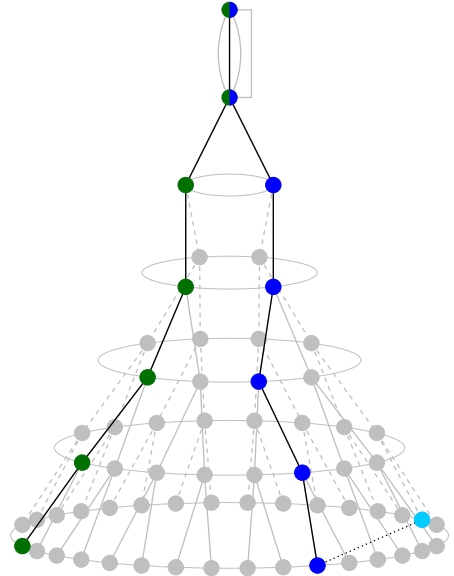
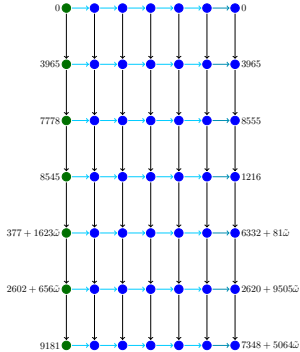
Alice secret key: $(\alpha_1^5, \alpha_2^3, \alpha_3^2)$



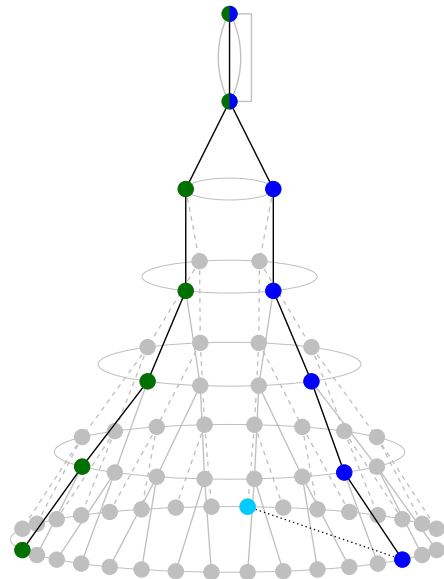
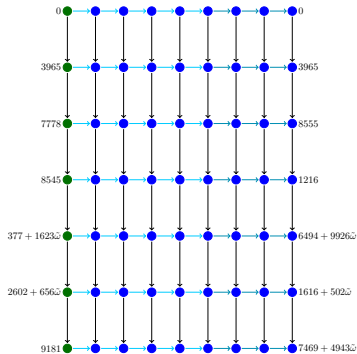
Alice secret key: (r_1^5, r_2^3, r_3^2)



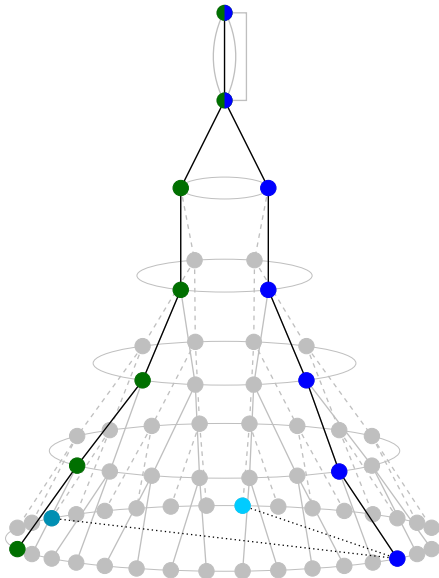
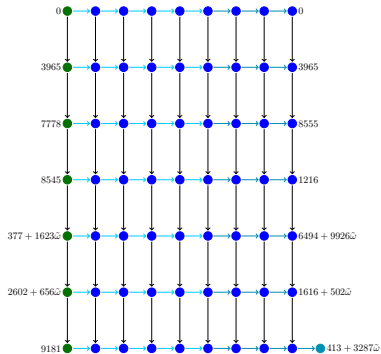
Alice secret key: (r_1^5, r_2^3, r_3^2)



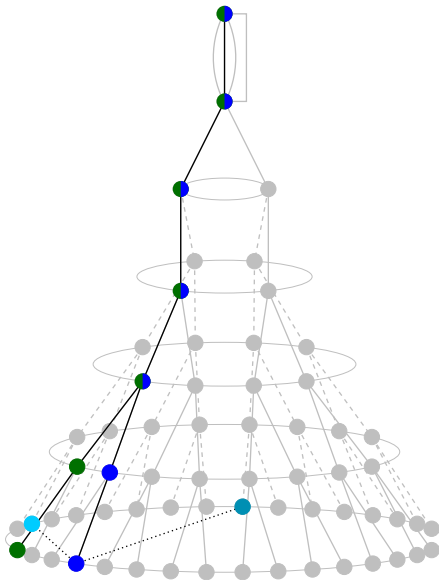
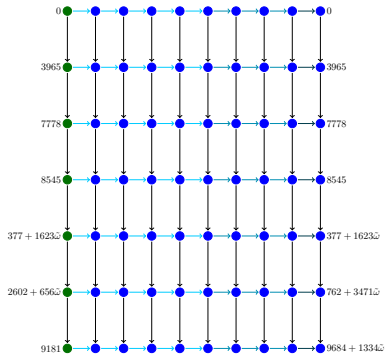
Alice secret key: $(\alpha_1^5, \alpha_2^3, \alpha_3^2)$



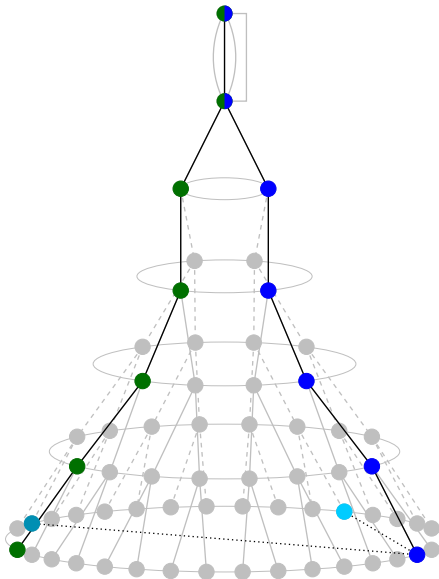
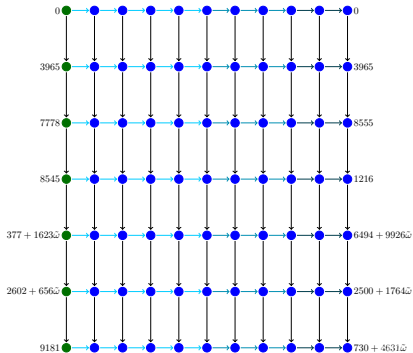
Alice secret key: $(\alpha_1^5, \alpha_2^3, \alpha_3^2)$



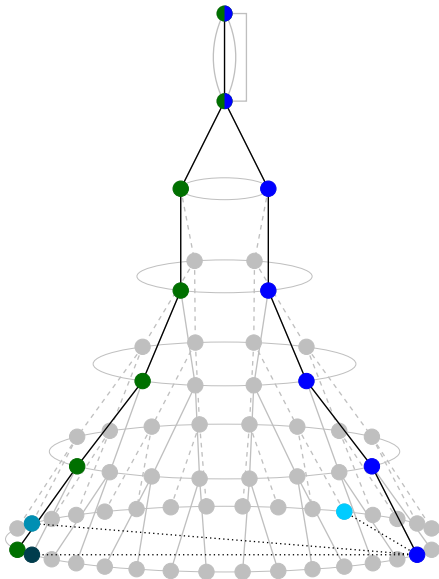
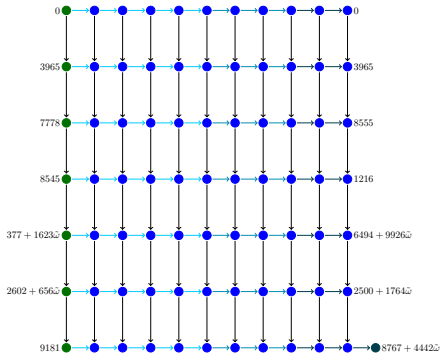
Alice secret key: $(\alpha_1^5, \alpha_2^3, \alpha_3^2)$



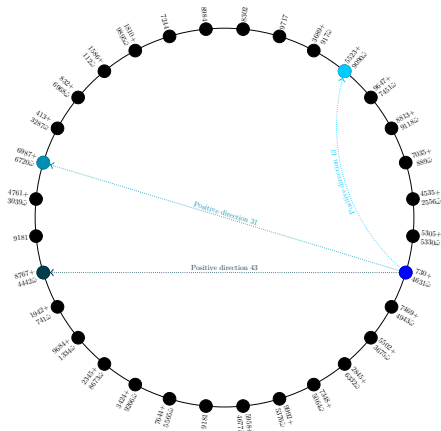
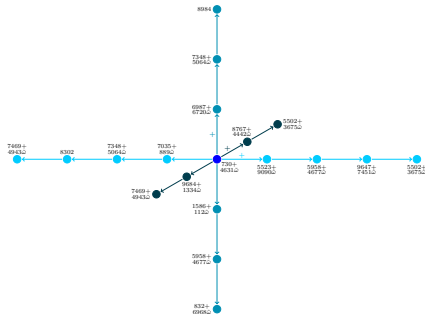
Alice secret key: $(r_1^5 r_2^3 r_3^2)$



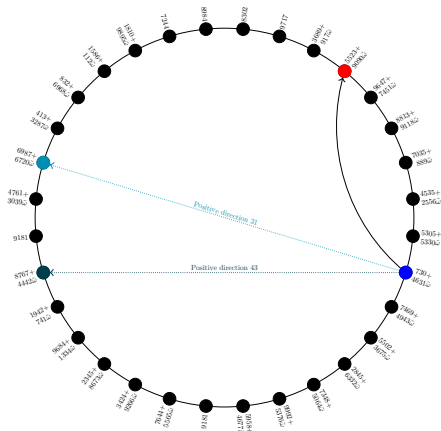
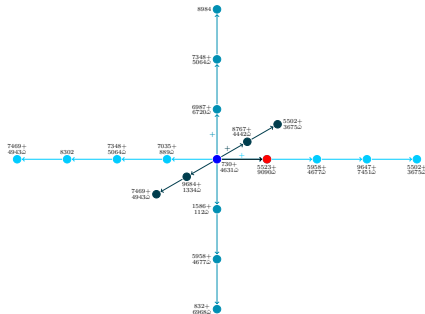
Alice secret key: (r_1^5, r_2^3, r_3^2)



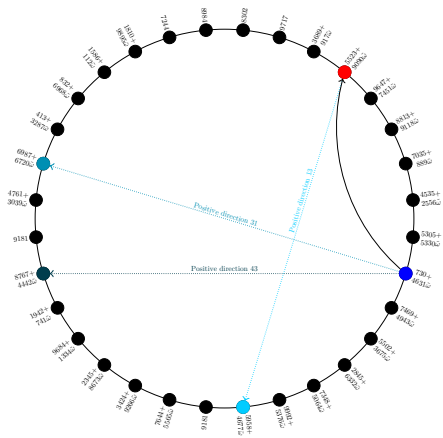
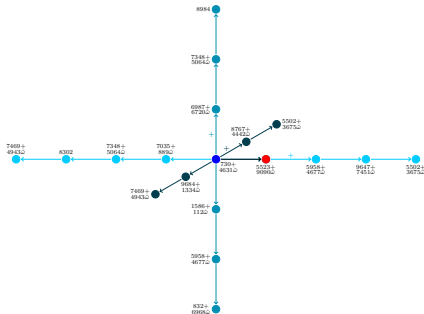
Bob secret key: $\begin{matrix} \color{orange}1^3 & \color{orange}2^2 & \color{orange}3^2 \\ \color{orange}1 & \color{orange}2 & \color{orange}3 \end{matrix}$



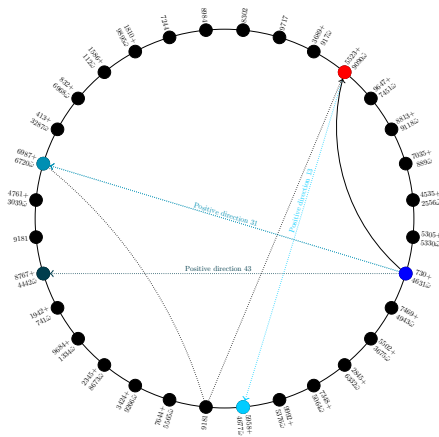
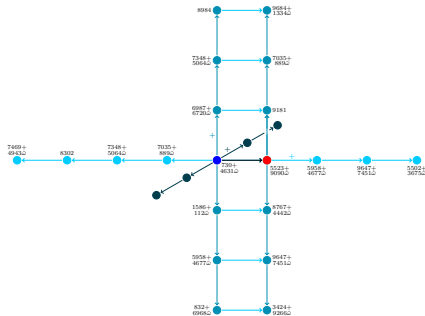
Bob secret key: $\begin{bmatrix} 1 & 3 \\ 1 & 2 \\ 2 & 3 \end{bmatrix}$



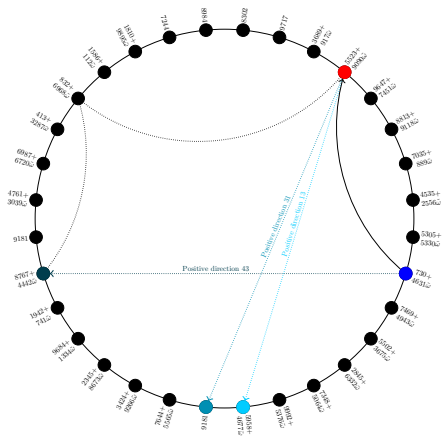
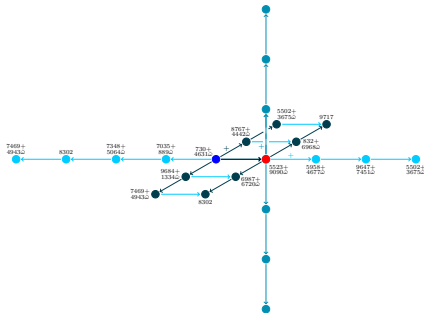
Bob secret key: $\begin{matrix} 1^3 & 1^2 & 1^2 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{matrix}$



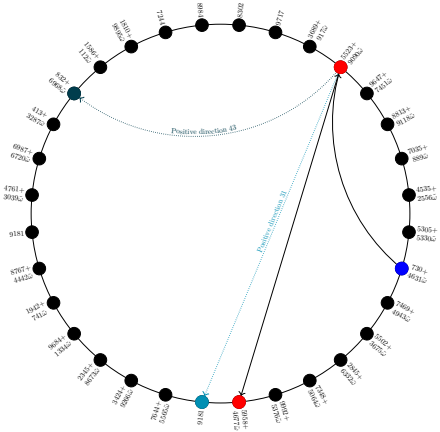
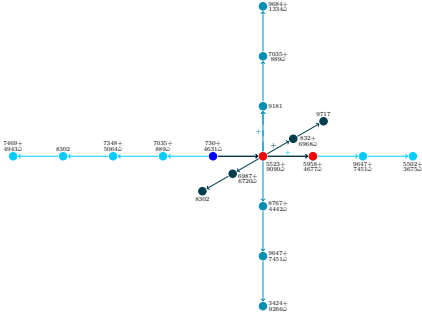
Bob secret key: $\begin{bmatrix} 3 \\ 1 \\ 2 \\ 3 \end{bmatrix}$



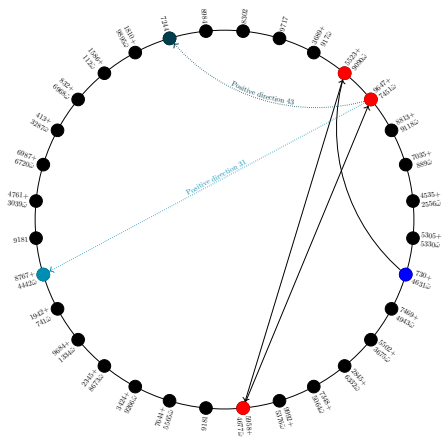
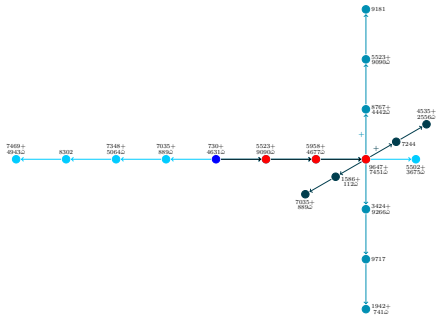
Bob secret key: $\begin{matrix} \color{orange} 1^3 & \color{orange} 1_2 & \color{orange} 2^3 \\ \color{orange} 1 & \color{orange} 2 & \color{orange} 3 \end{matrix}$



Bob secret key: $\begin{matrix} 1 & 2 & 3 \\ \hline 1 & 2 & 3 \end{matrix}$

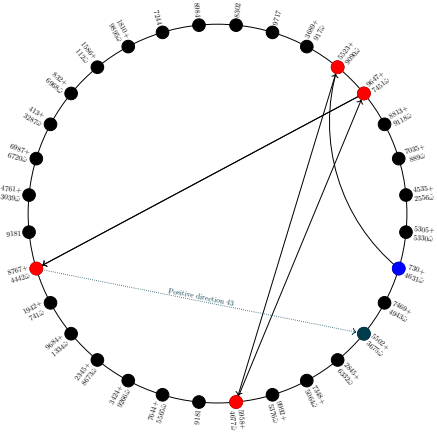
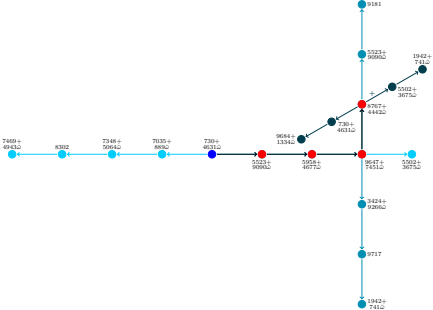


Bob secret key: $\begin{matrix} 1 & 2 & 3 \\ \color{orange} 1 & \color{orange} 2 & \color{orange} 3 \end{matrix}$



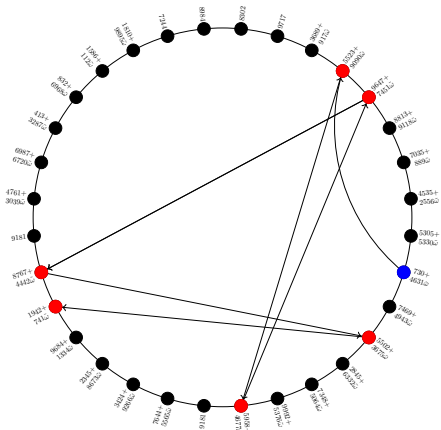
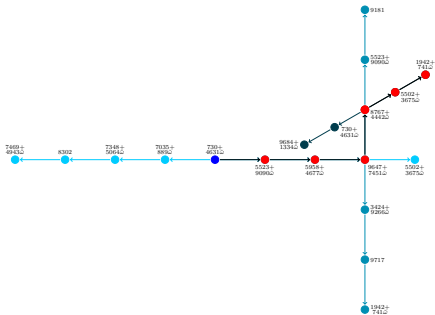
OSIDH PROTOCOL - AN EXAMPLE

Bob secret key: $\begin{matrix} 1^3 \\ 1^2 \\ 2^2 \\ 3^2 \end{matrix}$

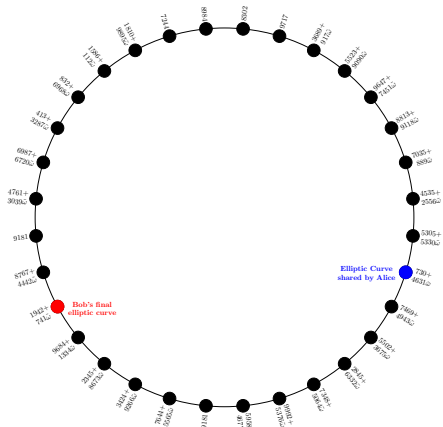
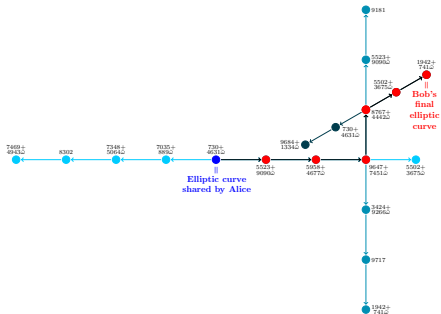


OSIDH PROTOCOL - AN EXAMPLE

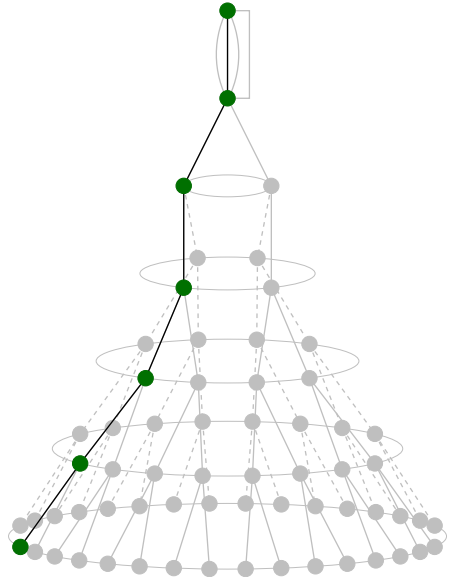
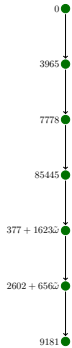
Bob secret key: $[L_1^3 L_2^2 L_3^2]$



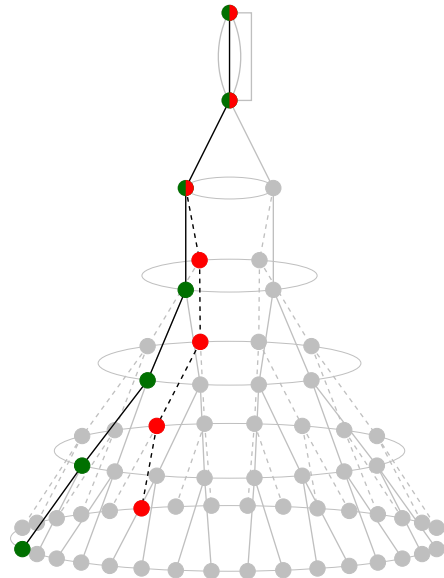
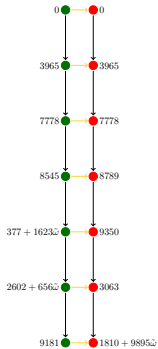
Bob secret key: $\begin{bmatrix} 1 & 3 \\ 1 & 2 \\ 1 & 3 \end{bmatrix}$



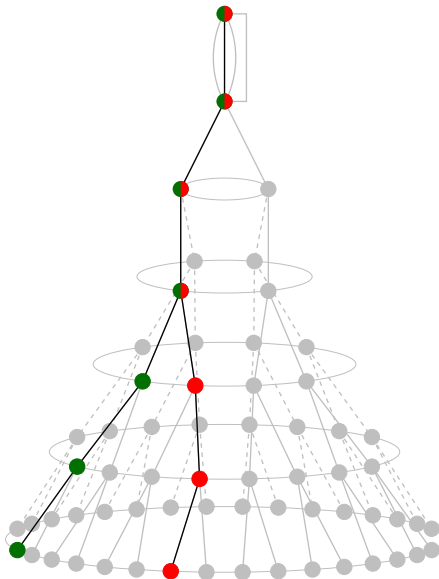
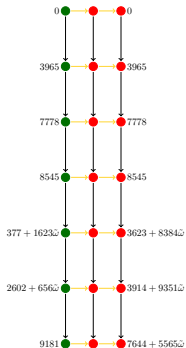
Bob secret key: $\{L_1^3, L_2^2, L_3^2\}$



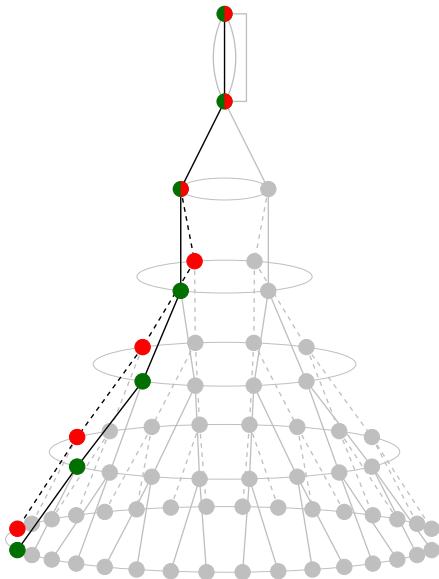
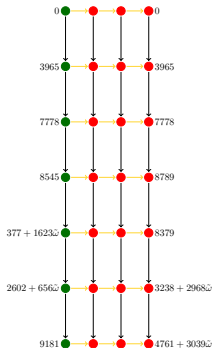
Bob secret key: $\begin{bmatrix} 1 & 3 \\ 1 & 2 \\ 2 & 3 \end{bmatrix}$



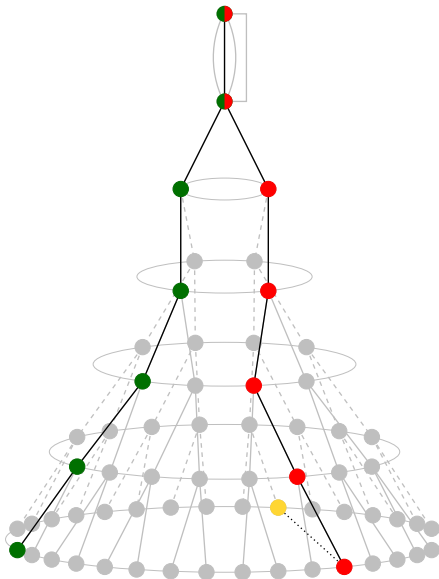
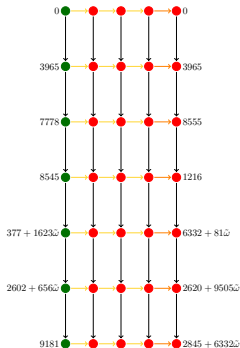
Bob secret key: $\begin{bmatrix} 1 & 3 \\ 1 & 2 \\ 3 & 2 \end{bmatrix}$



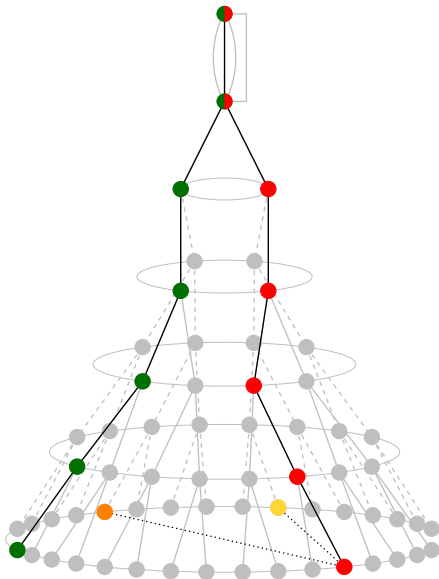
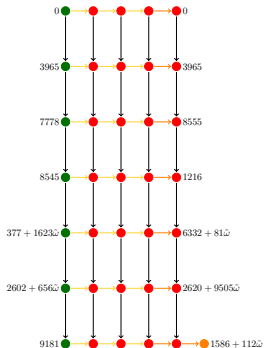
Bob secret key: $\begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}$



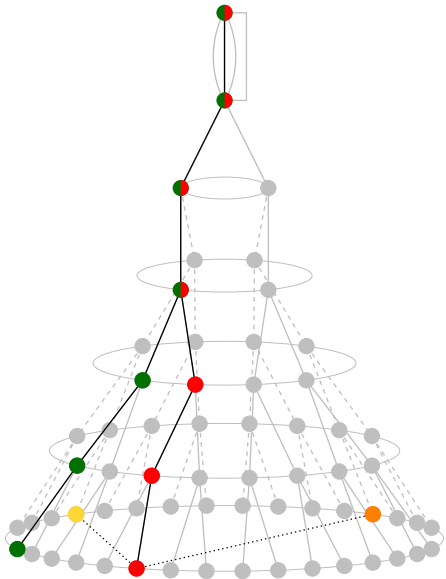
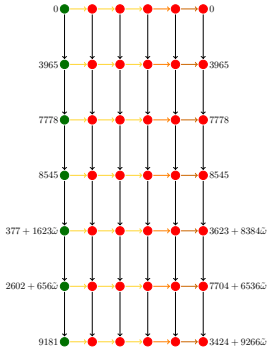
Bob secret key: $\begin{bmatrix} 1 & 3 \\ 1 & 2 \\ 3 & 2 \end{bmatrix}$



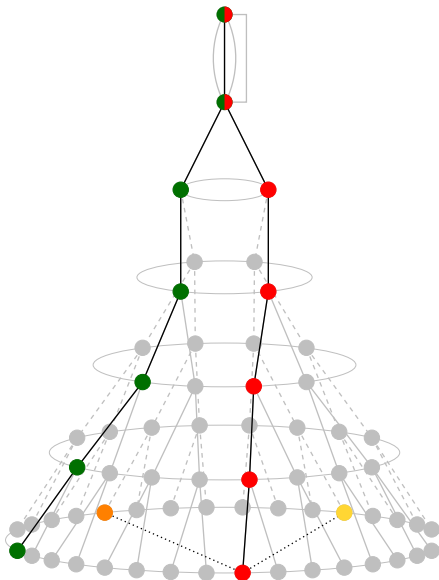
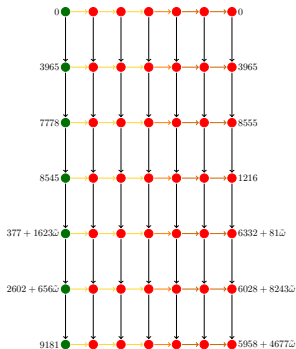
Bob secret key: $\begin{bmatrix} 1 & 3 \\ 1 & 2 \\ 3 & 2 \end{bmatrix}$



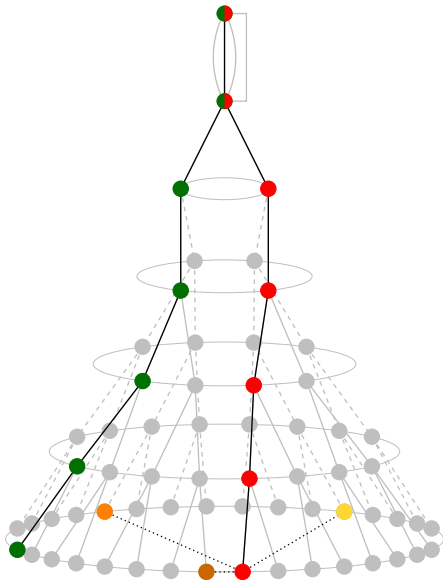
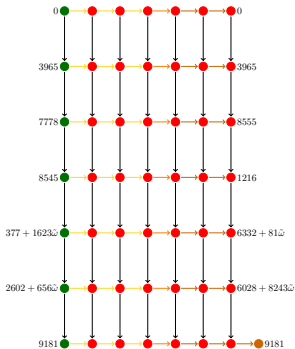
Bob secret key: (L_1^3, L_2^2, L_3^2)



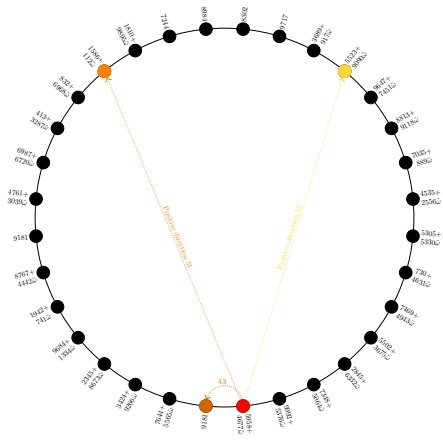
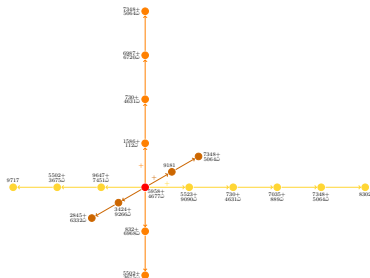
Bob secret key: $\begin{matrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 2 & 3 \end{matrix}$



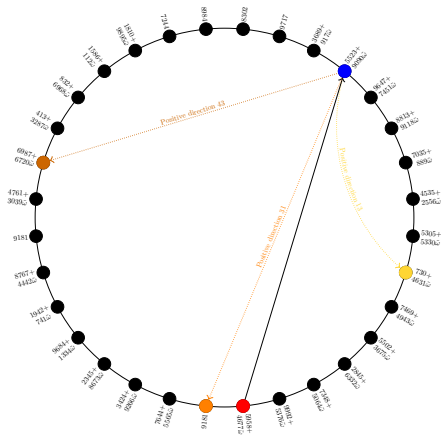
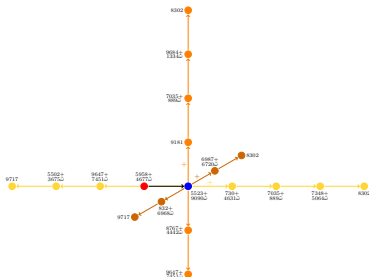
Bob secret key: $\begin{pmatrix} 1 & 3 \\ 1 & 2 \\ 2 & 3 \end{pmatrix}$



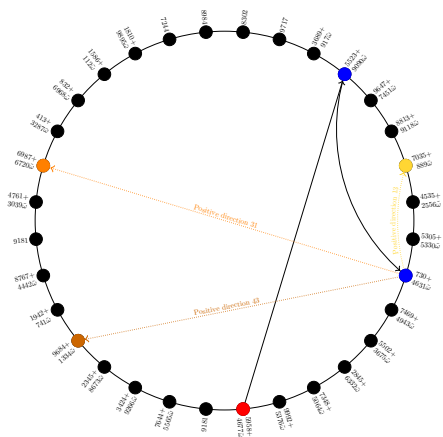
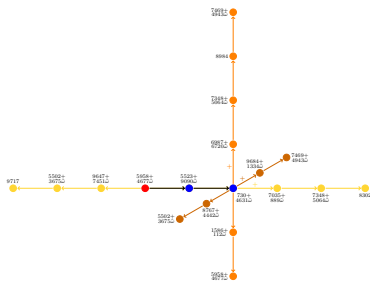
Alice secret key: $\begin{bmatrix} 5 \\ 1 \end{bmatrix} \begin{bmatrix} 3 \\ 2 \end{bmatrix} \begin{bmatrix} 2 \\ 3 \end{bmatrix}$



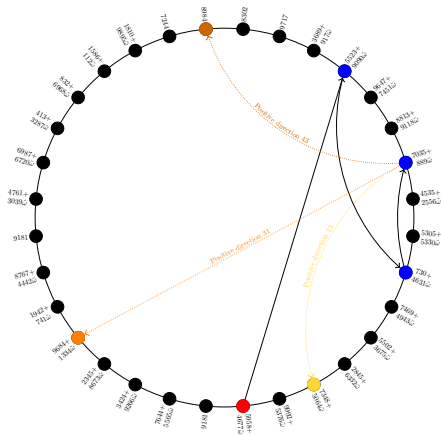
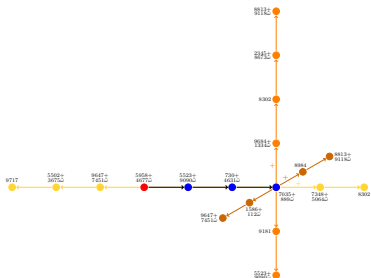
Alice secret key: $\begin{bmatrix} 5 \\ 1 \end{bmatrix} \begin{bmatrix} 3 \\ 2 \end{bmatrix} \begin{bmatrix} 2 \\ 3 \end{bmatrix}$



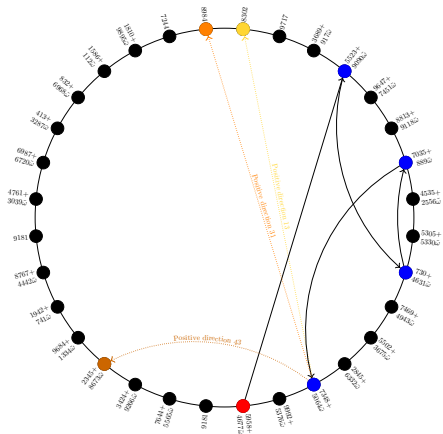
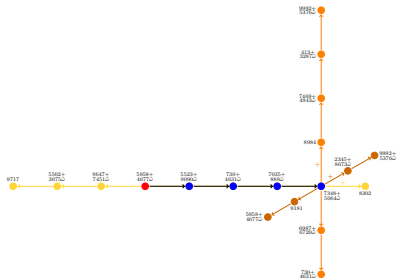
Alice secret key: $\begin{bmatrix} 5 & 1 & 3 \\ 1 & 2 & 2 \end{bmatrix}$



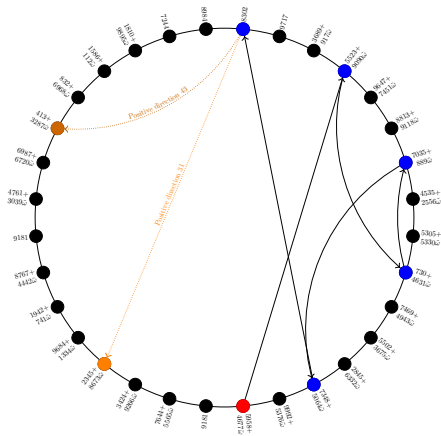
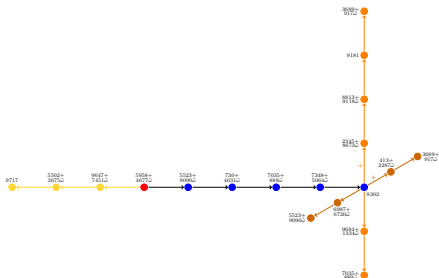
Alice secret key: $\begin{pmatrix} 5 & 1 \\ 3 & 2 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \end{pmatrix}$



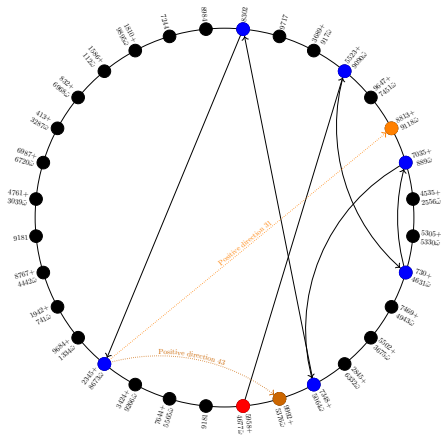
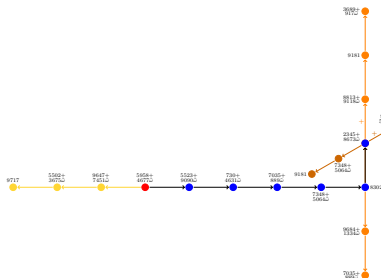
Alice secret key: $\begin{pmatrix} 5 & 1 \\ 1 & 2 \\ 3 & 2 \end{pmatrix}$



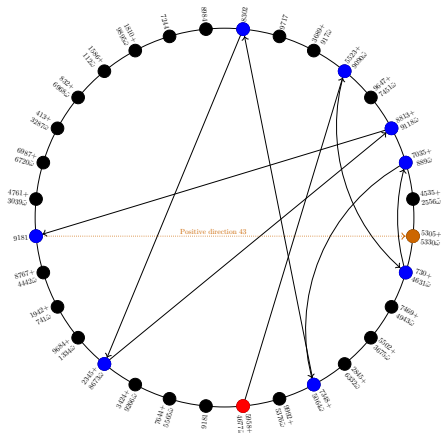
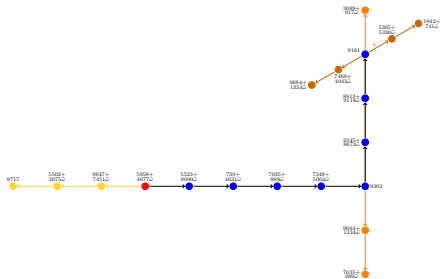
Alice secret key: $\begin{bmatrix} 5 \\ 1 \end{bmatrix} \begin{bmatrix} 3 \\ 2 \end{bmatrix} \begin{bmatrix} 2 \\ 3 \end{bmatrix}$



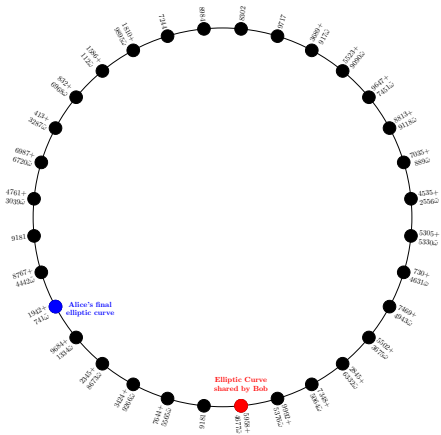
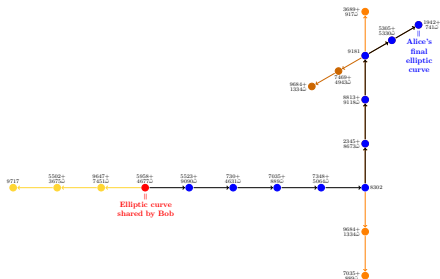
Alice secret key: $\begin{bmatrix} 5 & 3 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 2 \\ 3 \end{bmatrix}$



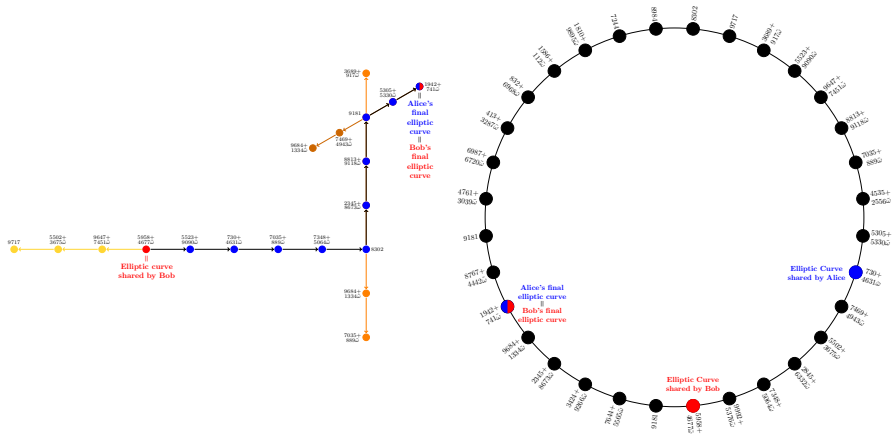
Alice secret key: $\begin{bmatrix} 5 \\ 1 \end{bmatrix} \begin{bmatrix} 3 \\ 2 \end{bmatrix} \begin{bmatrix} 2 \\ 3 \end{bmatrix}$



Alice secret key: $[1^5 1^3 2^3]$



OSIDH PROTOCOL - AN EXAMPLE



Endomorphism ring problem

Given a supersingular elliptic curve E/\mathbb{F}_{p^2} and $\pi = [p]$, determine

1. $\text{End}(E)$ as an abstract ring.
2. An explicit endomorphism $\phi \in \text{End}(E) - \mathbb{Z}$.
3. An explicit basis \mathfrak{B}^0 for $\text{End}^0(E)$ over \mathbb{Q} .

Endomorphism ring transfer problem

Given an isogeny chain $E_0 \rightarrow \dots \rightarrow E_n$ and $\text{End}(E_0)$, determine $\text{End}(E_n)$.

Endomorphism Generators Problem

Given a supersingular elliptic curve E/\mathbb{F}_{p^2} , an imaginary quadratic order \mathcal{O} admitting an embedding in $\text{End}(E)$ and a collection of compatible $(\mathcal{O}, \mathfrak{q}^n)$ -orientations of E for $(\mathfrak{q}, n) \in S$, determine

1. An explicit endomorphism $\phi \in \mathcal{O} \subseteq \text{End}(E)$
2. A generator ϕ of $\mathcal{O} \subseteq \text{End}(E)$

Consider an arbitrary supersingular endomorphism ring $\mathcal{O}_{\mathfrak{B}} \subset \mathfrak{B}$ with discriminant p^2 . There is a positive definite rank 3 quadratic form

$$\begin{array}{ccc} \text{disc} : \mathcal{O}_{\mathfrak{B}}/\mathbb{Z} & \longrightarrow & \mathbb{Z} \\ \wedge^2(\mathcal{O}_{\mathfrak{B}}) \supseteq \mathbb{Z} \wedge \mathcal{O}_{\mathfrak{B}} & \xrightarrow{\quad \alpha \longmapsto \quad} & |\text{disc}(\alpha)| = |\text{disc}(\mathbb{Z}[\alpha])| \end{array}$$

representing discriminants of orders embedding in $\mathcal{O}_{\mathfrak{B}}$.

The general order $\mathcal{O}_{\mathfrak{B}}$ has a reduced basis $1 \wedge \alpha_1, 1 \wedge \alpha_2, 1 \wedge \alpha_3$ satisfying

$$|\text{disc}(1 \wedge \alpha_i)| = \Delta_i \text{ where } \Delta_i \sim p^{2/3}$$

(Minkowski bound: $c_1 p^2 \leq \Delta_1 \Delta_2 \Delta_3 \leq c_2 p^2$).

In order to hide \mathcal{O}_n in $\mathcal{O}_{\mathfrak{B}}$ we impose

$$\ell^{2n} |\Delta_K| > c p^{2/3} \quad \Rightarrow \quad n \approx \frac{\log_{\ell}(p)}{3}$$

so that there is no special imaginary quadratic subring in $\mathcal{O}_{\mathfrak{B}} = \text{End}(E_n)$.

In order to have the action of $\mathcal{C}(\mathcal{O})$ cover a large portion of the supersingular elliptic curves, we require $\ell^n \sim p$, i.e., $n \sim \log_\ell(p)$.

- ▶ $\#SS_{\mathcal{O}}^{pr}(p) = h(\mathcal{O}_n) = \text{class number of } \mathcal{O}_n = \mathbb{Z} + \ell^n \mathcal{O}_K$.
- ▶ Class Number Formula

$$h(\mathbb{Z} + m\mathcal{O}_K) = \frac{h(\mathcal{O}_K)m}{[\mathcal{O}_K^\times : \mathcal{O}^\times]} \prod_{p|m} \left(1 - \left(\frac{\Delta_K}{p}\right) \frac{1}{p}\right)$$

- ▶ Units

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

- ▶ Number of Supersingular curves

$$\#\text{SS}(p) = \left[\frac{p}{12}\right] + \epsilon_p \quad \epsilon_p \in \{0, 1, 2\}$$

$$\text{Therefore, } h(\ell^n \mathcal{O}_K) = \frac{1 \cdot \ell^n}{2 \text{ or } 3} \left(1 - \left(\frac{\Delta_K}{\ell}\right) \frac{1}{\ell}\right) = \left[\frac{p}{12}\right] + \epsilon_p \implies p \sim \ell^n$$

SECURITY PARAMETERS - DEGREE OF PRIVATE WALKS

Suppose $E = E_n$ and F are two generic supersingular elliptic curves. Without an O_K -module structure we have a basis $\mathbf{Hom}(E, F) = \mathbb{Z}\psi_1 + \mathbb{Z}\psi_2 + \mathbb{Z}\psi_3 + \mathbb{Z}\psi_4$.

A reduced basis should satisfy $\deg(\psi_i) \approx \sqrt{p}$. In order that $\mathbb{Z}\psi_A$ is not a distinguished submodule of $\mathbf{Hom}(E, F)$, the private walk ψ_A should satisfy

$$\log_p(\deg(\psi_A)) \geq \frac{1}{2}$$

Again, we can think of the number of curves that we can reach: for a fixed degree m the number of curves that can be attained is

$$|\mathbb{P}(E[m])| \simeq |\mathbb{P}^1(\mathbb{Z}/m\mathbb{Z})| \approx m$$

The total number of isogenies of any degree d up to m is $\sum_{d=1}^m |\mathbb{P}(E[d])| \approx m^2$ but the choice of ψ_A is restricted to a subset of \mathcal{O} -oriented isogenies in $\mathcal{C}(\mathcal{O})$. Such isogenies are restricted to a class proportional to m .

Consequently, to cover a subset of p^λ classes, we need

$$\log_p(\deg(\psi_A)) \geq \lambda$$

In practice, rather than bounding the degree, for efficient evaluation one fixes a subset of small split primes, and the space of exponent vectors is bounded.

We choose exponents (e_1, \dots, e_r) in the space $I_1 \times \dots \times I_r \subset \mathbb{Z}^r$ where $I_j = [-m_j, m_j]$, defining ψ_A with kernel $E[\mathbf{p}_1^{e_1} \dots \mathbf{p}_r^{e_r}]$.

We want the map

$$\prod_{j=1}^r I_j \longrightarrow \mathcal{C}(\mathcal{O}) \longrightarrow \mathbf{SS}(p)$$

to be effectively injective - either injective or computationally hard to find a nontrivial element of the kernel in $(I_1 \times \dots \times I_r) \cap \ker(\mathbb{Z}^r \rightarrow \mathcal{C}(\mathcal{O}))$

In order to cover as many classes as possible, the latter should be nearly surjective. If the former map is injective with image of size p^λ in $\mathbf{SS}(p)$ this gives

$$p^\lambda < \prod_{j=1}^r (2m_j + 1) < |\mathcal{C}(\mathcal{O})| \approx \ell^n$$

for fixed $m = m_j$ this yields

$$n > r \log_\ell (2m + 1) > \lambda \log_\ell (p)$$

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 $\mathcal{C}l(\mathcal{O})$ 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.

The map from ℓ -isogeny chains to its terminus forgets the structure of the orientation, and the original curve E_0 , giving rise to a generic s.s. elliptic curve.

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 modular 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 .

Future directions:

- ▶ Security analysis and setting security parameters.
- ▶ Comparison with earlier protocols.
- ▶ Implementation and algorithmic optimization.
- ▶ Forgetful map.
- ▶ Use of canonical liftings.
- ▶ Higher dimensions.

Future directions:

- ▶ Security analysis and setting security parameters.
- ▶ Comparison with earlier protocols.
- ▶ Implementation and algorithmic optimization.
- ▶ Forgetful map.
- ▶ Use of canonical liftings.
- ▶ Higher dimensions.

MERCI POUR VOTRE ATTENTION