BORDEAUX, 14 MARCH 2023

L.COLÒ I2M

ORIENTED SUPERSINGULAR ELLIPTIC CURVES & CLASS GROUP ACTIONS

LEONARDO COLÒ & DAVID KOHEL
Institut de Mathématiques de Marseille

Séminaire LFANT

CONTENTS

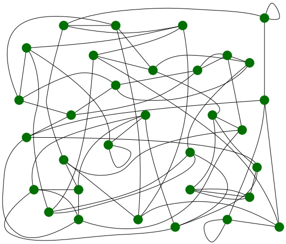
ORIENTATIONS AND CLASS GROUP ACTIONS

SUPERSINGULAR ISOGENY GRAPHS

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.



ORIENTATIONS

Let $\mathcal{O}$ be an order in an imaginary quadratic field K.
An $\mathcal{O}$-*orientation* on a supersingular elliptic curve E is an embedding

$$\iota : \mathcal{O} \hookrightarrow \mathrm{End}(E).$$

A K-*orientation* is an embedding

$$\iota : K \hookrightarrow \mathrm{End}^0(E) = \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

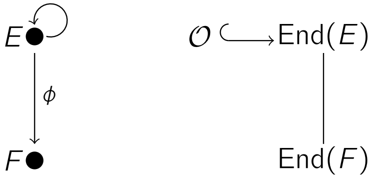
An $\mathcal{O}$-orientation is *primitive* if

$$\mathcal{O} \simeq \mathrm{End}(E) \cap \iota(K).$$

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.

ORIENTATIONS - ORIENTING ISOGENIES



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.

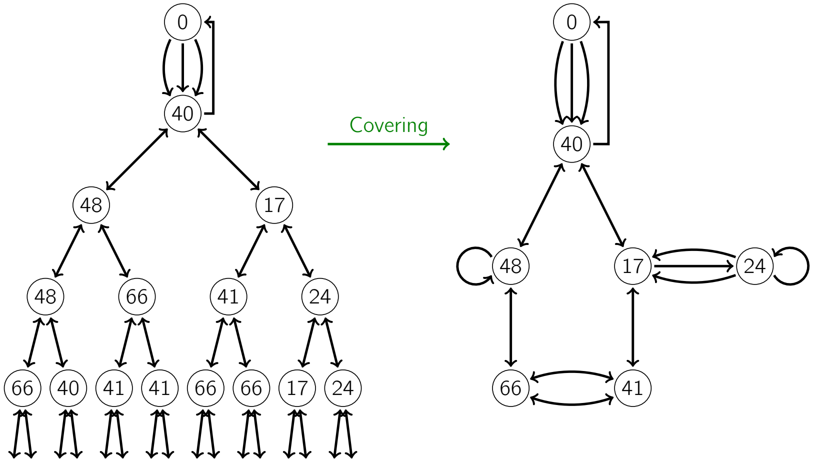
ORIENTED ISOGENY GRAPHS - VERTICES & EDGES

Two K-oriented curves are isomorphic if and only if there exists a K-oriented isomorphism between them.
We denote $G_S(E, K)$ the S-isogeny graph of K-oriented supersingular elliptic curves whose

- vertices are isomorphism classes of K-oriented supersingular elliptic curves
- edges are equivalence classes of K-oriented isogenies of degree in S.

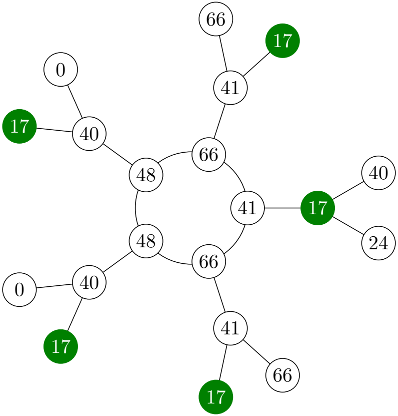
ORIENTED ISOGENY GRAPHS - AN EXAMPLE

Let $p = 71$ and $E_0/\mathbb{F}_{71}$ be the supersingular elliptic curve with $j(E) = 0$ oriented by the $\mathcal{O}_K = \mathbb{Z}[\omega]$, where $\omega^2 + \omega + 1 = 0$.
The orientation by $K = \mathbb{Q}[\omega]$ differentiates vertices in the descending paths from E_0, determining an infinite graph shown here to depth 4:



Oriented isogeny graphs - yet another example

We let again $p = 71$ and we consider the isogeny graph oriented by $\mathbb{Z}[\omega_{79}]$ where ω_{79} generates the ring of integers of $\mathbb{Q}(\sqrt{-79})$.



PRIMITIVE ORIENTATIONS

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

An element of $\mathrm{SS}^{pr}_{\mathcal{O}}(p)$ consists of

- A supersingular elliptic curve $E/\overline{\mathbb{F}}_p$;
- a primitive orientation $\iota : \mathcal{O} \hookrightarrow \mathrm{End}(E)$;
- a structure of a p-orientation which is a homomorphism $\rho : \mathcal{O} \to \overline{\mathbb{F}}_p$.

$$\rho : \mathcal{O} \longrightarrow \mathcal{O}/\mathfrak{p} \xrightarrow{\iota} \mathrm{End}(E)/\mathfrak{P} \hookrightarrow \overline{\mathbb{F}}_p$$

- $\mathrm{SS}^{pr}_{\mathcal{O}}(\rho) =$ set of oriented supersingular elliptic curves with ρ induced by ι.

CLASS GROUP ACTION

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

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

Proposition

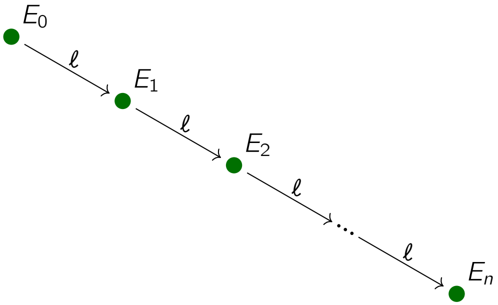
The set $\mathrm{SS}_{\mathcal{O}}^{pr}(\rho)$ is a torsor for the class group $\mathcal{C}\ell(\mathcal{O})$.

For fixed primitive p-oriented supersingular curve E, we get bijection of sets:

$$\mathcal{C}\ell(\mathcal{O}) \longrightarrow \mathrm{SS}_{\mathcal{O}}^{pr}(\rho)$$

EFFECTIVE CLASS GROUP ACTIONS

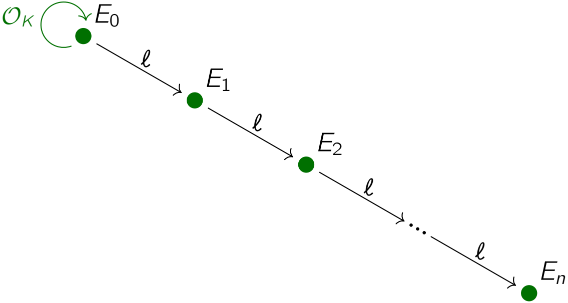
We consider an elliptic curve E_0 with an effective endomorphism ring (eg. $j_0 = 0, 1728$) and a chain of ℓ-isogenies.



EFFECTIVE CLASS GROUP ACTIONS

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

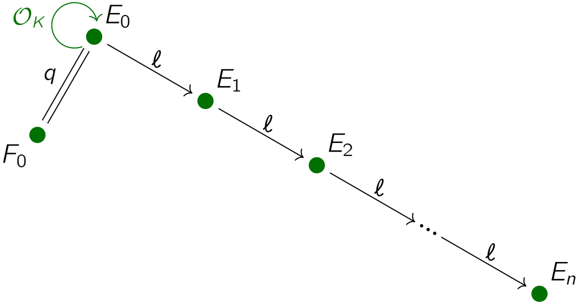
- For $\ell = 2$ (or 3) a suitable candidate for $\mathcal{O}_K$ could be the Gaussian integers $\mathbb{Z}[i]$ or the Eisenstein integers $\mathbb{Z}[\omega]$.



EFFECTIVE CLASS GROUP ACTIONS

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

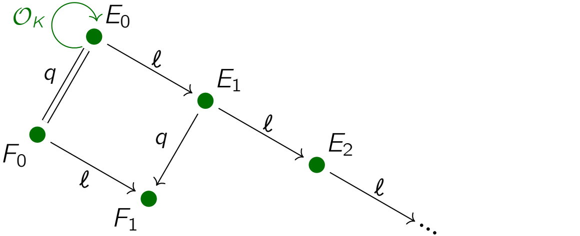
- Horizontal isogenies must be endomorphisms



EFFECTIVE CLASS GROUP ACTIONS

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

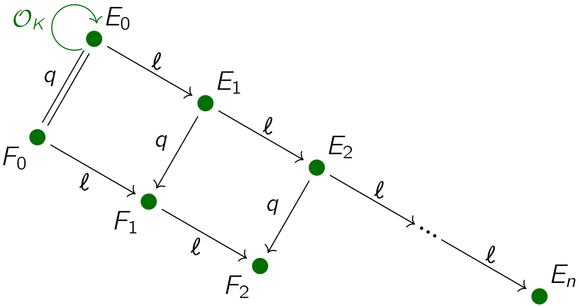
- We push forward our q-orientation obtaining F_1.



EFFECTIVE CLASS GROUP ACTIONS

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.

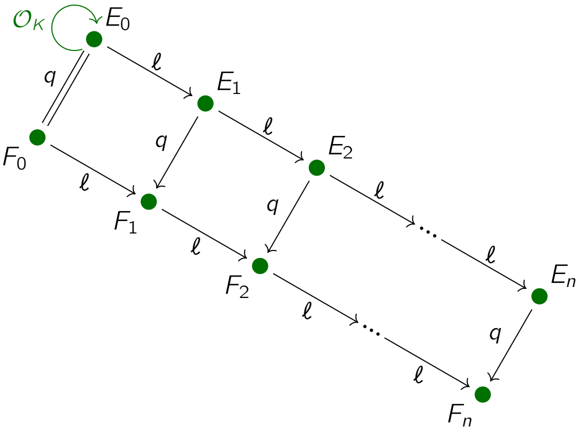


EFFECTIVE CLASS GROUP ACTIONS

L.COLÒ I2M

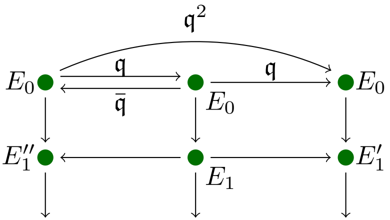
We consider an elliptic curve E_0 with an effective endomorphism ring (eg. $j_0 = 0, 1728$) and a chain of ℓ-isogenies.

- And again till F_n.



ADDING LEVEL STRUCTURE

DIFFERENTIATING CONJUGATE IDEAL CLASSES



$E_i' \neq E_i''$ 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 $\ell^{2i} \gg q^2$, we are guaranteed that $\mathfrak{q}^2$ is not principal.

INITIALIZING THE LADDER - AN EXAMPLE

L.COLÒ 1 2 M

Suppose $D_K = -3$, and $\ell = 2$; we note that for all $n \geq 3$, that

$$\mathcal{C}\ell(\mathcal{O}_n) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}$$

and in particular, $\mathcal{C}\ell(\mathcal{O}_n)[2]$ consist of the classes of binary quadratic forms

$$\{\langle 1, 0, |D_K|\ell^{2(n-1)}\rangle, \langle |D_K|, 0, \ell^{2(n-1)}\rangle, \langle \ell^2, \ell^2, n_1\rangle, \langle \ell^2|D_K|, \ell^2|D_K|, n_2\rangle\}.$$

For $n = 3$, the form $\langle 12, 12, 7\rangle$ reduces to $\langle 7, 2, 7\rangle$ and the reduced representatives are:

$$\{\langle 1, 0, 48\rangle, \langle 3, 0, 16\rangle, \langle 4, 4, 13\rangle, \langle 7, 2, 7\rangle\}.$$

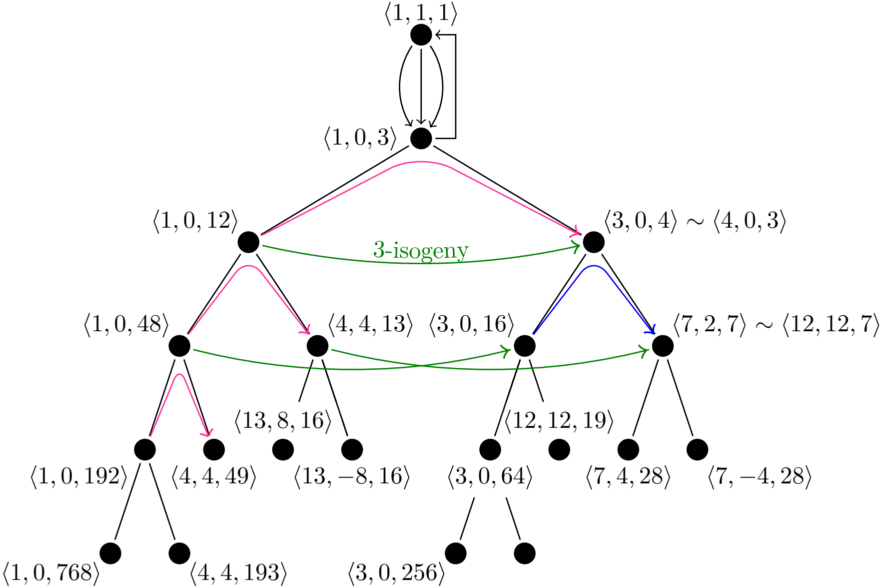
but for for $n \geq 4$, since $12 < n_2$, the forms

$$\{\langle 1, 0, 3 \cdot 4^{n-1}\rangle, \langle 3, 0, 4^{n-1}\rangle, \langle 4, 4, n_1\rangle, \langle 12, 12, n_2\rangle\}$$

are reduced.

INITIALIZING THE LADDER - A PICTURE

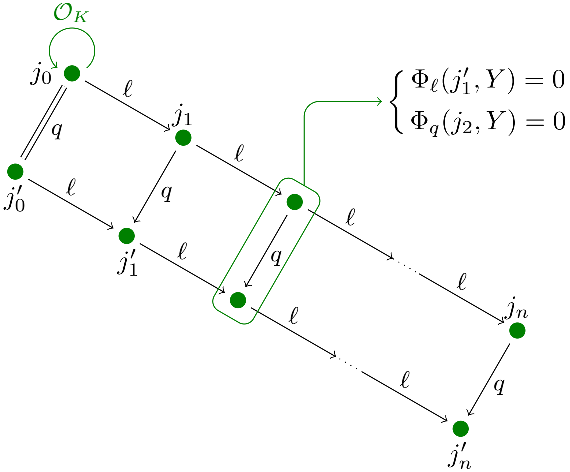
L.COLÒ I2M



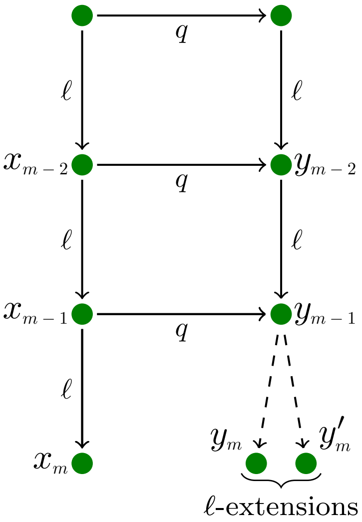
INITIALIZING THE LADDER - A TABLE

q	m	f_m	$[f_m]$	$[f_{m-1}]$
7	4	$\langle 7, 4, 28\rangle$	$[\langle 7, 4, 28\rangle]$	$[\langle 7, 2, 7\rangle]$
13	4	$\langle 13, 8, 16\rangle$	$[\langle 13, 8, 16\rangle]$	$[\langle 4, 4, 13\rangle]$
19	5	$\langle 19, 14, 43\rangle$	$[\langle 19, 14, 43\rangle]$	$[\langle 12, 12, 19\rangle]$
31	4	$\langle 31, 10, 7\rangle$	$[\langle 7, 4, 28\rangle]$	$[\langle 7, 2, 7\rangle]$
37	4	$\langle 37, 34, 13\rangle$	$[\langle 13, -8, 16\rangle]$	$[\langle 4, 4, 13\rangle]$
43	5	$\langle 43, 14, 19\rangle$	$[\langle 19, -14, 43\rangle]$	$[\langle 12, 12, 19\rangle]$
61	4	$\langle 61, 56, 16\rangle$	$[\langle 13, -8, 16\rangle]$	$[\langle 4, 4, 13\rangle]$
67	6	$\langle 67, 24, 48\rangle$	$[\langle 48, -24, 67\rangle]$	$[\langle 12, 12, 67\rangle]$
73	5	$\langle 73, 40, 16\rangle$	$[\langle 16, -8, 49\rangle]$	$[\langle 4, 4, 49\rangle]$
79	4	$\langle 79, 38, 7\rangle$	$[\langle 7, 4, 28\rangle]$	$[\langle 7, 2, 7\rangle]$
97	5	$\langle 97, 56, 16\rangle$	$[\langle 16, 8, 49\rangle]$	$[\langle 4, 4, 49\rangle]$
103	4	$\langle 103, 46, 7\rangle$	$[\langle 7, -4, 28\rangle]$	$[\langle 7, 2, 7\rangle]$
109	4	$\langle 109, 70, 13\rangle$	$[\langle 13, 8, 16\rangle]$	$[\langle 4, 4, 13\rangle]$
127	4	$\langle 127, 116, 28\rangle$	$[\langle 7, 4, 28\rangle]$	$[\langle 7, 2, 7\rangle]$

COMPLETING SQUARES OF ISOGENIES



EXTENDING THE LADDER



Let $\ell = 2$.

- The two ℓ-extensions are determined by a quadratic polynomial (deduced from y_{m-1}, y_{m-2}:

$$\phi_\ell(y) = 0$$

  We can solve for y_m, y'_m, its roots.

- We have a degree $q+1$ polynomial $\phi_q(y) = 0$ determined by x_m but we do note need to compute it. It suffices

$$\phi_q(y) \mod \phi_\ell(y)$$

  Indeed

$$\Phi_q(x, y) \equiv \phi_q(y) \mod (x - x_m, \phi_\ell(y))$$

ADDING LEVEL STRUCTURE

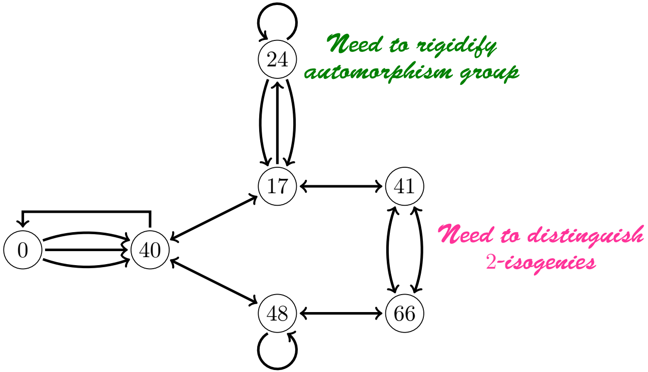
There are multiple reasons to add level structure to our construction:

- With an ℓ-level structure, the extension of ℓ-isogenies by modular correspondences allows one to automatically remove the dual isogeny (backtracking): there are ℓ rather than $\ell + 1$ extensions.

ADDING LEVEL STRUCTURE

There are multiple reasons to add level structure to our construction:

- With an ℓ-level structure, the extension of ℓ-isogenies by modular correspondences allows one to automatically remove the dual isogeny (backtracking): there are ℓ rather than $\ell + 1$ extensions.
- The modular isogeny chain is a potentially-non injective image of the isogeny chain.



ADDING LEVEL STRUCTURE

There are multiple reasons to add level structure to our construction:

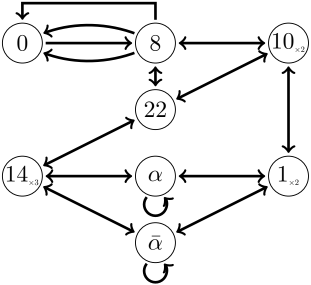
- With an ℓ-level structure, the extension of ℓ-isogenies by modular correspondences allows one to automatically remove the dual isogeny (backtracking): there are ℓ rather than $\ell + 1$ extensions.
- The modular isogeny chain is a potentially-non injective image of the isogeny chain.
- Rigidifying automorphisms should also shorten the distance to which we need to go in order to differentiate 2 points (two torsion of $\mathcal{C}\ell(\mathcal{O})$ may lift to non 2-torsion point in $\mathcal{C}\ell(\mathcal{O}, \Gamma)$).

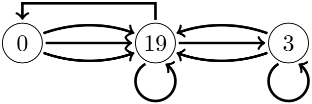
ADDING LEVEL STRUCTURE

There are multiple reasons to add level structure to our construction:

- With an ℓ-level structure, the extension of ℓ-isogenies by modular correspondences allows one to automatically remove the dual isogeny (backtracking): there are ℓ rather than $\ell + 1$ extensions.
- The modular isogeny chain is a potentially-non injective image of the isogeny chain.
- Rigidifying automorphisms should also shorten the distance to which we need to go in order to differentiate 2 points (two torsion of $\mathcal{Cl}(\mathcal{O})$ may lift to non 2-torsion point in $\mathcal{Cl}(\mathcal{O}, \Gamma)$).
- q-modular polynomial of higher level are smaller.

For any congruence subgroup Γ of level coprime to the characteristic, we have a covering $G_S(E,\Gamma) \to G_S(E)$ whose vertices are pairs $(E, \Gamma(P,Q))$ of supersingular elliptic curves/$\mathbb{F}_{p^2}$ and a Γ-level structure, and edges are isogenies $\psi : (E,\Gamma(P,Q)) \to (E',\Gamma(P',Q'))$ such that $\psi(\Gamma(P,Q)) = \Gamma(P',Q')$.



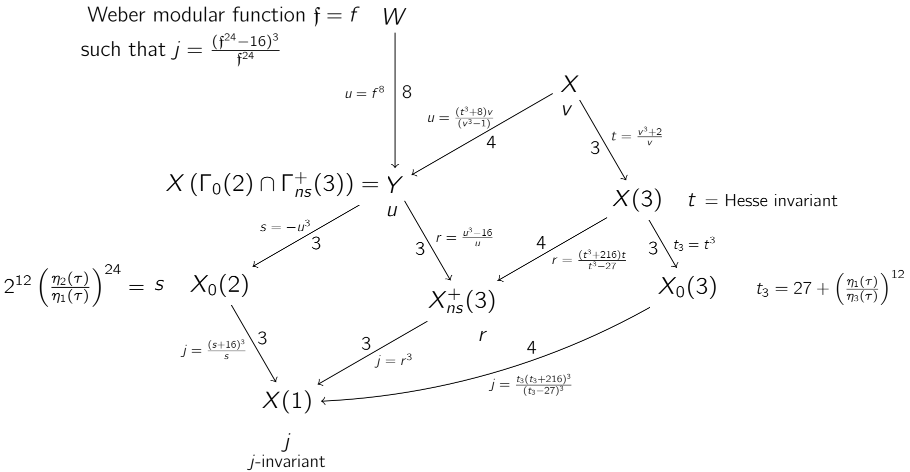


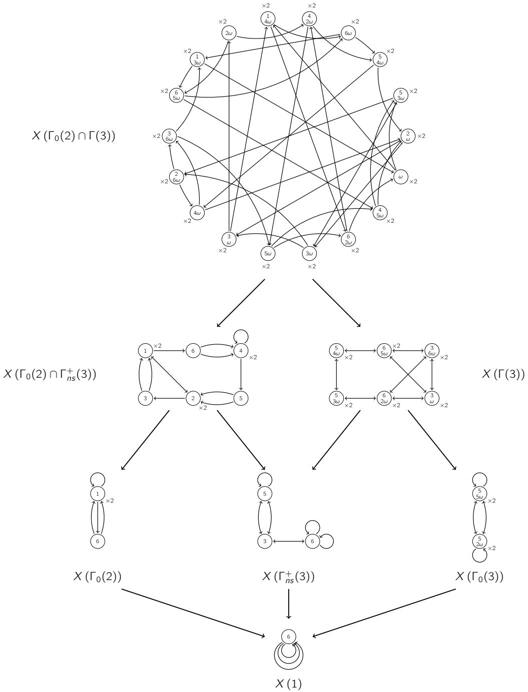
Eg. $\Gamma_0(N)$-structures.
Vertices (E, G) with $G \leq E[N]$ of order N
$\mathrm{End}(E, G) = \{\alpha \in \mathrm{End}(E) \,|\, \alpha(G) \subseteq G\}$ isomorphic to Eichler order.

On the left the $\Gamma_0(3)$ supersingular 2-isogeny graph.

$14 \leftrightarrow \{(E_0, G_1), (E_0, G_2), (E_0, G_3)\}$ where G_1, G_2, G_3 maps to each other under the automorphism of E_0; they define 3 isogenies to E_3.

SOME MODULAR CURVES OF INTEREST





X (Γ0(2) ∩ Γ(3))
X (Γ0(2) ∩ Γ+ns(3))
X (Γ(3))
X (Γ0(2))
X (Γ+ns(3))
X (Γ0(3))
X (1)

WEBER INITIALIZATIONS

Let u be a supersingular value of the Weber function,

$$r = u^3 \qquad t = -u^8 \qquad s = t^3$$

along the chain $\mathcal{W}_8 \to Y \to X_0(2)$.We get

$$\Psi_2(x,y) = (x^2 - y)y + 16x \qquad \Psi_3(x,y) = x^4 - x^3y^3 + 8xy + y^4$$

The elliptic curves associated to Weber invariants are the fiber in the family:

$$y^2 + xy = x^3 - \frac{1}{u^{24} - 64}x$$

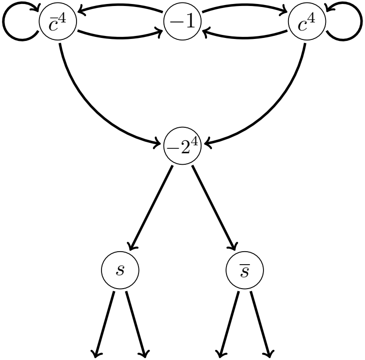
over u on the Weber curve.

The initial values with which to build the public ℓ-isogeny chains are

D	j_0	s_0	t_0	D	j_1	s_1	t_1
-3	0	-2^4	$-(\sqrt[3]{2})^4$	-12	$2^4 15^3$	-2^8	$-(\sqrt[3]{2})^8$
-4	12^3	2^3	2	-16	66^3	2^9	2^3
-7	-15^3	-1	-1	-28	255^3	-2^{12}	-2^4
-8	20^3	2^6	2^2	-32	j_1	t_1^3	$2^3(\sqrt{2}+1)$

WEBER INITIALIZATIONS - DISCRIMINANT −7

Endomorphism ring is small: generated by an endomorphism of degree 2 we avoid any pathologies associated with the extra automorphisms.

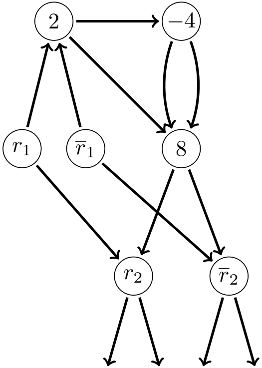


- $t_0 = -1$ and c root of $x^2 - x + 2$.
- c^4 and $\bar{c}^4$ also t-values over $j = -15^3$.
- $\Psi_2(-1, c^4) = \Psi_2(-1, \bar{c}^4) = 0$, the two extensions correspond to the horizontal 2-isogenies.
- $\Psi_2(c^4, c^4) = \Psi_2(c^4, -2^4) = 0$: the former enters a cycle the latter induces a descending isogeny.

Initialization: $(t_0, t_1, t_2, \ldots)$ beginning with $(-1, c^4, -2^4, \ldots)$.
Successive solutions to $\Psi_2(t_i, t_{i+1}) = 0$ are necessarily descending.
Extension: random choice of root t_{i+1} of $\Psi_2(t_i, x)$.

WEBER INITIALIZATIONS - DISCRIMINANT -4

L.COLÒ I2M

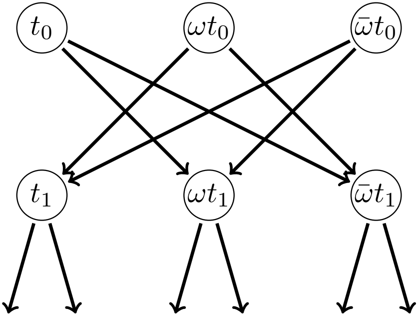


- t-invariants over $j = 12^3$ fall in two orbits of points, $\{2, 2\omega, 2\omega^2\}$ of multiplicity 2, and $\{-4, -4\omega, -4\omega^2\}$ of multiplicity 1.
- These points at the surface are linked by a 2-isogeny and to 2-depth 1, to $t = 8$.
- $\Psi_2(\omega x, \omega^2 y) = \omega\Psi_2(x, y)$: the choice of representative in the orbit gives rise to one of three distinct components of the 2-isogeny graph.

Initialization: $(t_0, t_1, t_2, \dots) = (2, 8, 8c, \dots)$ where c is a root of $x^2 - 8x - 2$.
Extension: random selection of a root t_{i+1} of $\Psi_2(t_i, x)$.

The full 2-isogeny graph has ascending edges from the depth one to $t_0 = 2$
If an isogeny is descending its only extension to a 2-isogeny chain is descending

WEBER INITIALIZATIONS - DISCRIMINANT −3



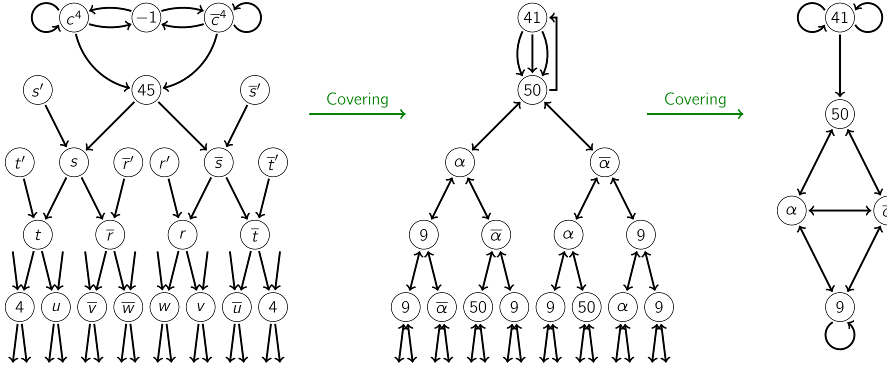
- $t_0 = -(\sqrt[3]{2})^4 = -2\sqrt[3]{2}$.
- $\{t_0, t_0\omega, t_0\omega^2\}$ are t-values over $j = 0$, each of multiplicity 3
- $t_1 = -t_0^2$, and $\Psi_2(t_0, t_1\omega) = \Psi_2(t_0, t_1\omega^2) = 0$,

Since 2 is inert, every path from t_0 is descending, so we may initialize the 2-isogeny chain with $(t_0, t_1\omega)$.

There are additional t-invariants at each depth > 0 which admit ascending and descending isogenies.
Any descending isogenies must rejoin this graph of descending isogenies from the surface.

WEBER INITIALIZATIONS - AN EXAMPLE OF GRAPHS

We orient the supersingular 2-isogeny graph in characteristic 61 by $\mathbb{Q}(\sqrt{-7})$ and we then climb the Weber modular tower.



OSIDH

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

ALICE	**BOB**

OSIDH PROTOCOL

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

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

OSIDH PROTOCOL

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

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

OSIDH PROTOCOL

L.COLÒ I2M

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

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

OSIDH PROTOCOL

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

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

OSIDH PROTOCOL

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

	ALICE	**BOB**
Choose integers in a bound $[-r, r]$	$(e_1, \ldots, e_t)$	$(d_1, \ldots, d_t)$
Construct an isogenous curve	$F_n = E_n / E_n \left[\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_t^{e_t}\right]$	$G_n = E_n / E_n \left[\mathfrak{p}_1^{d_1} \cdots \mathfrak{p}_t^{d_t}\right]$
Precompute all directions $\forall i$	$F_{n,i}^{(-r)} \leftarrow F_{n,i}^{(-r+1)} \leftarrow \ldots \leftarrow F_{n,i}^{(1)} \leftarrow F_n$	$G_{n,i}^{(-r)} \leftarrow G_{n,i}^{(-r+1)} \leftarrow \ldots \leftarrow G_{n,i}^{(1)} \leftarrow G_n$
... and their conjugates	$F_n \to F_{n,i}^{(1)} \to \ldots \to F_{n,i}^{(r-1)} \to F_{n,1}^{(r)}$	$G_n \to G_{n,i}^{(1)} \to \ldots \to G_{n,i}^{(r-1)} \to G_{n,1}^{(r)}$
Exchange data	G_n+directions	F_n+directions

OSIDH PROTOCOL

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

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

OSIDH PROTOCOL

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

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

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

OSIDH PROTOCOL - AN EXAMPLE

$\boldsymbol{p = 10007}$

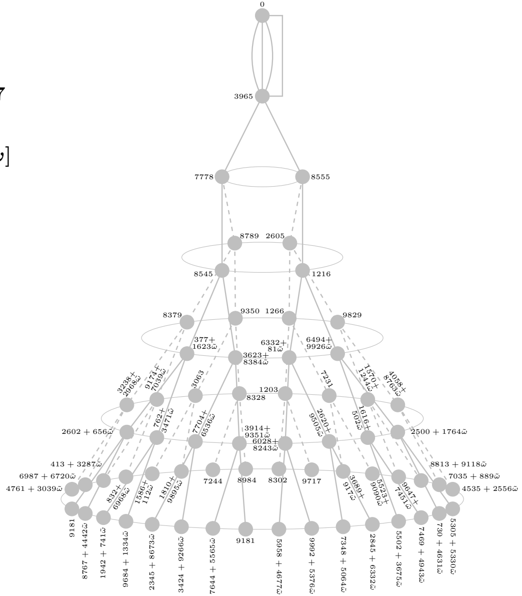
$\boldsymbol{\ell = 2}$

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

$\boldsymbol{\ell_1 = 13}$

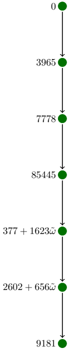
$\boldsymbol{\ell_2 = 31}$

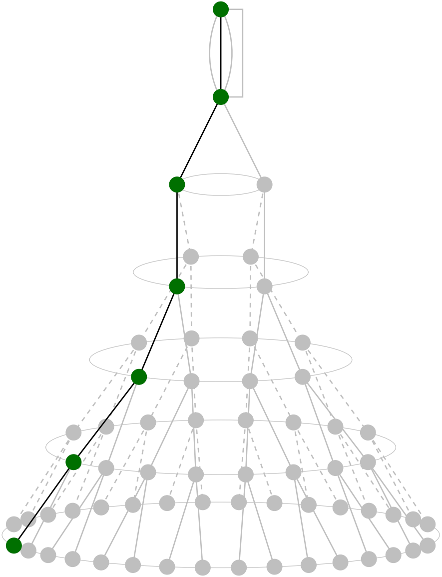
$\boldsymbol{\ell_3 = 43}$



OSIDH PROTOCOL - AN EXAMPLE

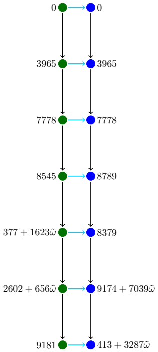
Alice secret key: $\mathfrak{l}_1^5\mathfrak{l}_2^3\mathfrak{l}_3^2$

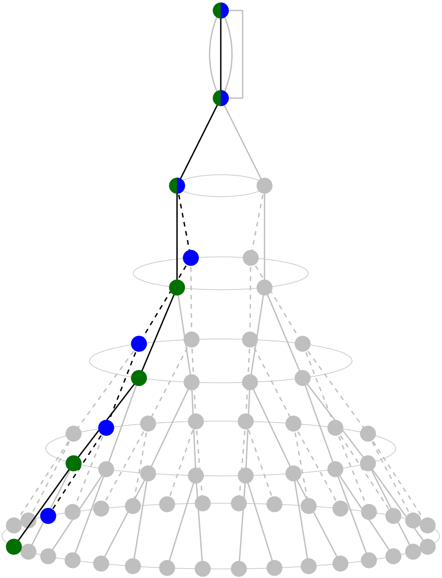




OSIDH PROTOCOL - AN EXAMPLE

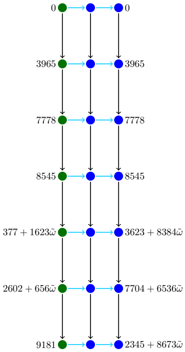
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$

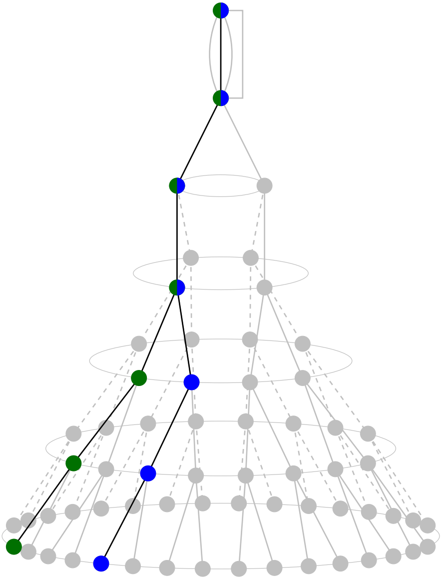




OSIDH PROTOCOL - AN EXAMPLE

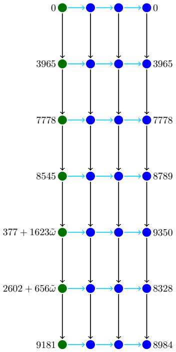
Alice secret key: $\mathfrak{l}_1^5\mathfrak{l}_2^3\mathfrak{l}_3^2$

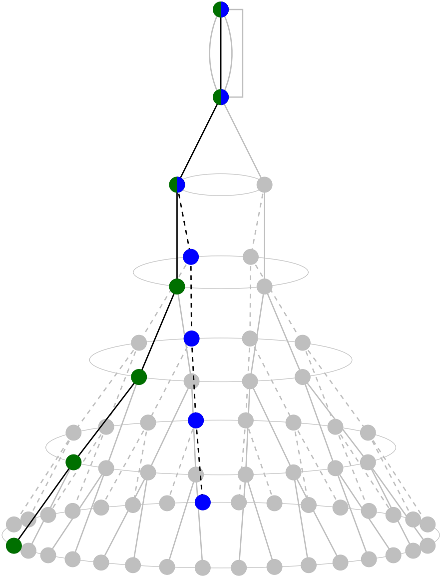




OSIDH PROTOCOL - AN EXAMPLE

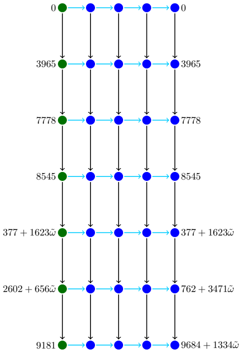
Alice secret key: $\mathfrak{l}_1^5\mathfrak{l}_2^3\mathfrak{l}_3^2$

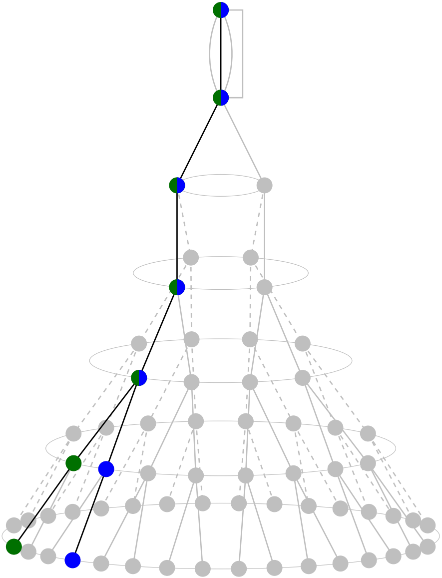




OSIDH PROTOCOL - AN EXAMPLE

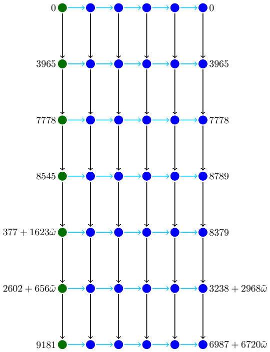
Alice secret key: $\mathfrak{l}_1^5\mathfrak{l}_2^3\mathfrak{l}_3^2$

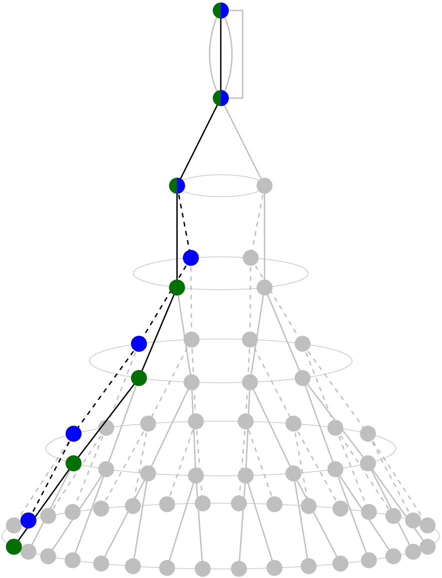




OSIDH PROTOCOL - AN EXAMPLE

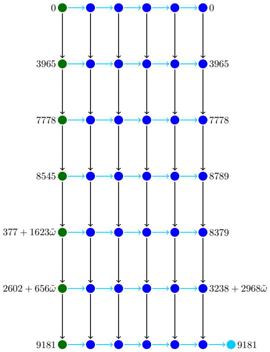
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$

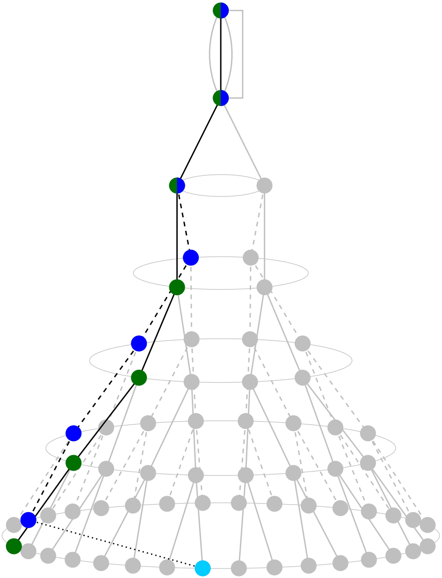




OSIDH PROTOCOL – AN EXAMPLE

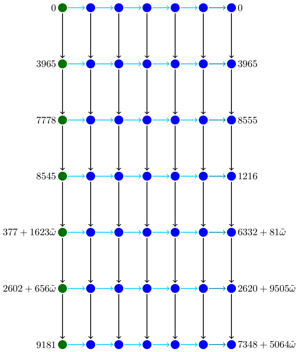
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$

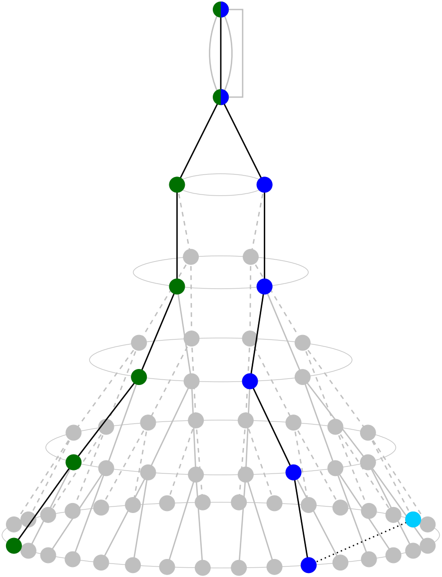




OSIDH PROTOCOL - AN EXAMPLE

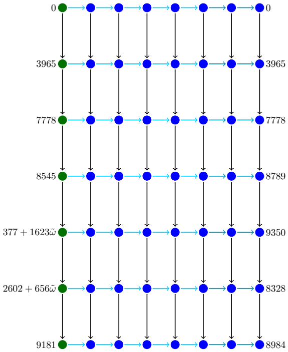
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$

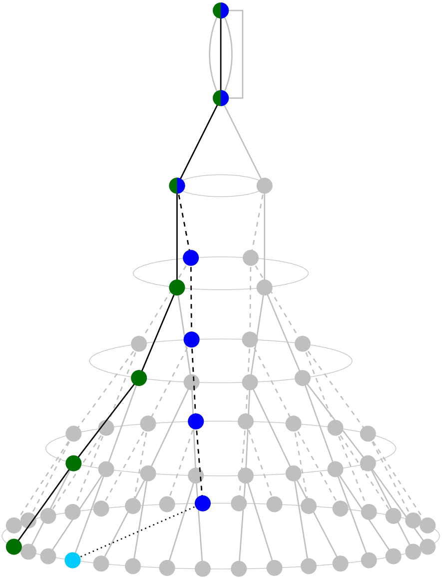




OSIDH PROTOCOL – AN EXAMPLE

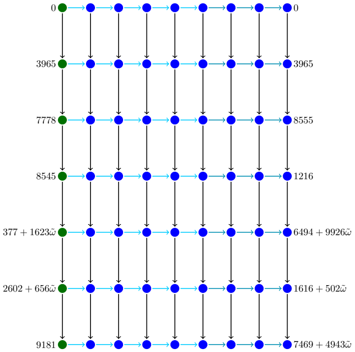
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$

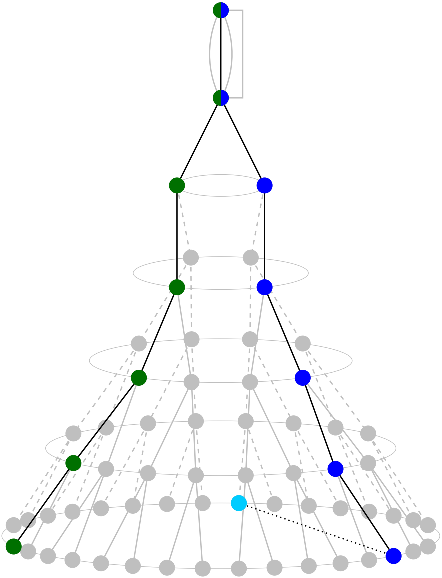




OSIDH PROTOCOL - AN EXAMPLE

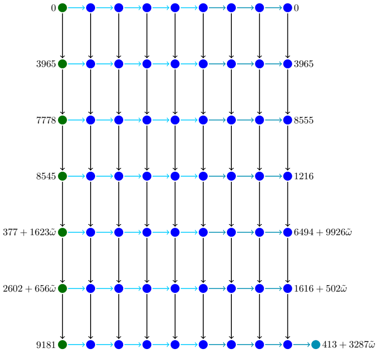
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$

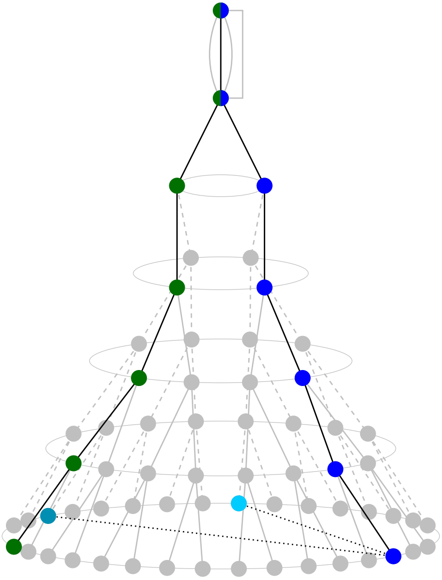




OSIDH PROTOCOL – AN EXAMPLE

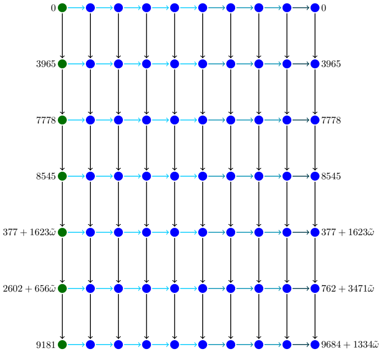
Alice secret key: $\mathfrak{l}_1^5\,\mathfrak{l}_2^3\,\mathfrak{l}_3^2$

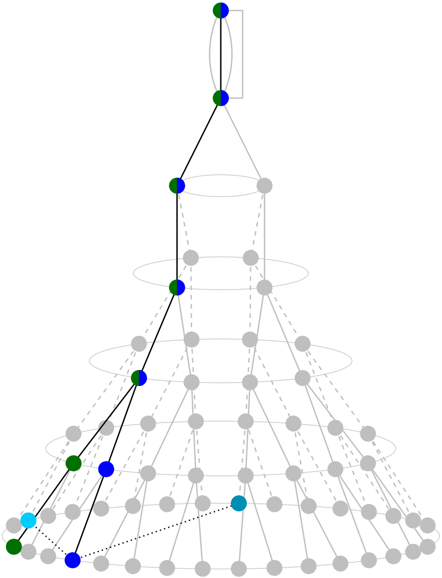




OSIDH PROTOCOL – AN EXAMPLE

Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$

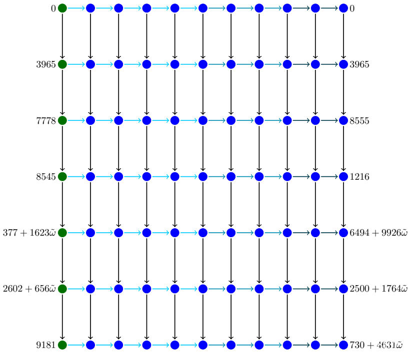


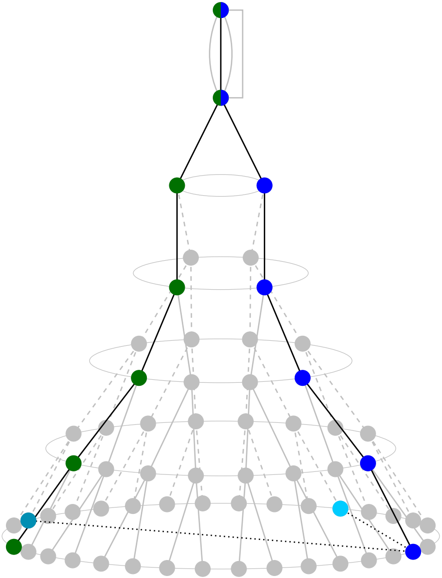


OSIDH PROTOCOL - AN EXAMPLE

L.COLÒ I2M

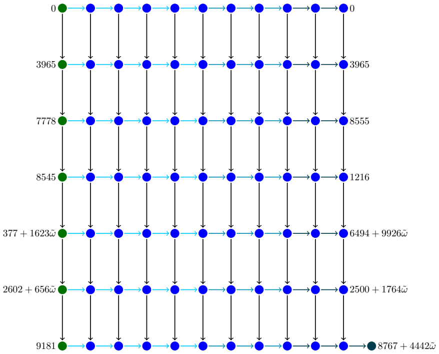
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$

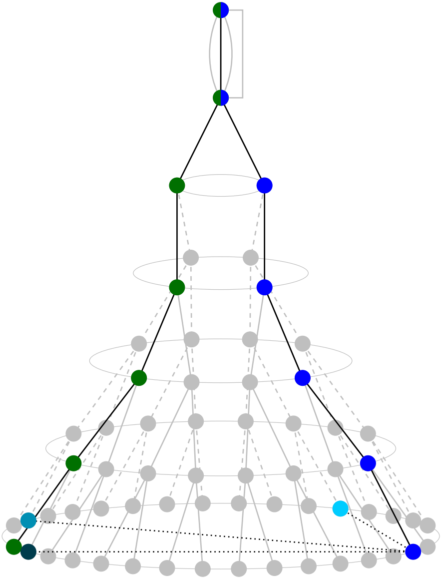




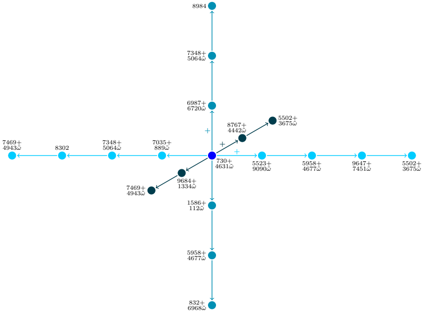
OSIDH PROTOCOL - AN EXAMPLE

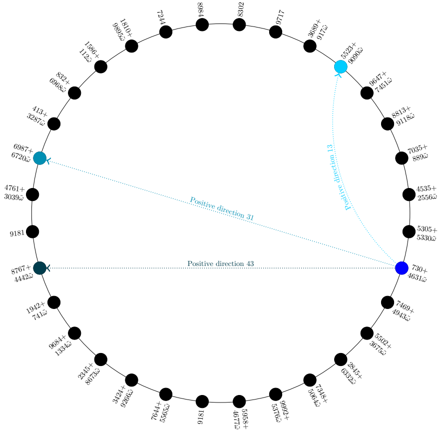
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$



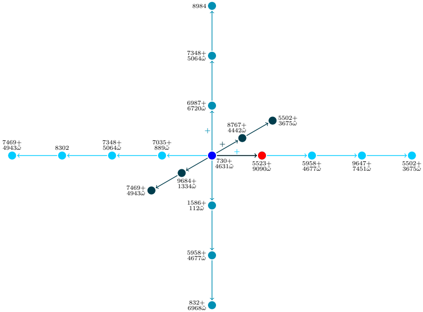


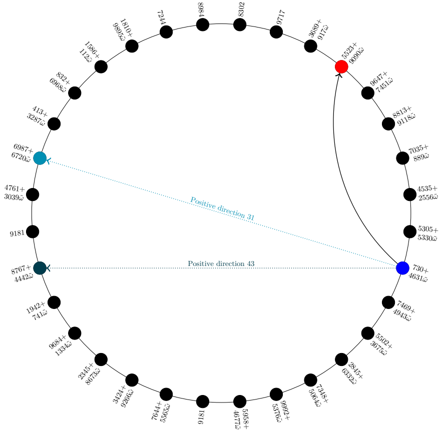
Bob secret key: $\mathfrak{l}_1^3 \mathfrak{l}_2 \mathfrak{l}_3^2$





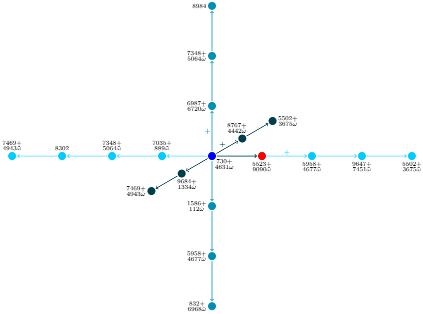
Bob secret key: $\mathfrak{l}_1^3 \mathfrak{l}_2 \mathfrak{l}_3^2$

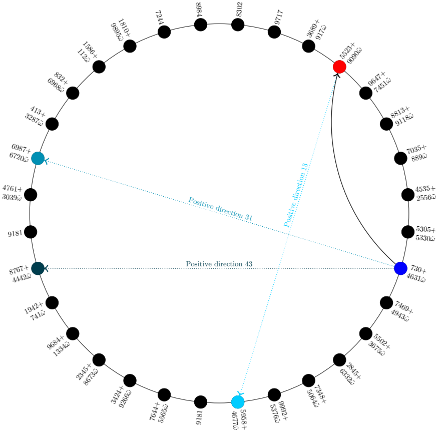




OSIDH PROTOCOL - AN EXAMPLE

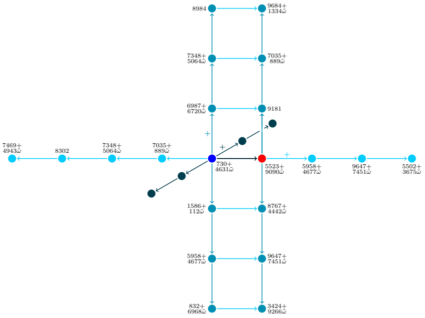
Bob secret key: $\mathfrak{l}_1^3 \mathfrak{l}_2 \mathfrak{l}_3^2$

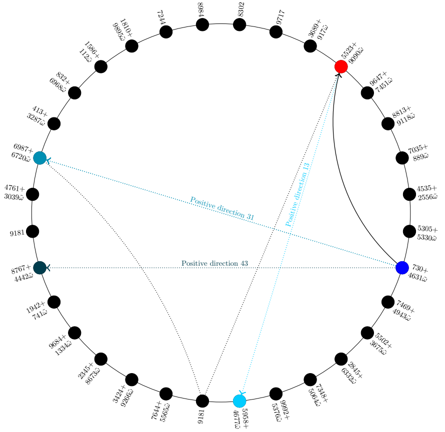




OSIDH PROTOCOL - AN EXAMPLE

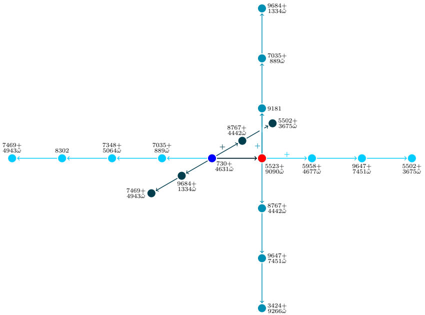
Bob secret key: $\mathfrak{l}_1^3 \mathfrak{l}_2 \mathfrak{l}_3^2$

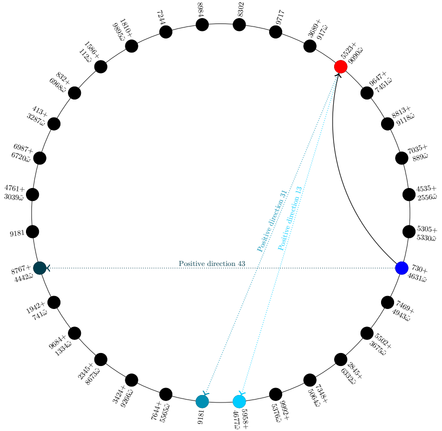




OSIDH PROTOCOL - AN EXAMPLE

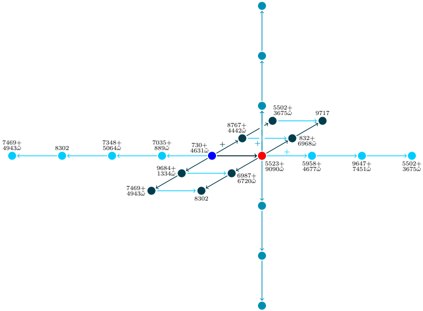
Bob secret key: $\mathfrak{l}_1^3 \mathfrak{l}_2 \mathfrak{l}_3^2$

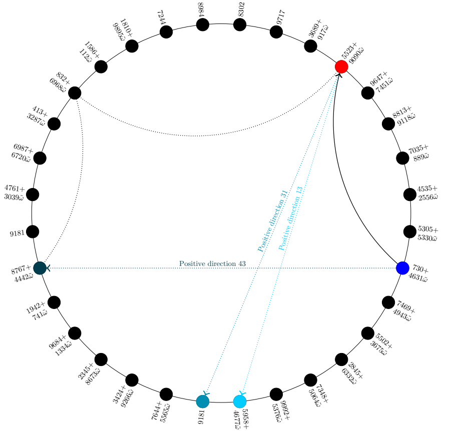




OSIDH PROTOCOL - AN EXAMPLE

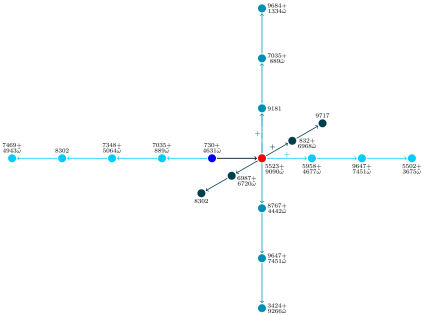
Bob secret key: $\mathfrak{l}_1^3 \mathfrak{l}_2 \mathfrak{l}_3^2$

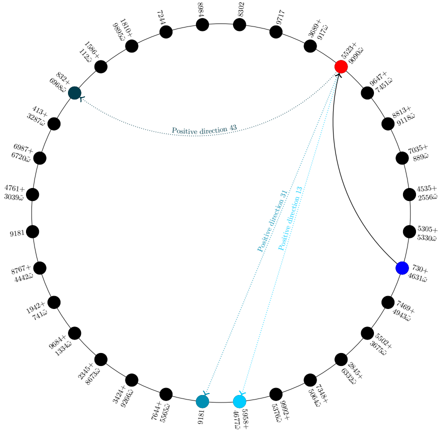




OSIDH PROTOCOL - AN EXAMPLE

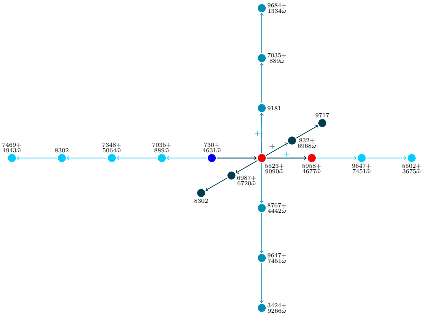
Bob secret key: $\mathfrak{l}_1^3 \mathfrak{l}_2 \mathfrak{l}_3^2$

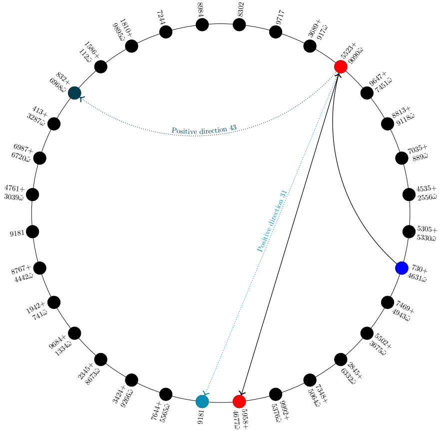




OSIDH PROTOCOL - AN EXAMPLE

Bob secret key: $\mathfrak{l}_1^3\,\mathfrak{l}_2\,\mathfrak{l}_3^2$

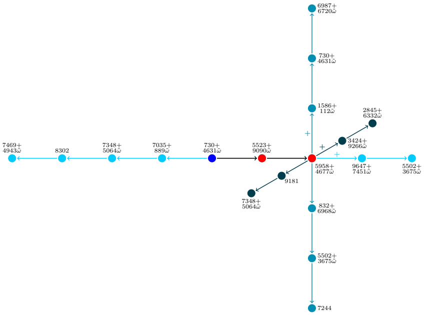


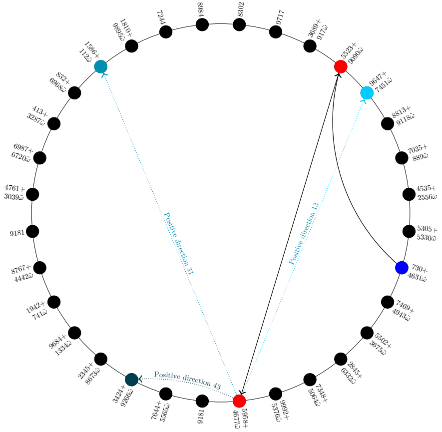


OSIDH PROTOCOL - AN EXAMPLE

L.COLÒ I2M

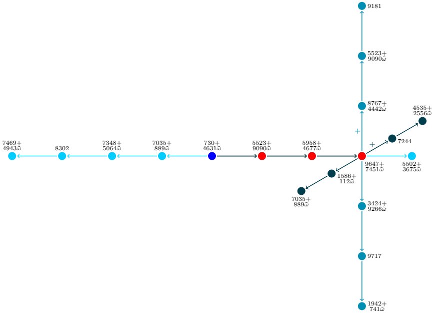
Bob secret key: $\mathfrak{l}_1^3 \mathfrak{l}_2 \mathfrak{l}_3^2$

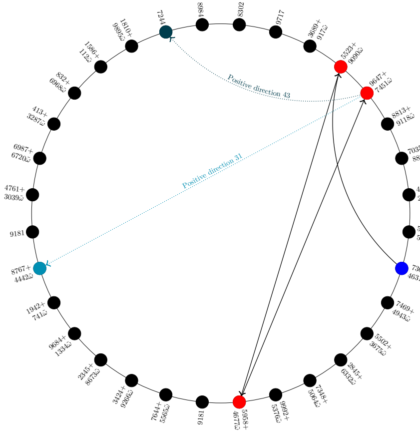




OSIDH PROTOCOL - AN EXAMPLE

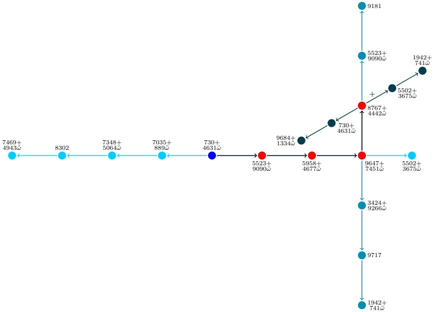
Bob secret key: $\mathfrak{l}_1^3 \mathfrak{l}_2 \mathfrak{l}_3^2$

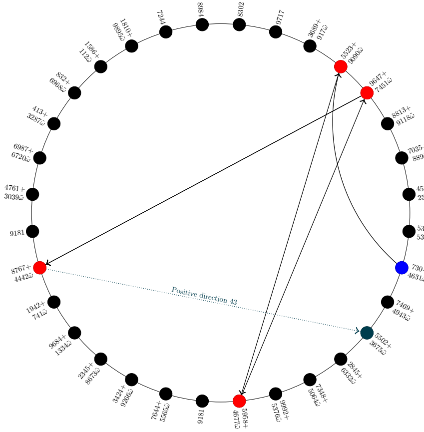




OSIDH PROTOCOL - AN EXAMPLE

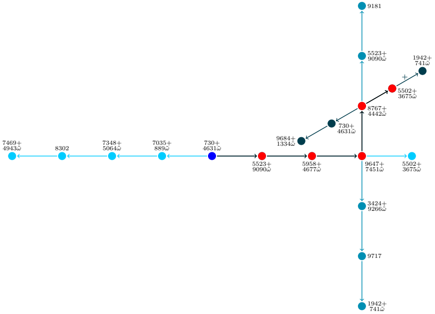
Bob secret key: $\mathfrak{l}_1^3 \mathfrak{l}_2 \mathfrak{l}_3^2$

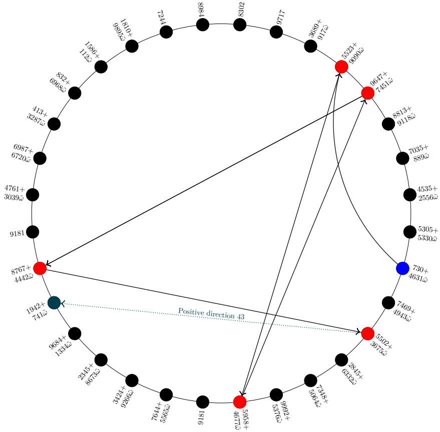




OSIDH PROTOCOL - AN EXAMPLE

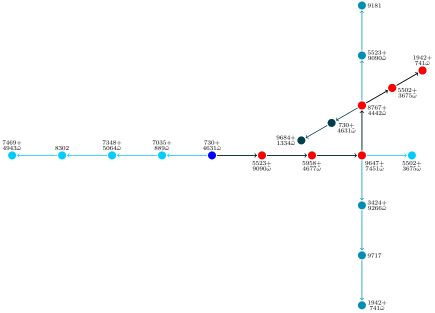
Bob secret key: $\mathfrak{l}_1^3\mathfrak{l}_2\mathfrak{l}_3^2$

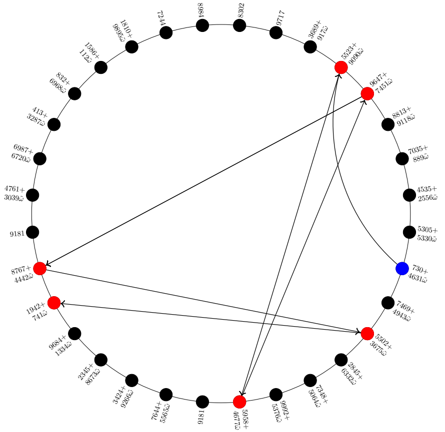




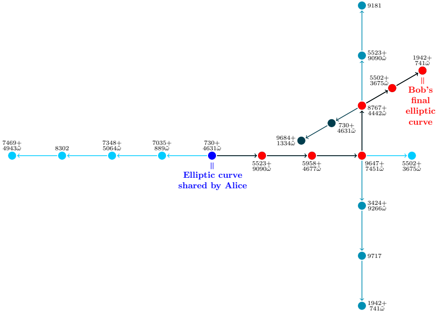
OSIDH PROTOCOL - AN EXAMPLE

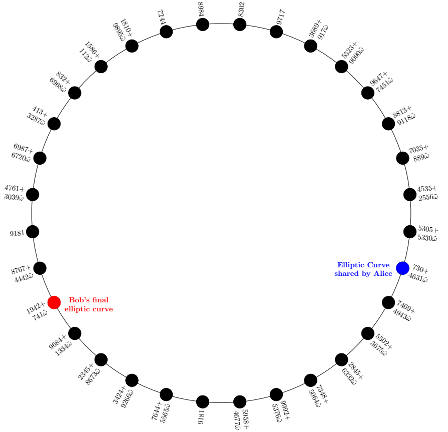
Bob secret key: $\mathfrak{l}_1^3 \mathfrak{l}_2 \mathfrak{l}_3^2$





Bob secret key: $\mathfrak{l}_1^3\mathfrak{l}_2\mathfrak{l}_3^2$

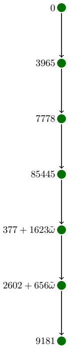


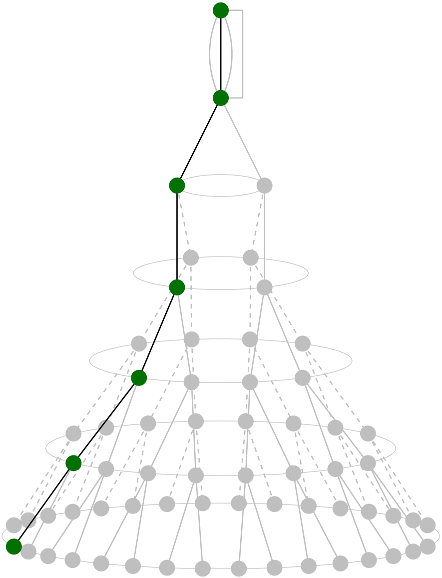


OSIDH PROTOCOL - AN EXAMPLE

L.COLÒ I2M

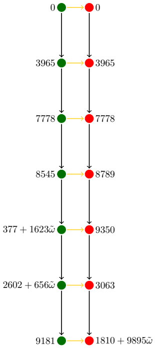
Bob secret key: $\mathfrak{l}_1^3\mathfrak{l}_2\mathfrak{l}_3^2$

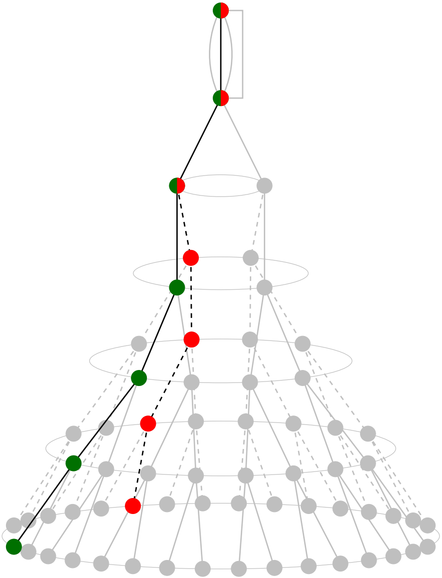




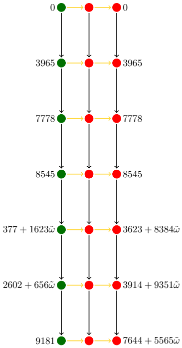
OSIDH PROTOCOL - AN EXAMPLE

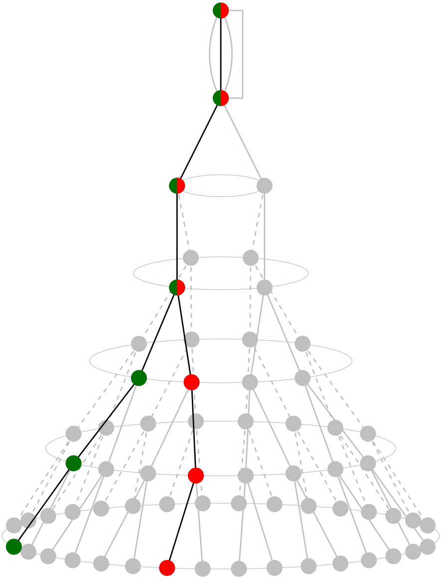
Bob secret key: $\mathfrak{l}_1^3\mathfrak{l}_2\mathfrak{l}_3^2$





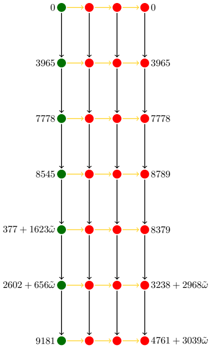
Bob secret key: $\mathfrak{l}_1^3\mathfrak{l}_2\mathfrak{l}_3^2$

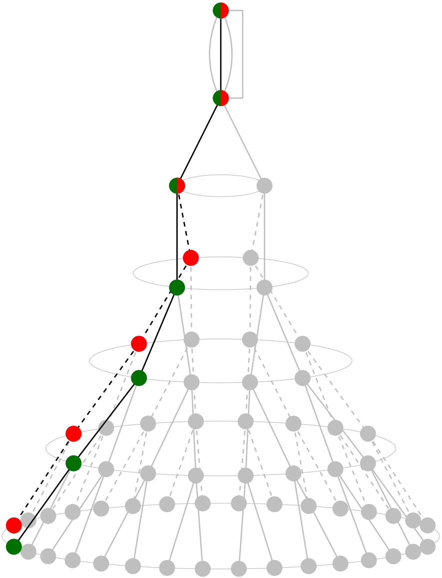




OSIDH PROTOCOL - AN EXAMPLE

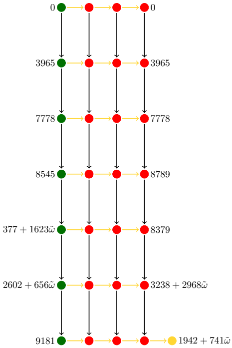
Bob secret key: $\mathfrak{l}_1^3 \mathfrak{l}_2 \mathfrak{l}_3^2$

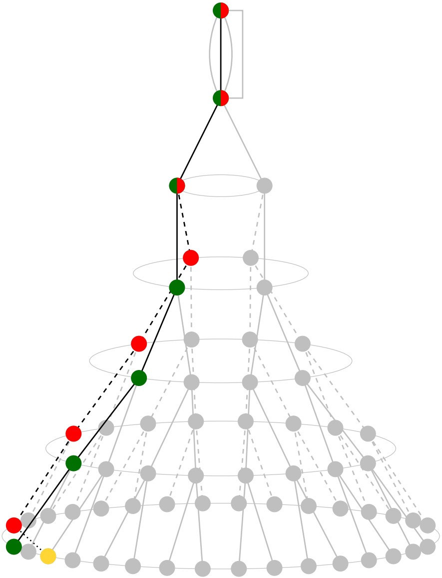




OSIDH PROTOCOL - AN EXAMPLE

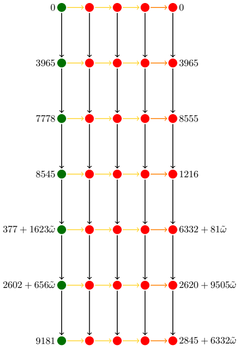
Bob secret key: $\mathfrak{l}_1^3\mathfrak{l}_2\mathfrak{l}_3^2$

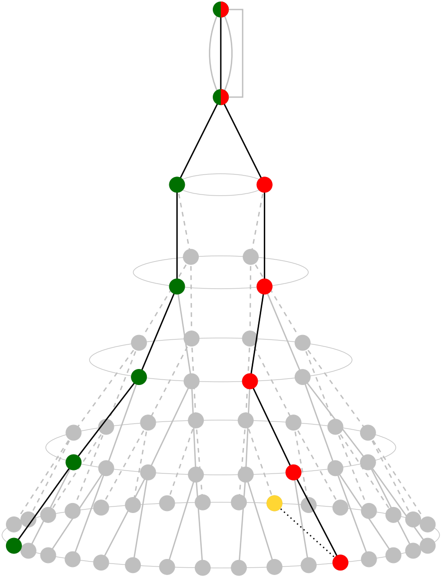




OSIDH PROTOCOL - AN EXAMPLE

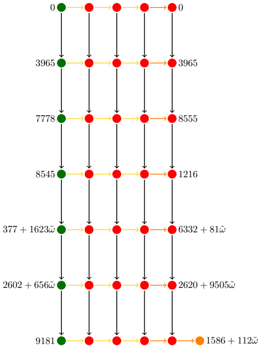
Bob secret key: $\mathfrak{l}_1^3\mathfrak{l}_2\mathfrak{l}_3^2$

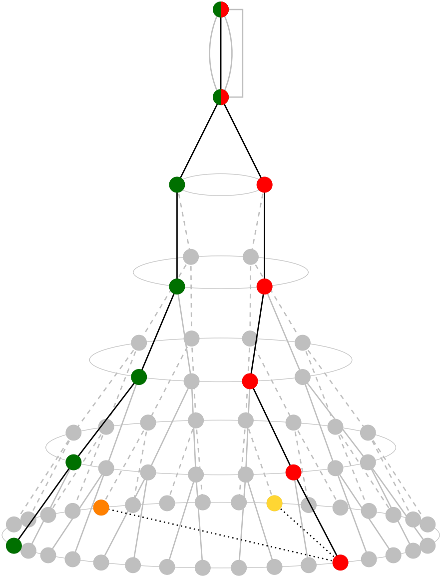




OSIDH PROTOCOL - AN EXAMPLE

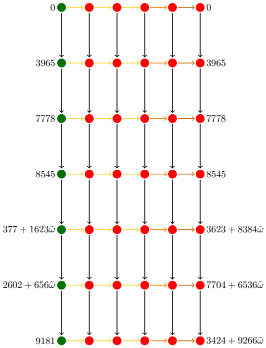
Bob secret key: $\mathfrak{l}_1^3 \mathfrak{l}_2 \mathfrak{l}_3^2$

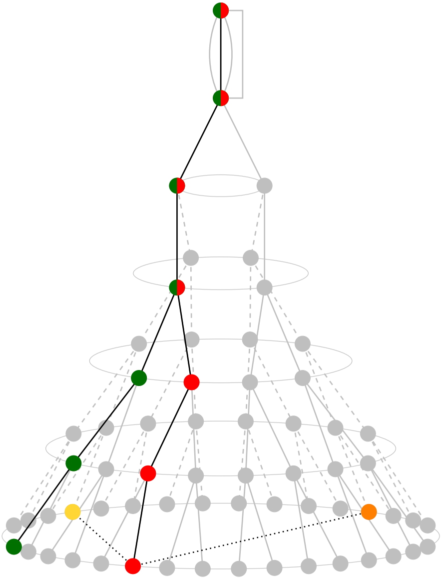




OSIDH PROTOCOL - AN EXAMPLE

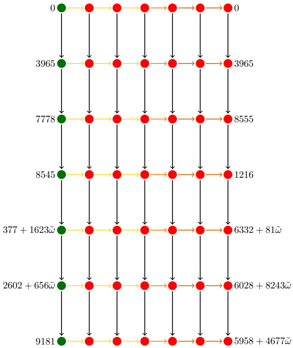
Bob secret key: $\mathfrak{l}_1^3 \mathfrak{l}_2 \mathfrak{l}_3^2$

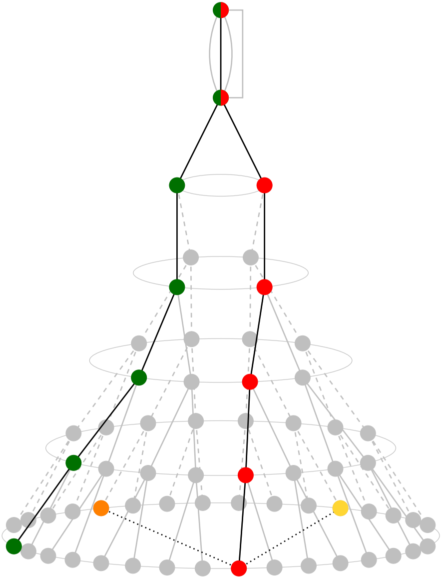




OSIDH PROTOCOL – AN EXAMPLE

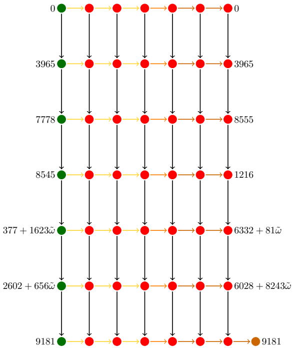
Bob secret key: $\mathfrak{l}_1^3\mathfrak{l}_2\mathfrak{l}_3^2$

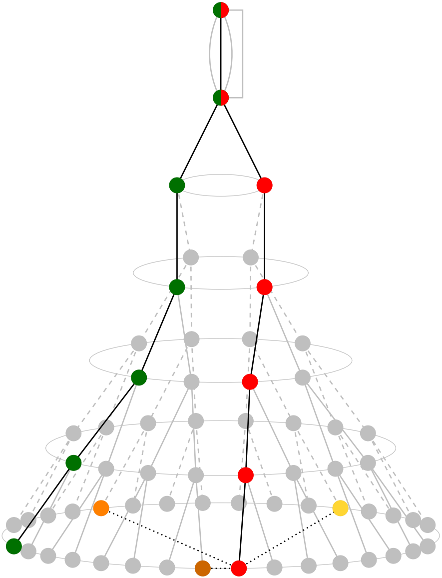




OSIDH PROTOCOL - AN EXAMPLE

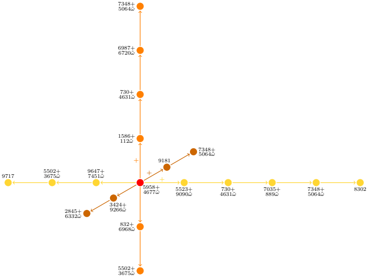
Bob secret key: $\mathfrak{l}_1^3\mathfrak{l}_2\mathfrak{l}_3^2$

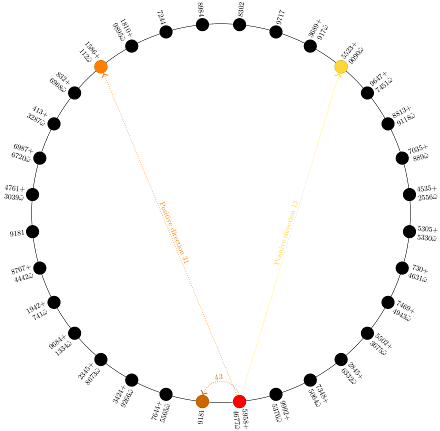




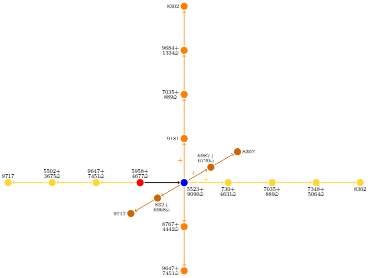
OSIDH PROTOCOL - AN EXAMPLE

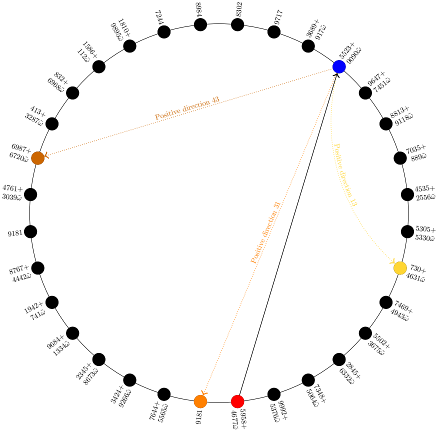
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$





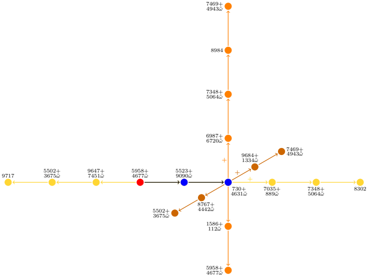
Alice secret key: $\mathfrak{l}_1^5\mathfrak{l}_2^3\mathfrak{l}_3^2$

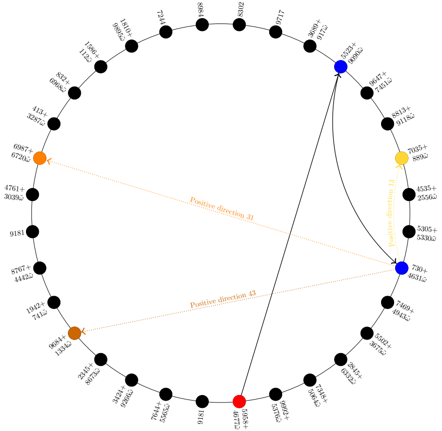




OSIDH PROTOCOL - AN EXAMPLE

Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$

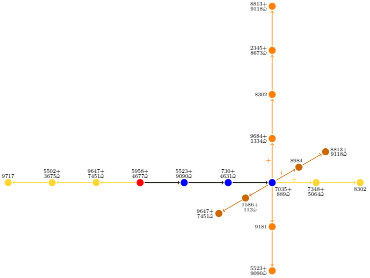


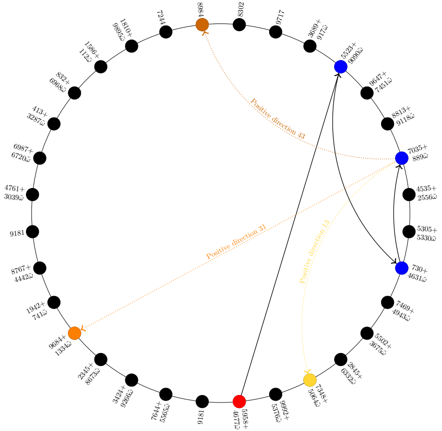


OSIDH PROTOCOL - AN EXAMPLE

L.COLÒ 1 2 M

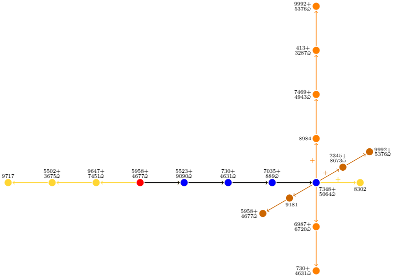
Alice secret key: $\mathfrak{l}_1^5\mathfrak{l}_2^3\mathfrak{l}_3^2$

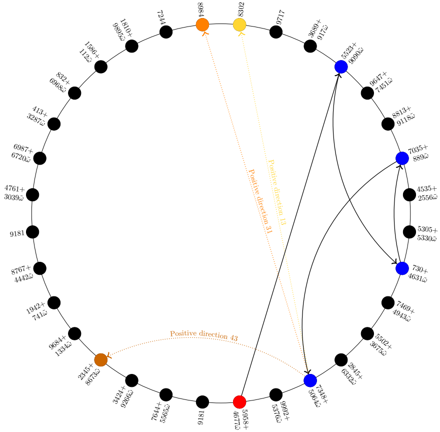




OSIDH protocol - an example

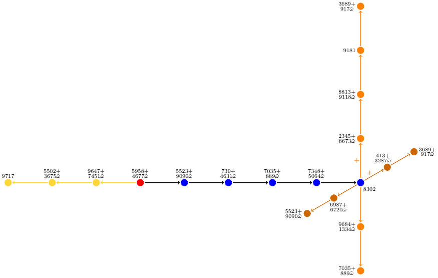
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$

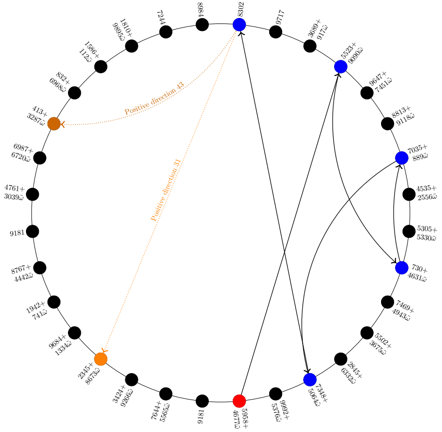




OSIDH PROTOCOL - AN EXAMPLE

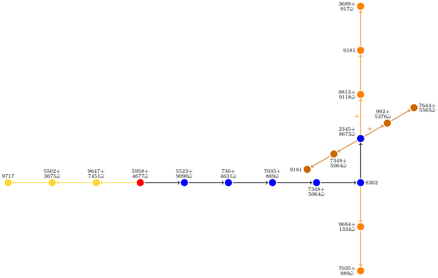
Alice secret key: $\mathfrak{l}_1^5\mathfrak{l}_2^3\mathfrak{l}_3^2$

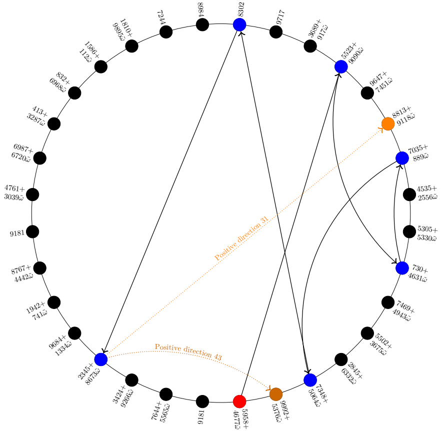




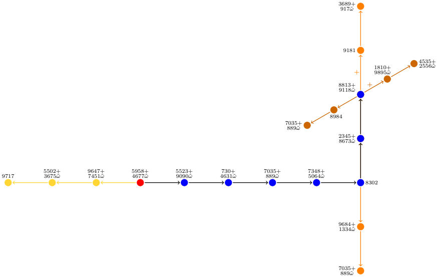
OSIDH PROTOCOL - AN EXAMPLE

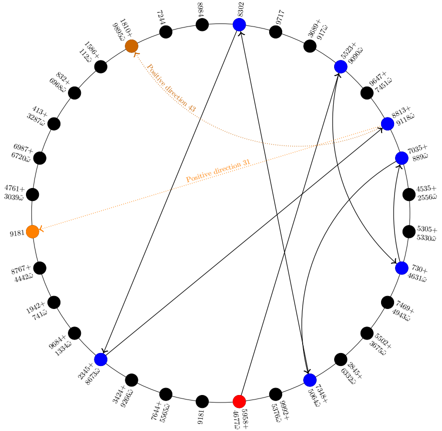
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$



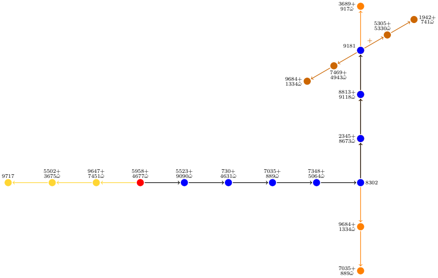


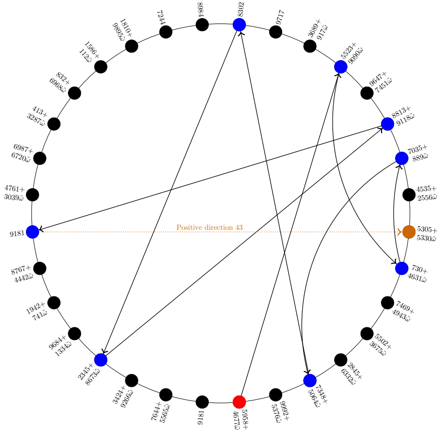
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$





Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$

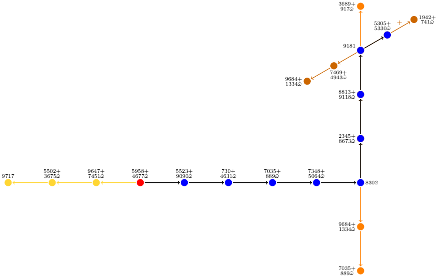


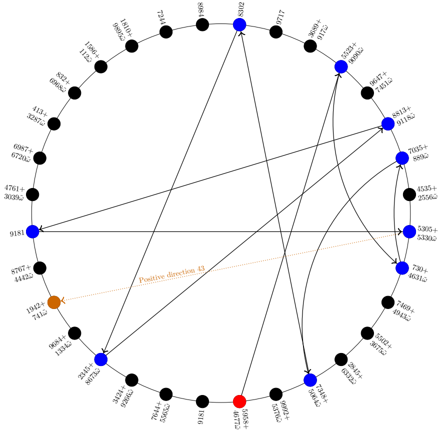


OSIDH PROTOCOL - AN EXAMPLE

L.COLÒ 1 2 M

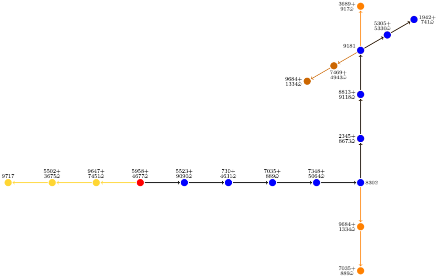
Alice secret key: $\mathfrak{l}_1^{5}\mathfrak{l}_2^{3}\mathfrak{l}_3^{2}$

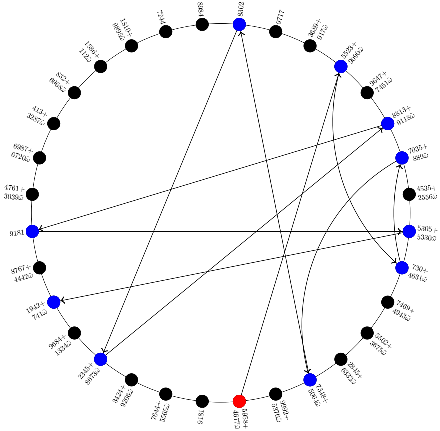




OSIDH PROTOCOL – AN EXAMPLE

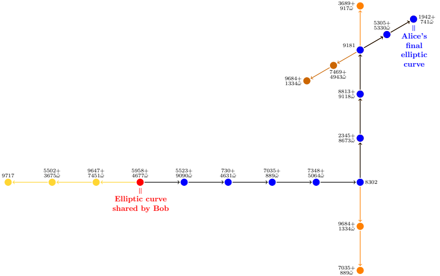
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$

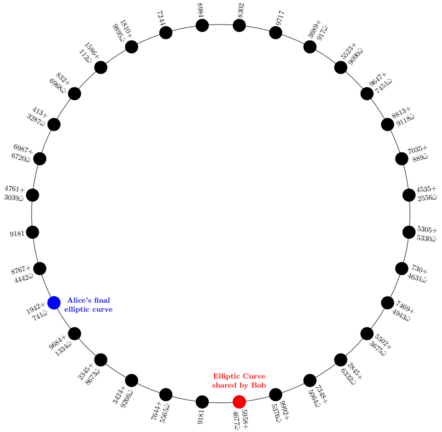




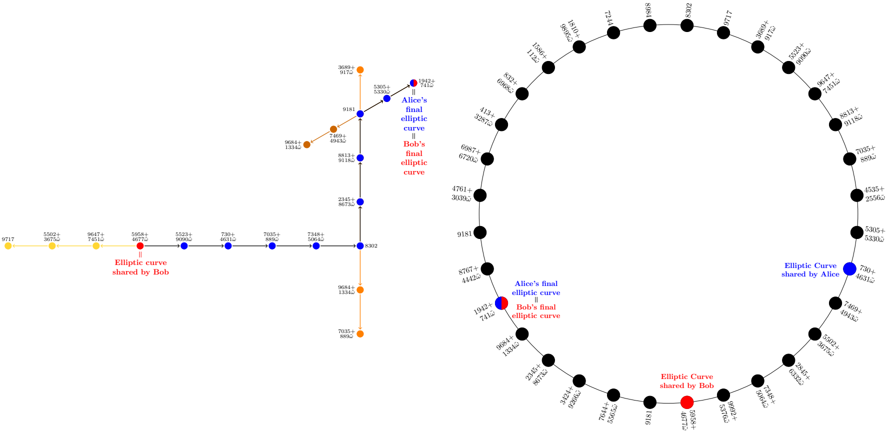
OSIDH PROTOCOL - AN EXAMPLE

Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$





OSIDH PROTOCOL - AN EXAMPLE



SECURITY CONSIDERATIONS

OSIDH PROTOCOL - SECURITY CONSIDERATIONS

L.COLÒ I2M

For an order $\mathcal{O}$ of conductor $\ell^n M$, we note that $\mathcal{C}\ell(\mathcal{O}) \simeq \mathrm{SS}_{\mathcal{O}}^{pr}(\rho)$ and define

$$I = I_1 \times \ldots \times I_t \subseteq \mathbb{Z}^t \quad \text{where } I_j = [-r_j, r_j].$$

The security of OSIDH depends on the following maps

$$I = \prod_{i=1}^{t} [-r_i, r_i] \longrightarrow \mathrm{SS}_{\mathcal{O}}^{pr}(\rho) \longrightarrow \mathrm{SS}(p)$$

Supersingular covering bound

We say that the map $\mathcal{C}\ell(\mathcal{O}) \simeq \mathrm{SS}_{\mathcal{O}}^{pr}(\rho) \longrightarrow \mathrm{SS}(p)$ is λ-*surjective* if

$$p^\lambda \leq \#\mathcal{C}\ell(\mathcal{O})$$

where λ is the *logarithmic covering radius*. We get

$$\lambda \log_\ell(p) \leq n + \log_\ell(M) + \log_\ell(h(\mathcal{O}_K))$$

For an order $\mathcal{O}$ of conductor $\ell^n M$, we note that $\mathcal{C}\ell(\mathcal{O}) \simeq \mathrm{SS}^{pr}_{\mathcal{O}}(\rho)$ and define

$$I = I_1 \times \ldots \times I_t \subseteq \mathbb{Z}^t \quad \text{where } I_j = [-r_j, r_j].$$

The security of OSIDH depends on the following maps

$$I = \prod_{i=1}^{t} [-r_i, r_i] \longrightarrow \mathrm{SS}^{pr}_{\mathcal{O}}(\rho) \longrightarrow \mathrm{SS}(p)$$

Supersingular injectivity bound

How can one insure the injectivity of the map $\mathrm{SS}^{pr}_{\mathcal{O}}(\rho) \to \mathrm{SS}(p)$? We set

$$n + \log_\ell(M) + \frac{1}{2}\log_\ell(|\Delta_K|) \leq \frac{1}{2}\log_\ell(p)$$

If (SIB) holds, then the map $\mathrm{SS}^{pr}_{\mathcal{O}}(\rho) \to (p)$ is injective.

OSIDH PROTOCOL - SECURITY CONSIDERATIONS

L.COLÒ I2M

For an order $\mathcal{O}$ of conductor $\ell^n M$, we note that $\mathcal{C}\ell(\mathcal{O}) \simeq \mathrm{SS}_{\mathcal{O}}^{pr}(p)$ and define

$$I = I_1 \times \ldots \times I_t \subseteq \mathbb{Z}^t \quad \text{where } I_j = [-r_j, r_j].$$

The security of OSIDH depends on the following maps

$$I = \prod_{i=1}^{t} [-r_i, r_i] \longrightarrow \mathrm{SS}_{\mathcal{O}}^{pr}(p) \longrightarrow \mathrm{SS}(p)$$

Class group covering bound

In order to have a uniform element of $\mathcal{C}\ell(\mathcal{O})$ it is desirable to be able to reach all elements of $\mathcal{C}\ell(\mathcal{O})$.

$$\sum_{i=1}^{t} \log_\ell(2r_i + 1) \geq \lambda\left(n + \log_\ell(M) + \log_\ell(h(\mathcal{O}_K))\right)$$

OSIDH PROTOCOL - SECURITY CONSIDERATIONS

L.COLÒ I2M

For an order $\mathcal{O}$ of conductor $\ell^n M$, we note that $\mathcal{C}\ell(\mathcal{O}) \simeq \mathrm{SS}^{pr}_{\mathcal{O}}(\rho)$ and define

$$I = I_1 \times \ldots \times I_t \subseteq \mathbb{Z}^t \quad \text{where } I_j = [-r_j, r_j].$$

The security of OSIDH depends on the following maps

$$I = \prod_{i=1}^{t} [-r_i, r_i] \longrightarrow \mathrm{SS}^{pr}_{\mathcal{O}}(\rho) \longrightarrow \mathrm{SS}(p)$$

Minkowski norm bound

The set of elements obtained by random walks should contain no cycle; thus,

$$\sum_{i=1}^{t} r_i \log_\ell(q_i) \leq n + \log_\ell(M) + \frac{1}{2}\log_\ell(|\Delta_K|/4)$$

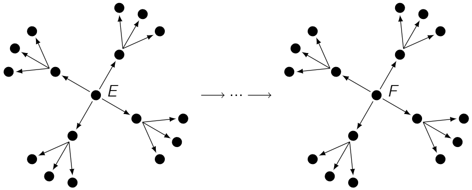
The attack of Dartois and De Feo exploits the non-injectivity of the map $I \to \mathrm{SS}^{pr}_{\mathcal{O}}(\rho)$ to recover an endomorphism of E.

Key generation

On one side, A begins with $F = E$.

- Split primes: for each prime q_i in $\mathcal{P}_S$, choose a random $s_i \in I_i$, constructs the q_i-isogeny walk of length s_i while pushing forward the other direction as well as the q-clouds at each prime q in $\mathcal{P}_A$ and $\mathcal{P}_B$.
- Non-split primes: for each prime choose a random walk in the cloud to a new curve F and push forward the remaining unused q-clouds.

The data F and q-isogeny chains at primes q in $\mathcal{P}_s$ and q-clouds at primes q in $\mathcal{P}_B$ constitute A's public key.



PARAMETER SELECTION - AN EXAMPLE

We set $\Delta_K = -3$ and $\ell = 2$.
We begin with $t = 10$ and a bit Bound $B_s = 32$.

Split Primes

	q :	7	13	19	31	37	43	61	67	73	79
$\mathcal{P}_s$:	r :	11	8	7	6	6	6	5	5	5	5
	# :	23	17	15	13	13	13	11	11	11	11

This gives a logarithmic contribution of

$$\sum_{j=1}^{10} \log_2(2r_j + 1) = 37.4569...$$

to the entropy of the random walk.
The logarithmic norm, which we must bound is:

$$\sum_{j=1}^{10} r_j \log_2(q_j) = 306.2115...(< 320 = 32 \cdot 10).$$

PARAMETER SELECTION - AN EXAMPLE

L.COLÒ 1 2 M

We set $\Delta_K = -3$ and $\ell = 2$.
We begin with $t = 10$ and a bit Bound $B_s = 32$.

Non-Split Primes

We partition the remaining primes up to 163 into sets $\mathcal{P}_A$ and $\mathcal{P}_B$, with a radius for the cloud (or eddy), as follows:

$\mathcal{P}_A$:															
	q :	2	11	17	41	47	59	83	101	103	109	131	149	151	157
	r :	7	2	1	1	1	1	1	1	1	1	1	1	1	1
	# :	128	132	18	42	48	60	84	102	102	108	132	150	150	156

$\mathcal{P}_B$:															
	q :	3	5	23	29	53	71	89	97	107	113	127	137	139	163
	r :	4	3	1	1	1	1	1	1	1	1	1	1	1	1
	# :	81	150	24	30	54	72	90	96	108	114	126	138	138	162

Both sets leak the horizontal directions for these primes, giving an additional contribution of ≈ 28 bits to the logarithmic norm.
These prime sets each contribute a $\log_2(M)$ of 90 bits, such that n must be at least 244 to defeat the lattice-based class group attack.

PARAMETER SELECTION - CONCLUSION

The norm bound suggests using a uniform bound B_s on $r_j \log_\ell(q_j)$ rather than the exponents r_j. This gives

$$\lambda \log_\ell(p) \leq \sum_{i=1}^{t} \log_\ell(2r_j + 1) \leq \sum_{j=1}^{t} r_j \log_\ell(q_j) \leq tB_s < n + \log_\ell(M)$$

for which $(t = 64, B_s = 16, n = 1024)$ represent a choice of parameters ensuring injectivity of $I \to \mathcal{C}\ell(\mathcal{O})$.

THANK YOU FOR YOUR ATTENTION