WATERLOO, 23 OCTOBER 2023

L.COLÒ UWAT

MODULAR AND FORMAL ORIENTATIONS BEYOND OSIDH

LEONARDO COLÒ & DAVID KOHEL

University of Waterloo

Isogeny Club

CONTENTS

- Orientations and class group actions.
- OSIDH protocol.
- Adding level structure.
- Formal orientations.

ORIENTATIONS AND CLASS GROUP ACTIONS

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

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

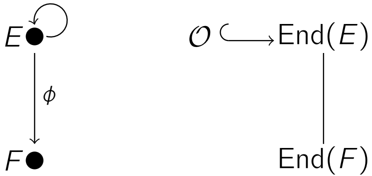
An $\mathcal{O}$-orientation is *primitive* if

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

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

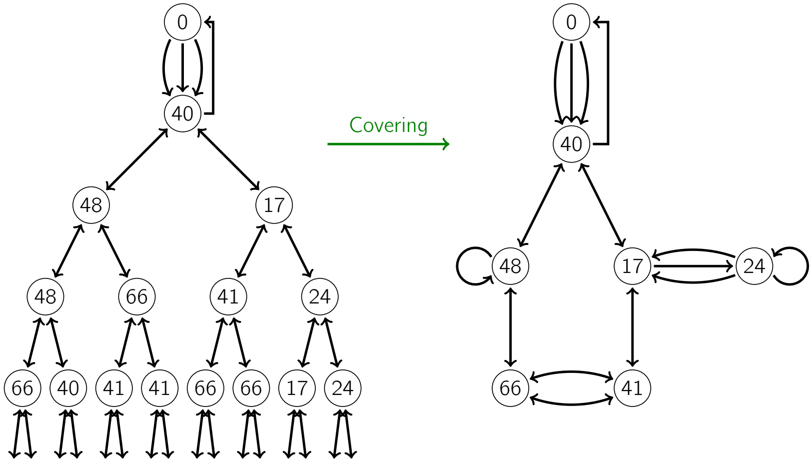
$$\phi_*(\iota)(\alpha) = \frac{1}{\ell}\,\phi \circ \iota(\alpha) \circ \hat{\phi}.$$

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 - AN EXAMPLE

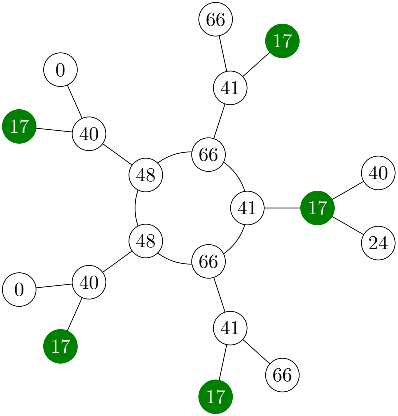
Let $p = 71$ and $E_0/\mathbb{F}_{71}$ be the supersingular elliptic curve with $j(E) = 0$ oriented by the $\mathcal{O}_K = \mathbb{Z}[\omega]$, where $\omega^2 + \omega + 1 = 0$.

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 $\mathbb{Q}(\sqrt{-79})$.



CLASS GROUP ACTION

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

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

Proposition

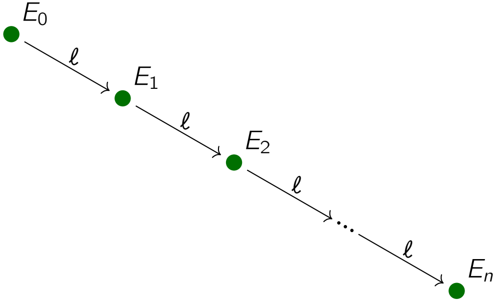
The set $\mathrm{SS}_{\mathcal{O}}^{pr}(\rho)$ is a torsor for the class group $\mathcal{Cl}(\mathcal{O})$.

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

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

EFFECTIVE CLASS GROUP ACTIONS

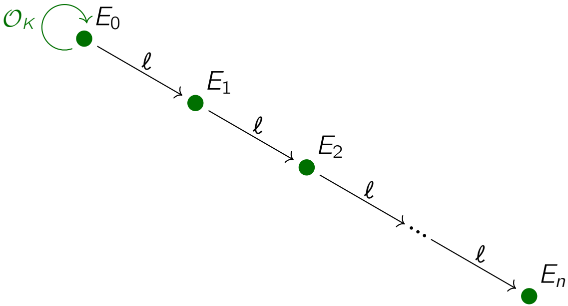
We consider an elliptic curve E_0 with an effective endomorphism ring (eg. $j_0 = 0, 1728$) and a chain of ℓ-isogenies.



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.

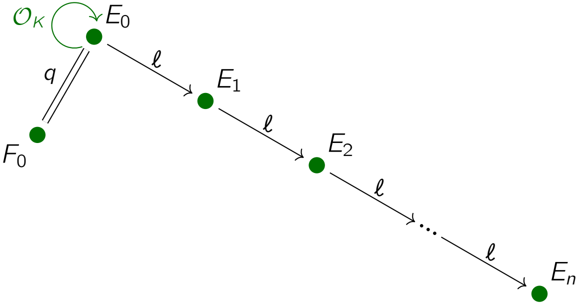
- For $\ell = 2$ (or 3) a suitable candidate for $\mathcal{O}_K$ could be the Gaussian integers $\mathbb{Z}[i]$ or the Eisenstein integers $\mathbb{Z}[\omega]$.



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

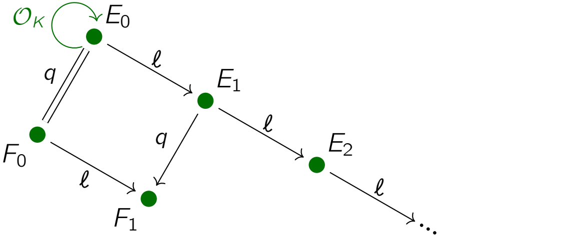


EFFECTIVE CLASS GROUP ACTIONS

L.COLÒ UWAT

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

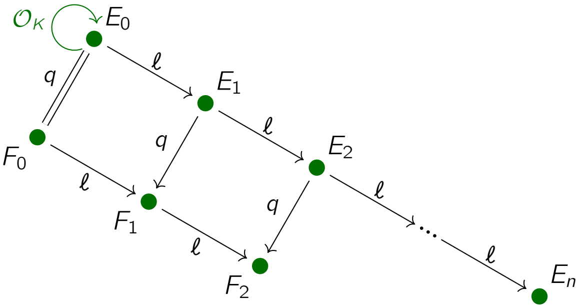
- We push forward our q-orientation obtaining F_1.



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.

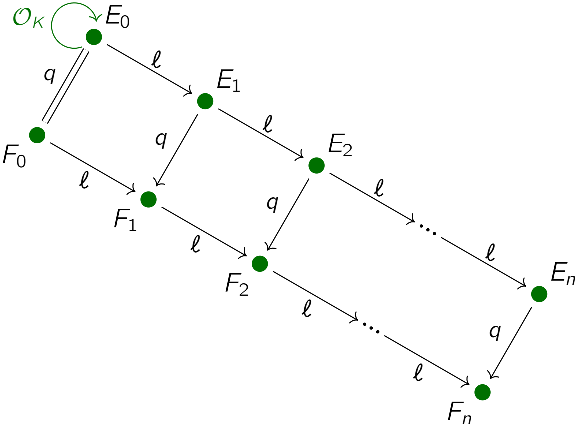
- We repeat the process for F_2.



EFFECTIVE CLASS GROUP ACTIONS

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.



OSIDH

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

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 UWAT

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 $\forall i$	$F_{n,i}^{(-r)} \leftarrow F_{n,i}^{(-r+1)} \leftarrow \ldots \leftarrow F_{n,i}^{(1)} \leftarrow F_n$	$G_{n,i}^{(-r)} \leftarrow G_{n,i}^{(-r+1)} \leftarrow \ldots \leftarrow G_{n,i}^{(1)} \leftarrow G_n$

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 $\mathfrak{p}_1, \ldots, \mathfrak{p}_t \subseteq \mathcal{O} \subseteq \mathrm{End}(E_n) \cap K \subseteq \mathcal{O}_K$

	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

OSIDH PROTOCOL

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

	ALICE	**BOB**
Choose integers in a bound $[-r, r]$	$(e_1, \dots, e_t)$	$(d_1, \dots, d_t)$
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 $\forall i$	$F_{n,i}^{(-r)} \leftarrow F_{n,i}^{(-r+1)} \leftarrow \dots \leftarrow F_{n,i}^{(1)} \leftarrow F_n$	$G_{n,i}^{(-r)} \leftarrow G_{n,i}^{(-r+1)} \leftarrow \dots \leftarrow G_{n,i}^{(1)} \leftarrow G_n$
... and their conjugates	$F_n \to F_{n,i}^{(1)} \to \dots \to F_{n,i}^{(r-1)} \to F_{n,1}^{(r)}$	$G_n \to G_{n,i}^{(1)} \to \dots \to G_{n,i}^{(r-1)} \to G_{n,1}^{(r)}$
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

$p = 10007$

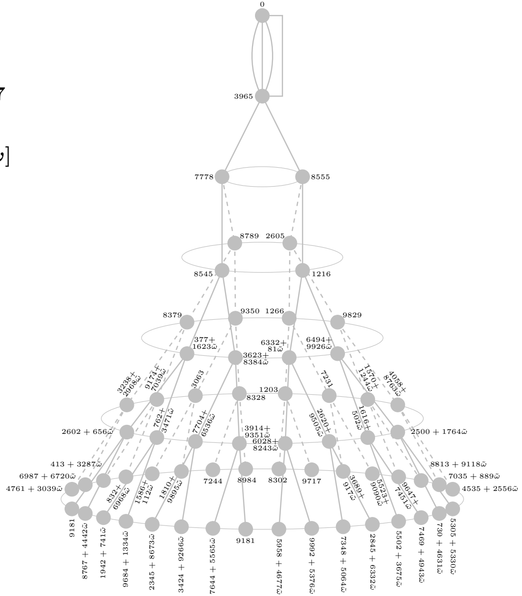
$\ell = 2$

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

$\ell_1 = 13$

$\ell_2 = 31$

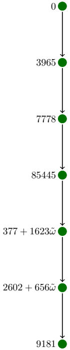
$\ell_3 = 43$

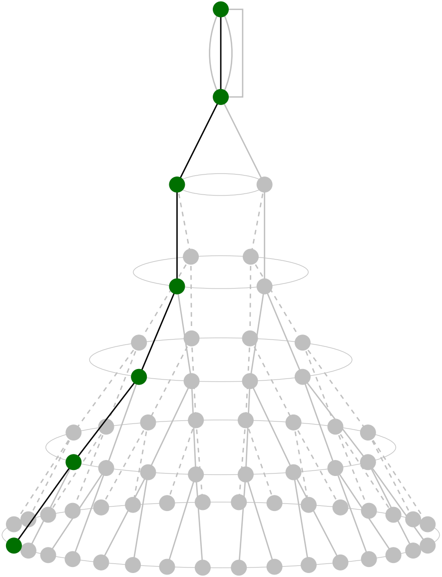


OSIDH PROTOCOL - AN EXAMPLE

L.COLÒ UWAT

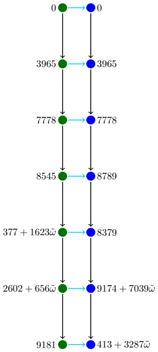
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$

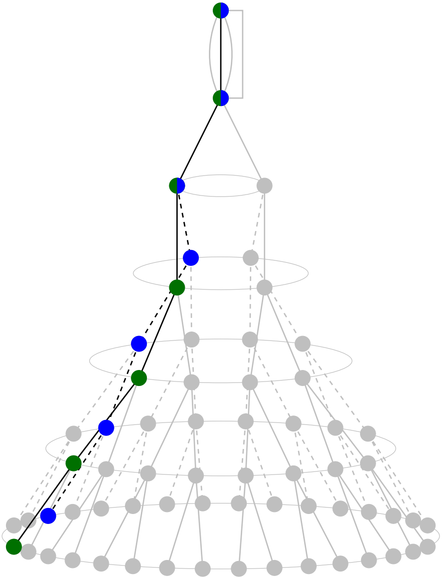




OSIDH PROTOCOL - AN EXAMPLE

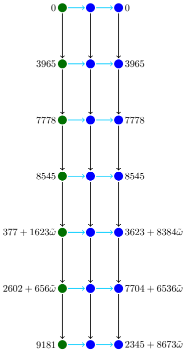
Alice secret key: $\mathfrak{l}_1^5\,\mathfrak{l}_2^3\,\mathfrak{l}_3^2$

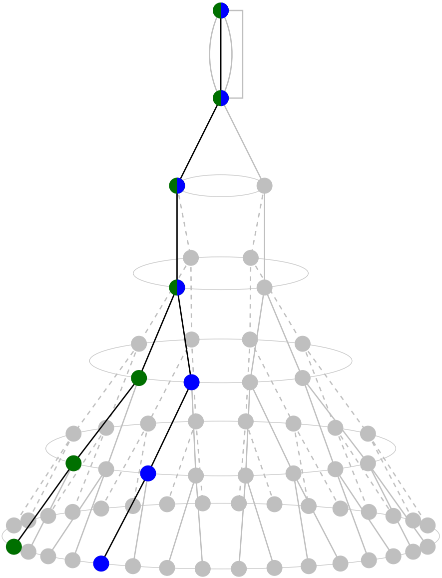




OSIDH PROTOCOL - AN EXAMPLE

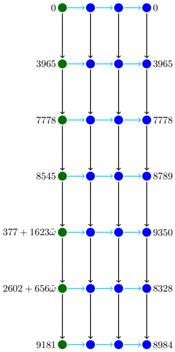
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$

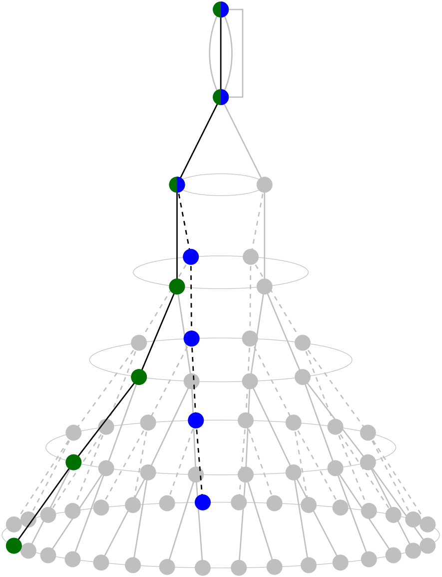




OSIDH PROTOCOL - AN EXAMPLE

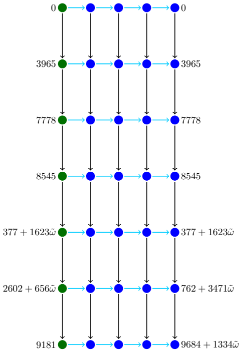
Alice secret key: $\mathfrak{l}_1^5\mathfrak{l}_2^3\mathfrak{l}_3^2$

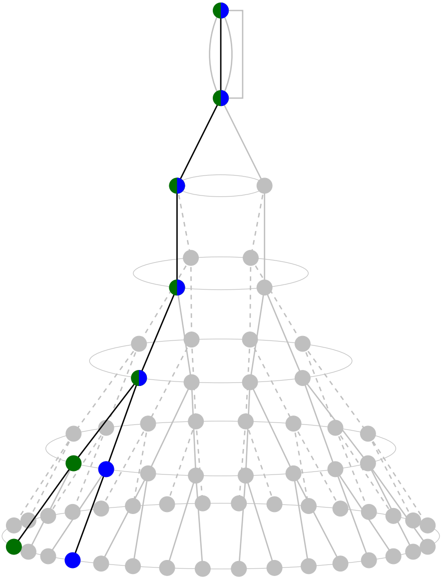




OSIDH PROTOCOL - AN EXAMPLE

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

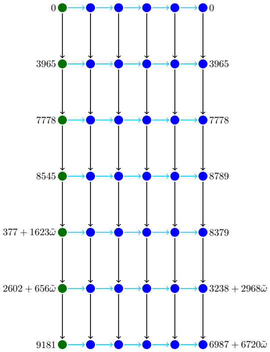


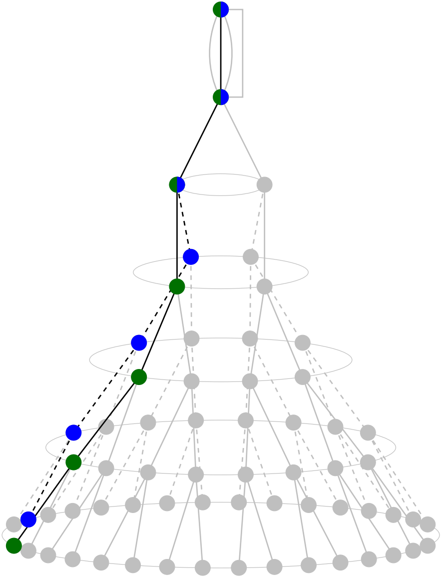


OSIDH PROTOCOL - AN EXAMPLE

L.COLÒ UWAT

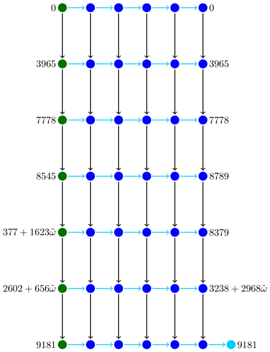
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$

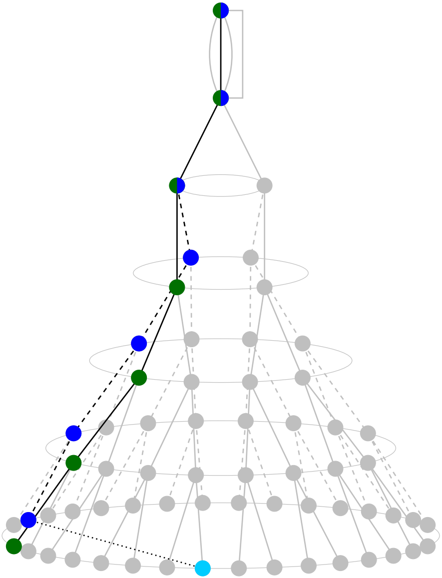




OSIDH PROTOCOL - AN EXAMPLE

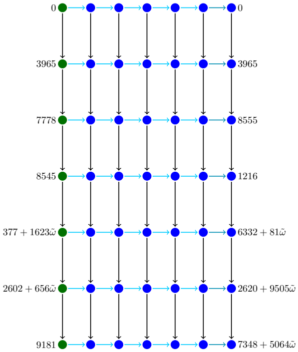
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$

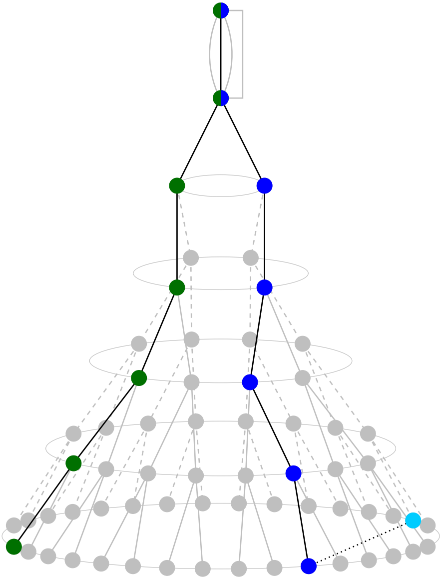




OSIDH PROTOCOL - AN EXAMPLE

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

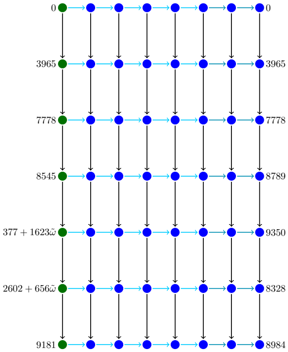


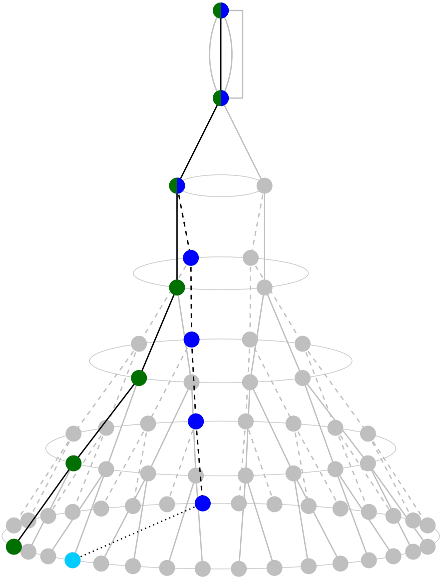


OSIDH PROTOCOL - AN EXAMPLE

L.COLÒ UWAT

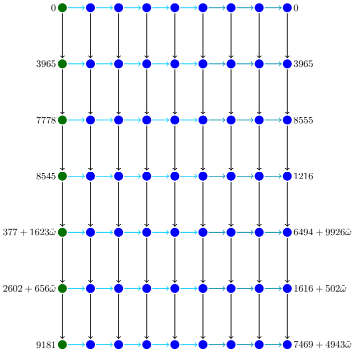
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$

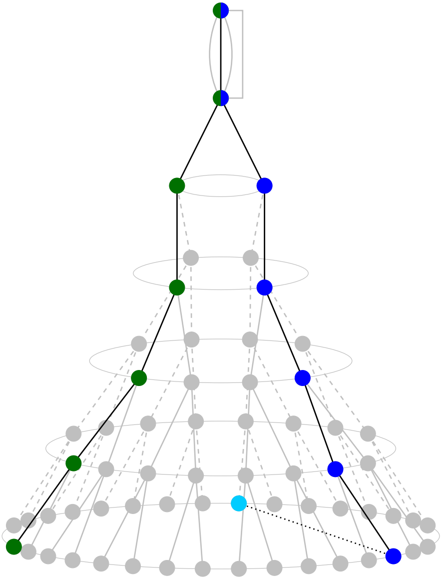




OSIDH PROTOCOL - AN EXAMPLE

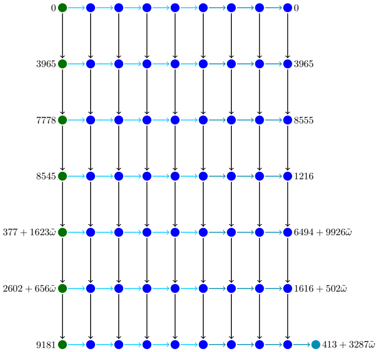
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$

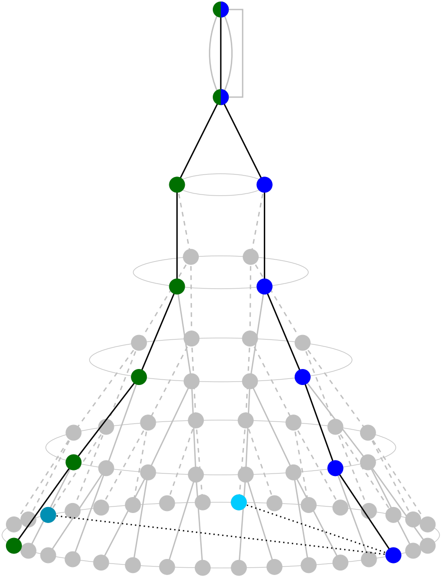




OSIDH PROTOCOL - AN EXAMPLE

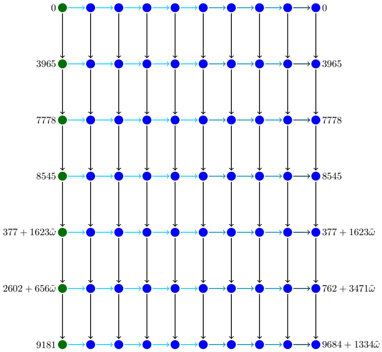
Alice secret key: $\mathfrak{l}_1^5\,\mathfrak{l}_2^3\,\mathfrak{l}_3^2$

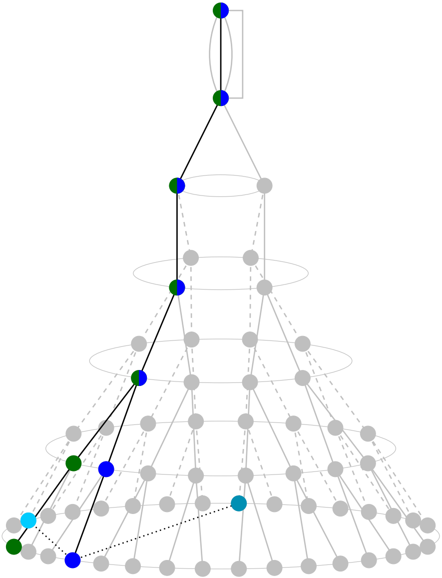




OSIDH PROTOCOL - AN EXAMPLE

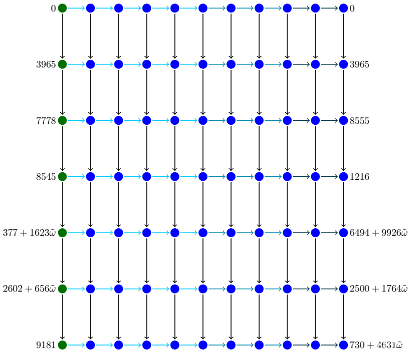
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$

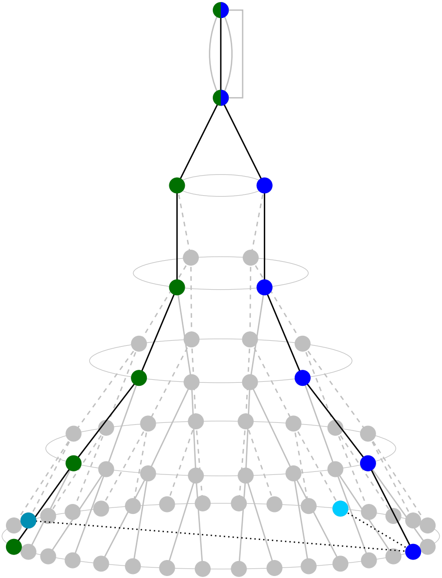




OSIDH PROTOCOL - AN EXAMPLE

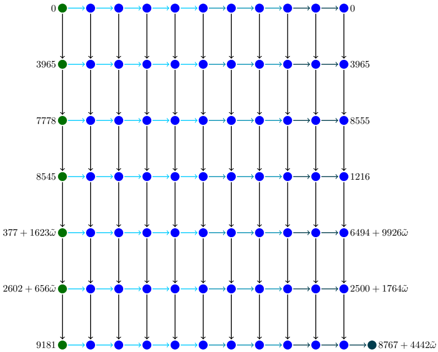
Alice secret key: $\mathfrak{l}_1^5\,\mathfrak{l}_2^3\,\mathfrak{l}_3^2$

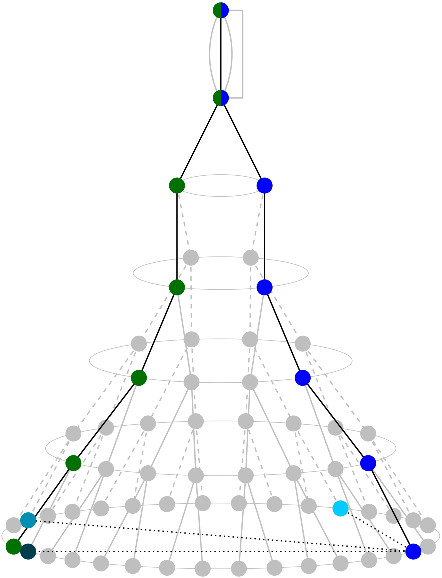




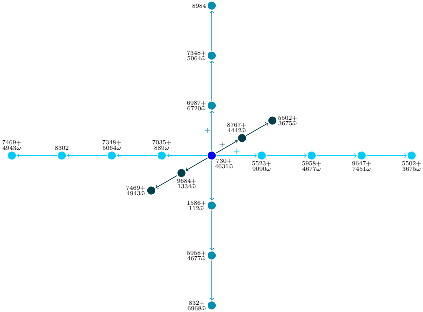
OSIDH PROTOCOL - AN EXAMPLE

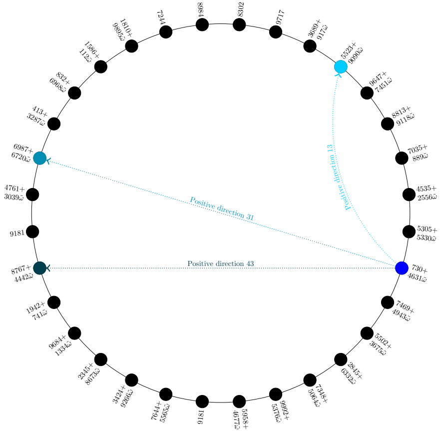
Alice secret key: $\mathfrak{l}_1^5\,\mathfrak{l}_2^3\,\mathfrak{l}_3^2$





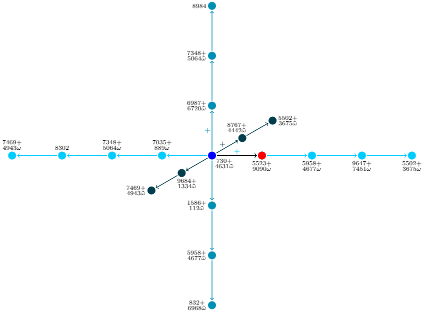
Bob secret key: $\mathfrak{l}_1^3 \mathfrak{l}_2 \mathfrak{l}_3^2$

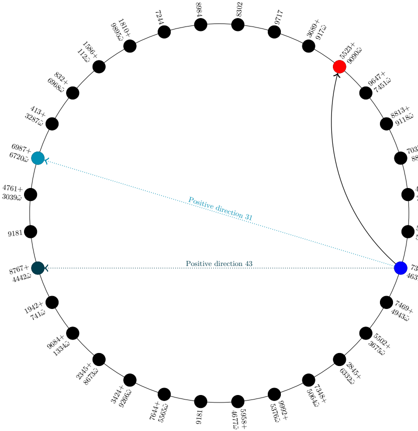




OSIDH PROTOCOL - AN EXAMPLE

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

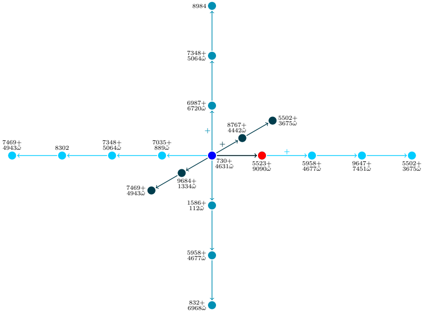


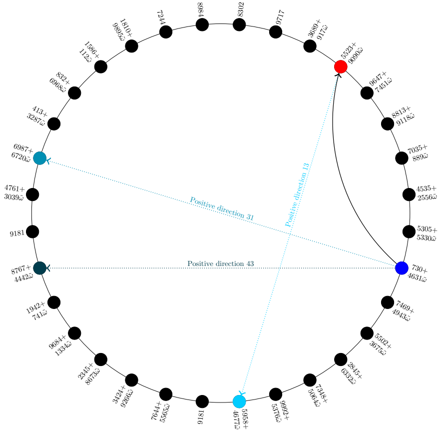


OSIDH PROTOCOL - AN EXAMPLE

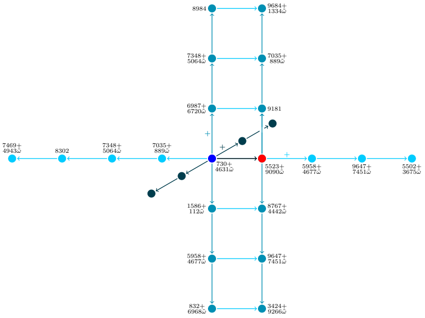
L.COLÒ UWAT

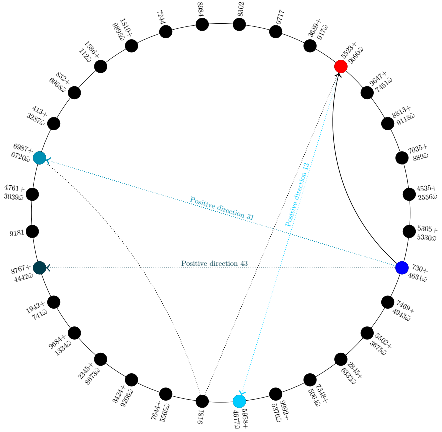
Bob secret key: $\mathfrak{l}_1^3\mathfrak{l}_2\mathfrak{l}_3^2$





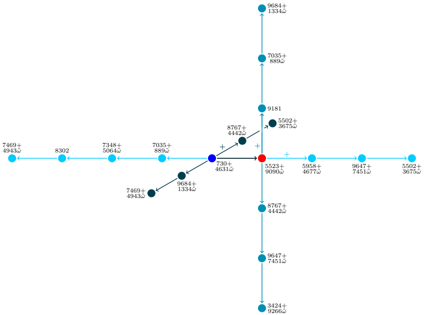
Bob secret key: $\mathfrak{l}_1^3\mathfrak{l}_2\mathfrak{l}_3^2$

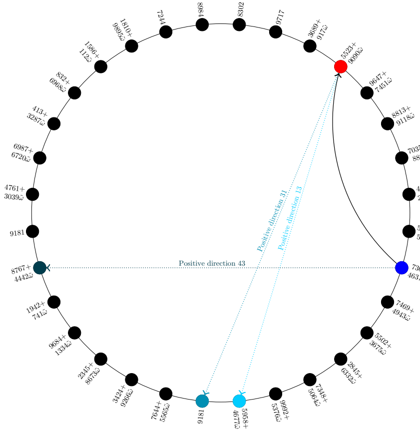




OSIDH PROTOCOL - AN EXAMPLE

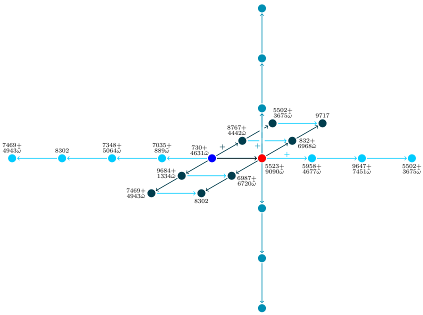
Bob secret key: $\mathfrak{l}_1^3 \mathfrak{l}_2 \mathfrak{l}_3^2$

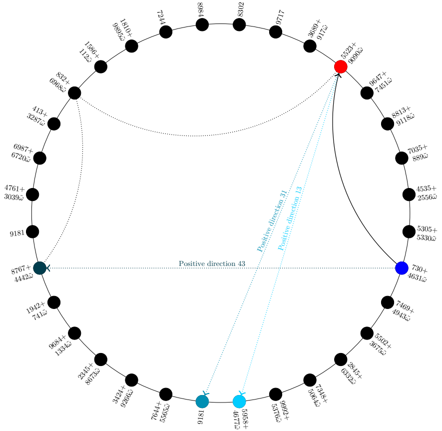




OSIDH PROTOCOL - AN EXAMPLE

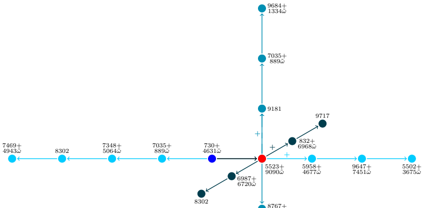
Bob secret key: $\mathfrak{l}_1^3 \mathfrak{l}_2 \mathfrak{l}_3^2$

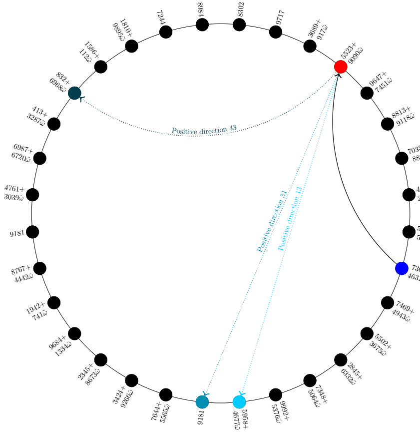




OSIDH PROTOCOL - AN EXAMPLE

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

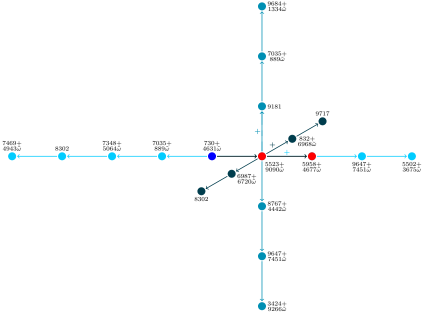


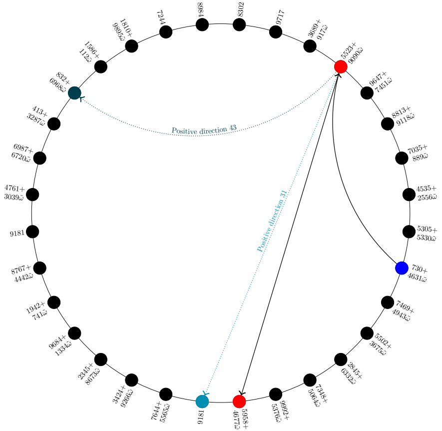


OSIDH PROTOCOL - AN EXAMPLE

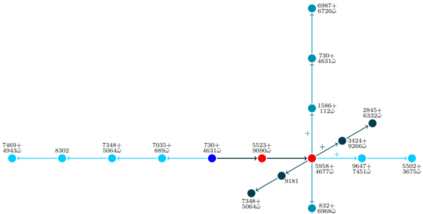
L.COLÒ UWAT

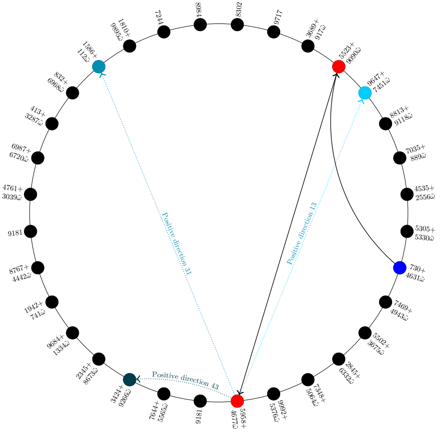
Bob secret key: $\mathfrak{l}_1^3 \mathfrak{l}_2 \mathfrak{l}_3^2$





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

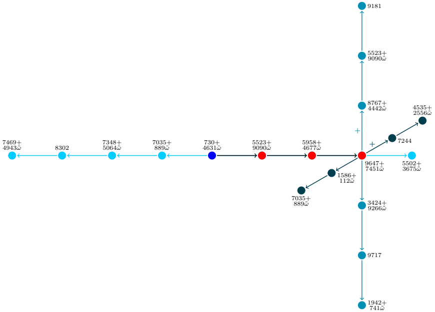


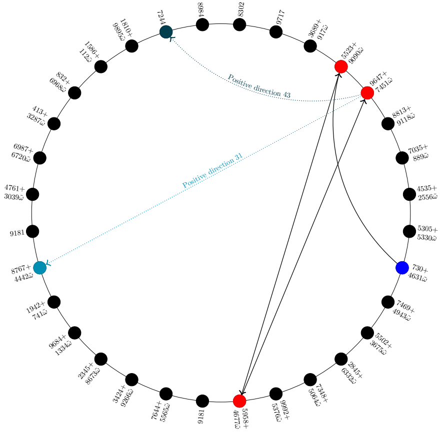


OSIDH PROTOCOL - AN EXAMPLE

L.COLÒ UWAT

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

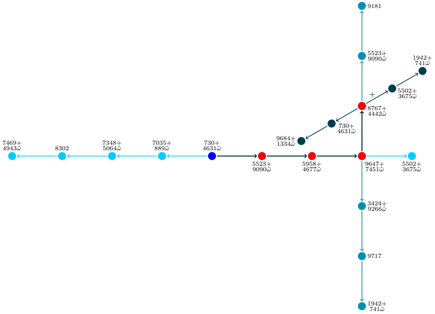


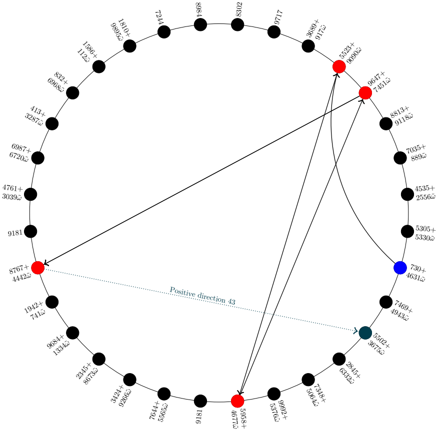


OSIDH PROTOCOL - AN EXAMPLE

L.COLÒ UWAT

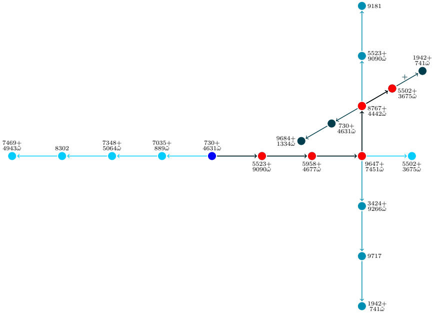
Bob secret key: $\mathfrak{l}_1^3 \mathfrak{l}_2 \mathfrak{l}_3^2$

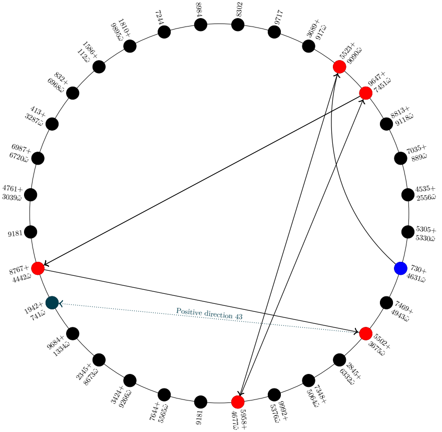




OSIDH PROTOCOL - AN EXAMPLE

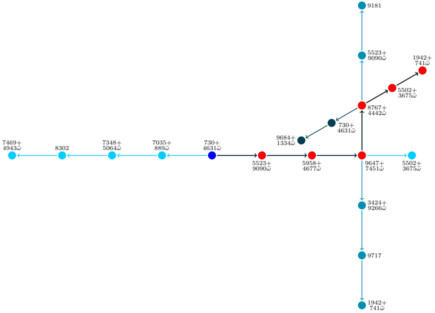
Bob secret key: $\mathfrak{l}_1^3\mathfrak{l}_2\mathfrak{l}_3^2$

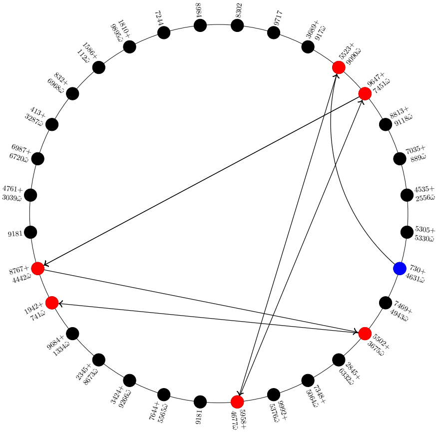




OSIDH PROTOCOL - AN EXAMPLE

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

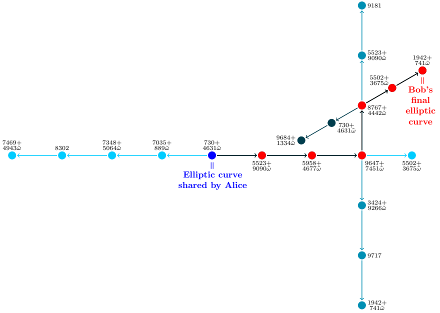


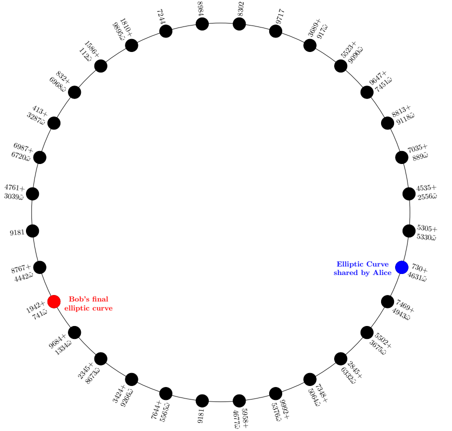


OSIDH PROTOCOL - AN EXAMPLE

L.COLÒ UWAT

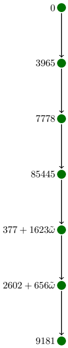
Bob secret key: $\mathfrak{l}_1^3 \mathfrak{l}_2 \mathfrak{l}_3^2$

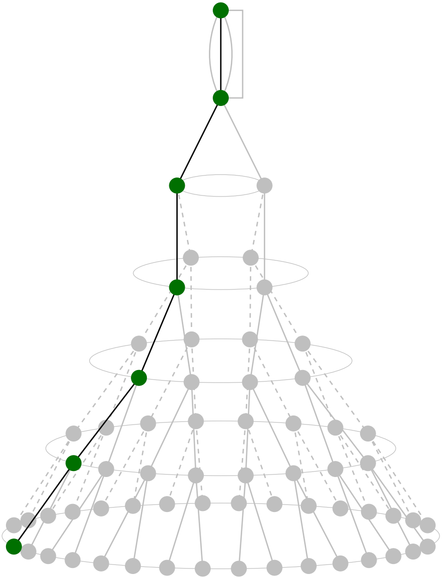




OSIDH PROTOCOL - AN EXAMPLE

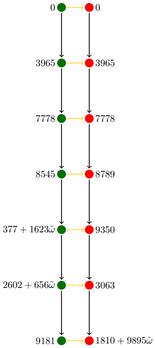
Bob secret key: $\mathfrak{l}_1^3\mathfrak{l}_2\mathfrak{l}_3^2$

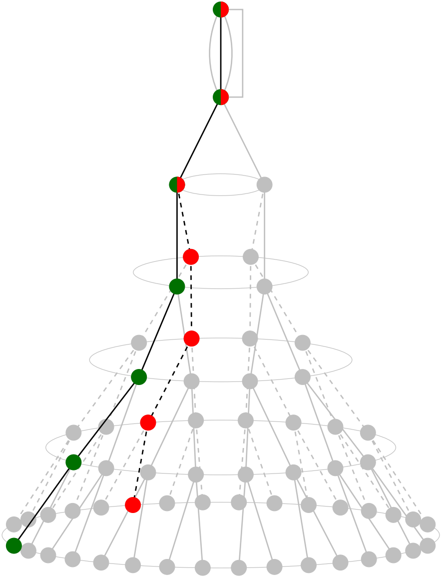




OSIDH PROTOCOL - AN EXAMPLE

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

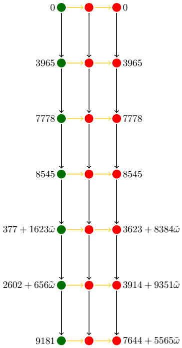


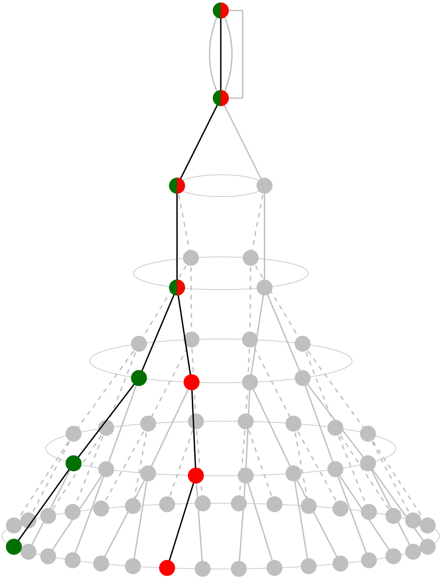


OSIDH PROTOCOL - AN EXAMPLE

L.COLÒ UWAT

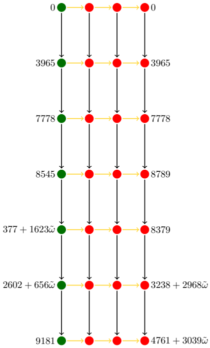
Bob secret key: $\mathfrak{l}_1^3 \mathfrak{l}_2 \mathfrak{l}_3^2$

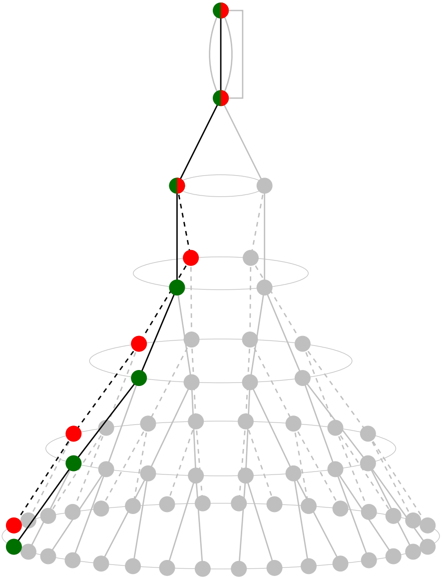




OSIDH PROTOCOL - AN EXAMPLE

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

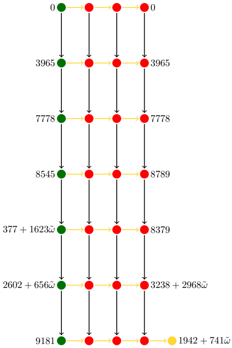


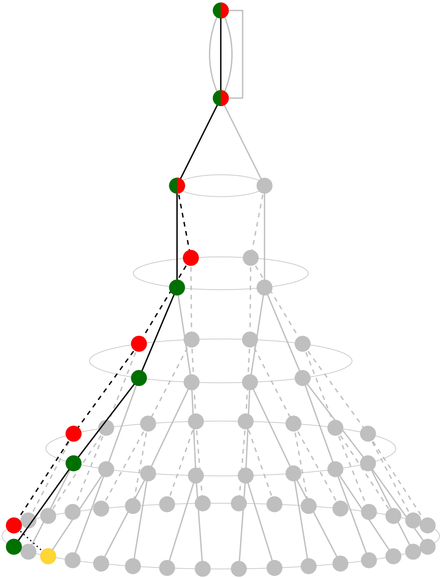


OSIDH PROTOCOL - AN EXAMPLE

L.COLÒ UWAT

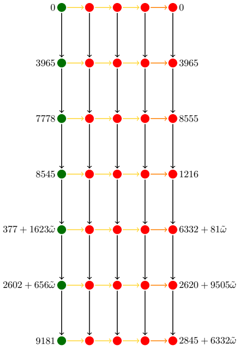
Bob secret key: $\mathfrak{l}_1^3 \mathfrak{l}_2 \mathfrak{l}_3^2$

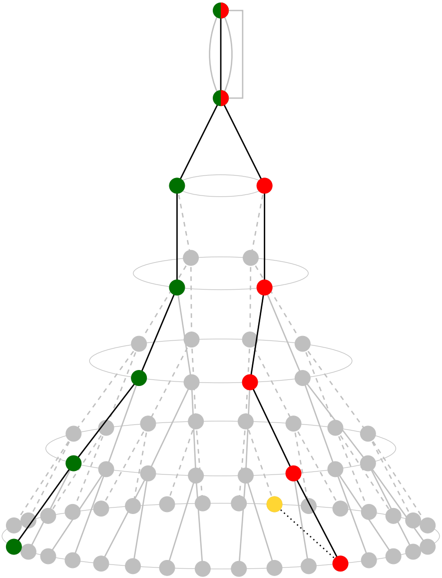




OSIDH PROTOCOL - AN EXAMPLE

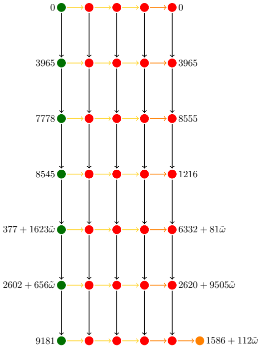
Bob secret key: $\mathfrak{l}_1^3 \mathfrak{l}_2 \mathfrak{l}_3^2$

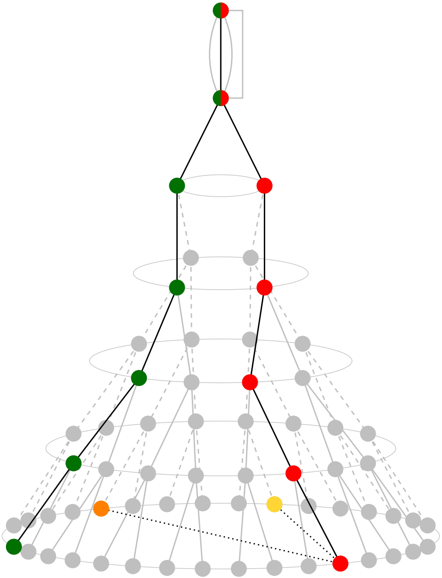




OSIDH PROTOCOL - AN EXAMPLE

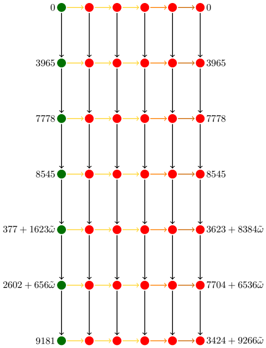
Bob secret key: $\mathfrak{l}_1^3 \mathfrak{l}_2 \mathfrak{l}_3^2$

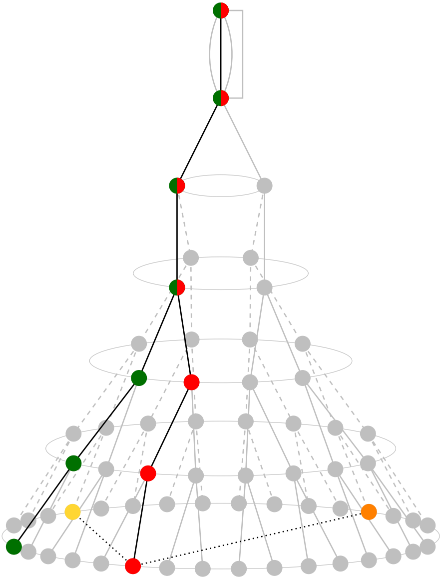




OSIDH PROTOCOL - AN EXAMPLE

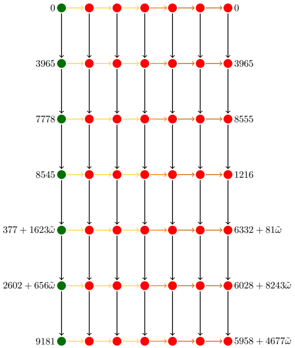
Bob secret key: $\mathfrak{l}_1^3 \mathfrak{l}_2 \mathfrak{l}_3^2$

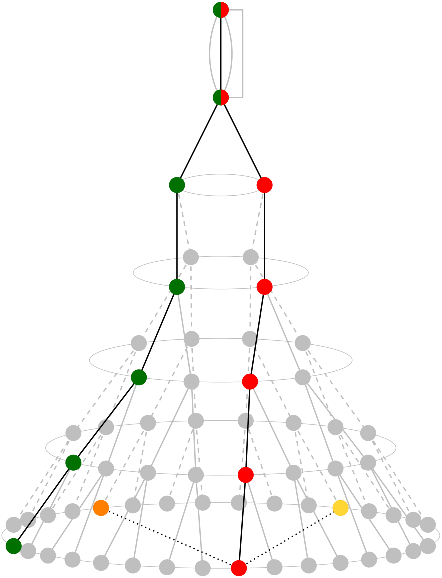




OSIDH PROTOCOL - AN EXAMPLE

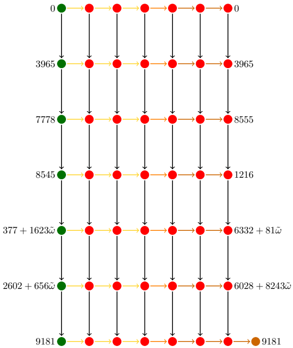
Bob secret key: $\mathfrak{l}_1^3\mathfrak{l}_2\mathfrak{l}_3^2$

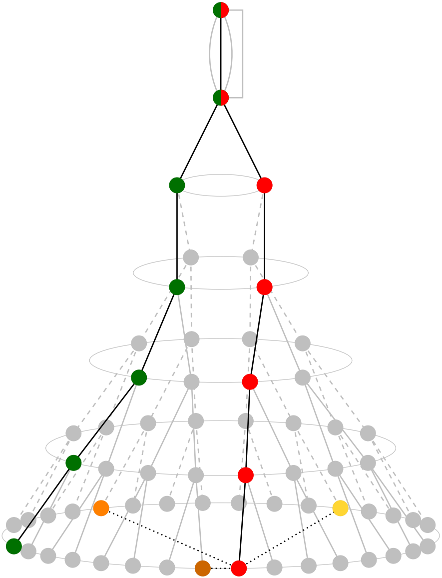




OSIDH PROTOCOL - AN EXAMPLE

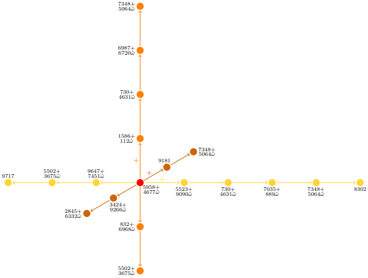
Bob secret key: $\mathfrak{l}_1^3\mathfrak{l}_2\mathfrak{l}_3^2$

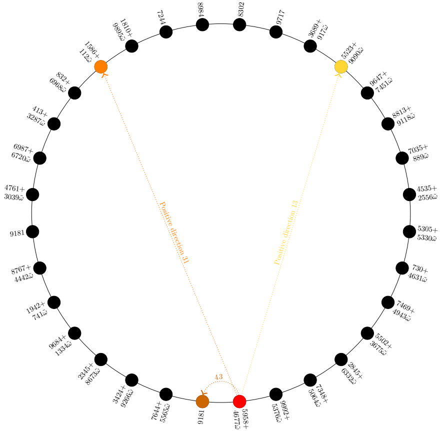




OSIDH PROTOCOL - AN EXAMPLE

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

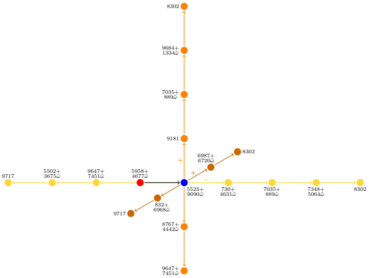


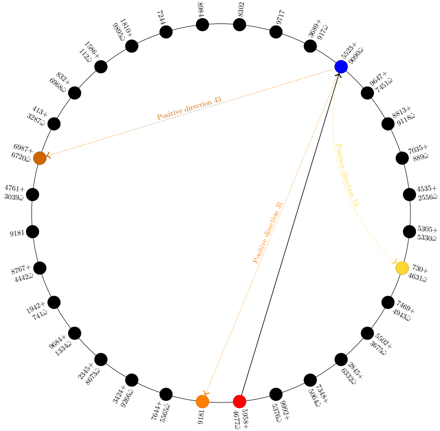


OSIDH PROTOCOL - AN EXAMPLE

L.COLÒ UWAT

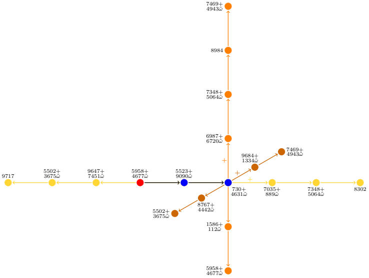
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$

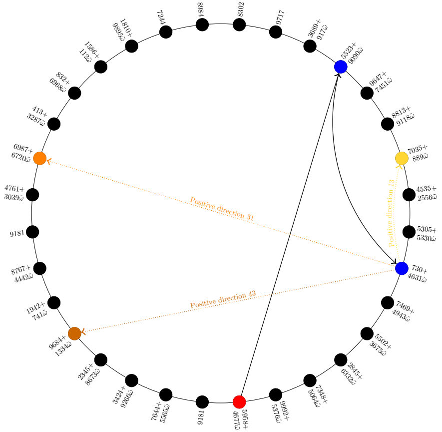




OSIDH PROTOCOL - AN EXAMPLE

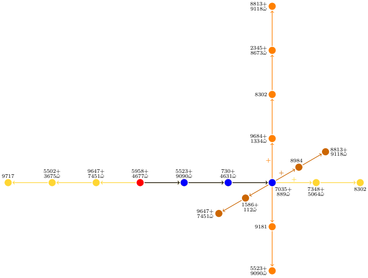
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$

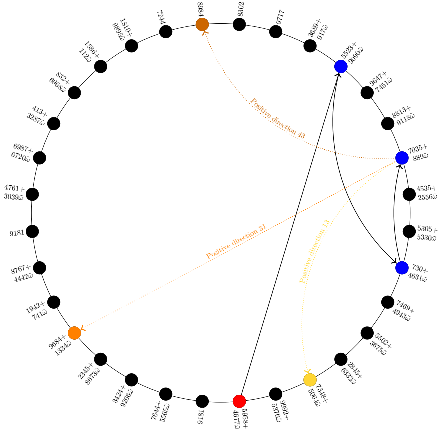




OSIDH PROTOCOL - AN EXAMPLE

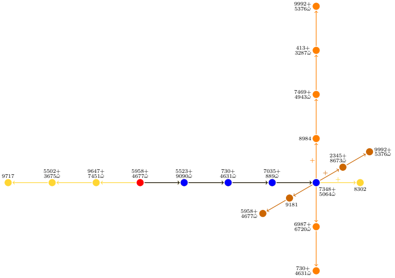
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$

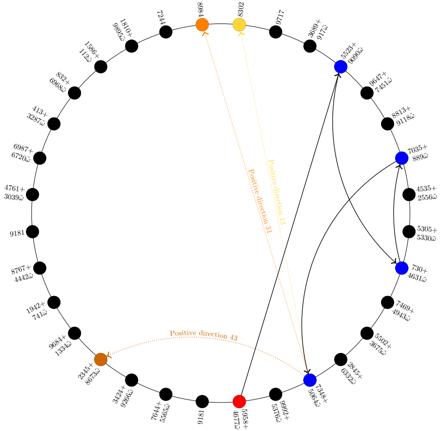




OSIDH PROTOCOL - AN EXAMPLE

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

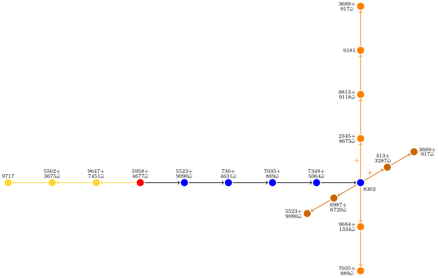


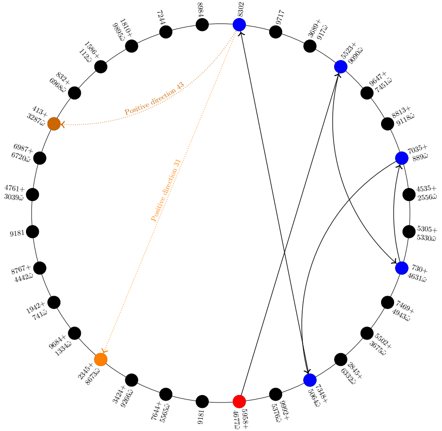


OSIDH PROTOCOL - AN EXAMPLE

L.COLÒ UWAT

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

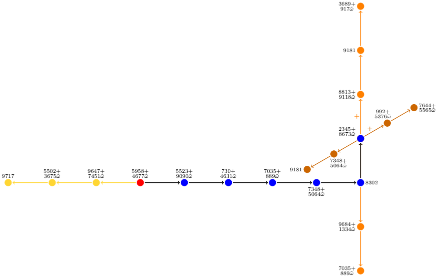


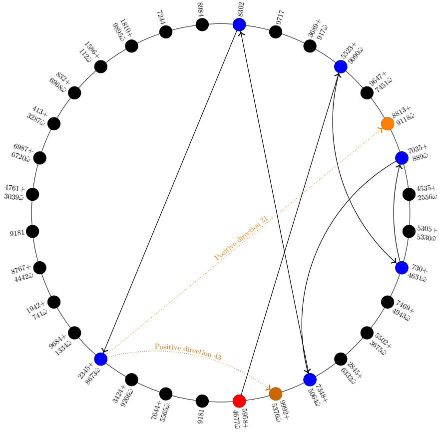


OSIDH PROTOCOL - AN EXAMPLE

L.COLÒ UWAT

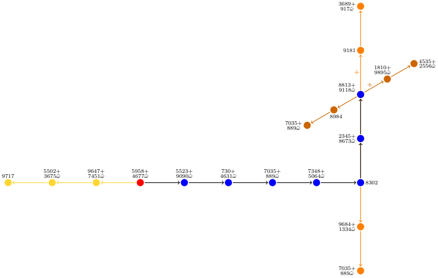
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$

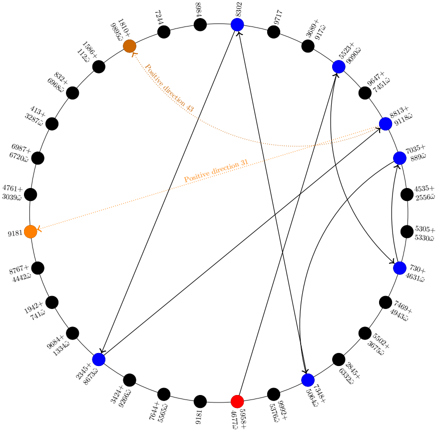




OSIDH PROTOCOL - AN EXAMPLE

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

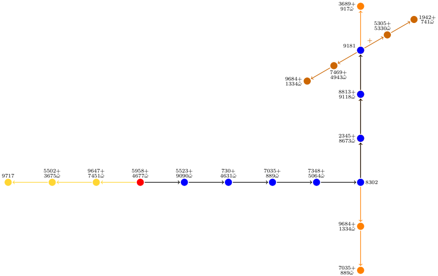


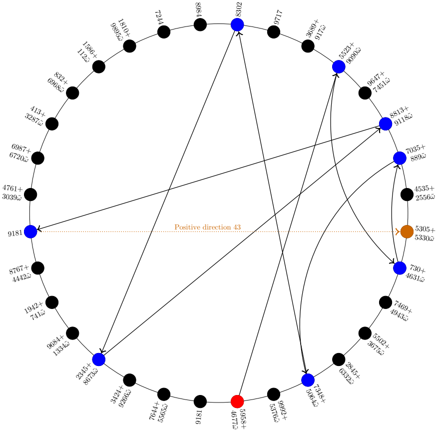


OSIDH PROTOCOL - AN EXAMPLE

L.COLÒ UWAT

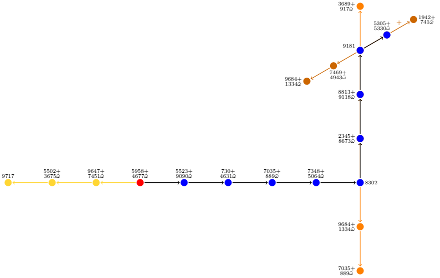
Alice secret key: $\mathfrak{l}_1^5\,\mathfrak{l}_2^3\,\mathfrak{l}_3^2$

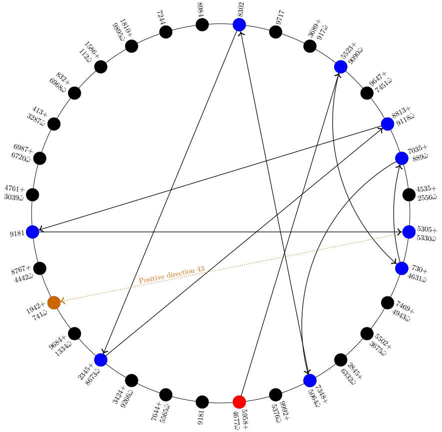




OSIDH PROTOCOL - AN EXAMPLE

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

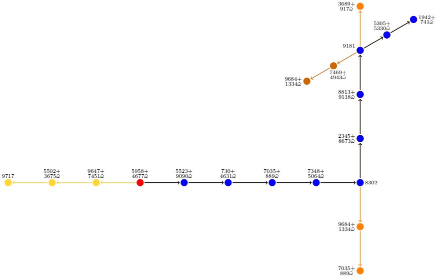


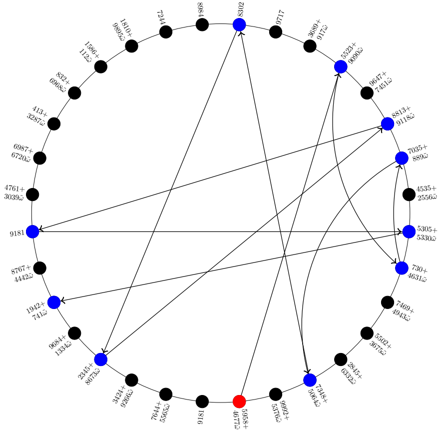


OSIDH PROTOCOL - AN EXAMPLE

L.COLÒ UWAT

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

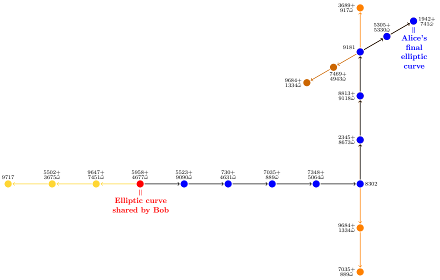


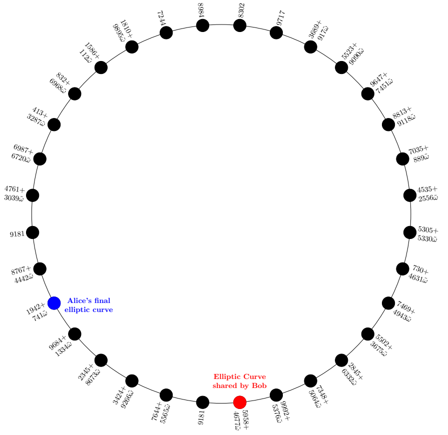


OSIDH PROTOCOL - AN EXAMPLE

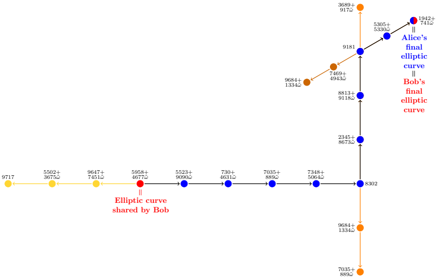
L.COLÒ UWAT

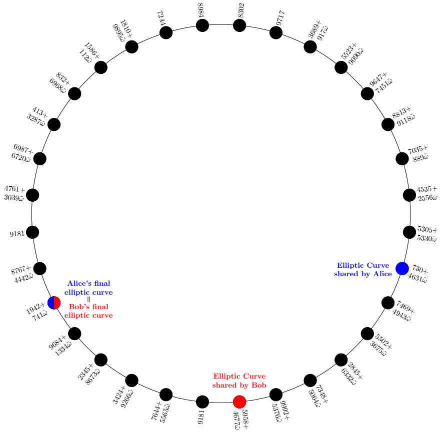
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$





OSIDH PROTOCOL - AN EXAMPLE





SECURITY CONSIDERATIONS

OSIDH PROTOCOL - SECURITY CONSIDERATIONS

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

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

We want the first map to be injective and the second one to be surjective. The attack of Dartois and De Feo exploits the non-injectivity of the map $I \to \mathrm{SS}_{\mathcal{O}}^{pr}(p)$ to recover an endomorphism of E.

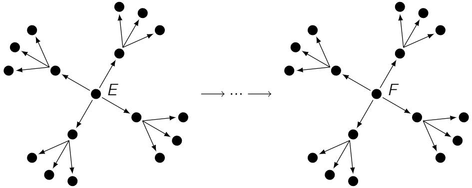
COUNTERMEASURES - THE USE OF NON-SPLIT PRIME

Key generation

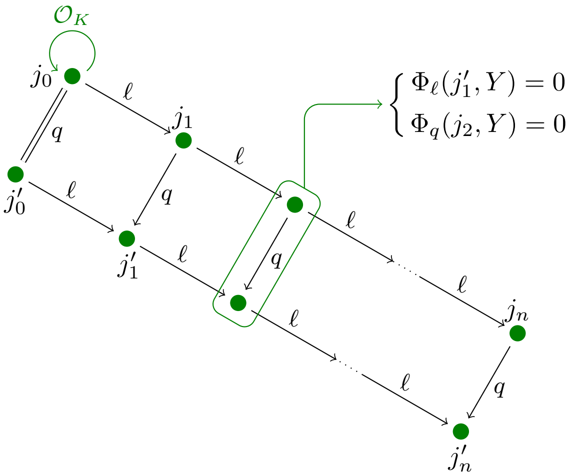
On one side, A begins with $F = E$.

- 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.



ADDING LEVEL STRUCTURE



$\mathcal{O}_K$
j_0
ℓ
q
j_1
j'_0
j'_1
j_n
j'_n
$\begin{cases} \Phi_\ell(j'_1, Y) = 0 \\ \Phi_q(j_2, Y) = 0 \end{cases}$

ADDING LEVEL STRUCTURE

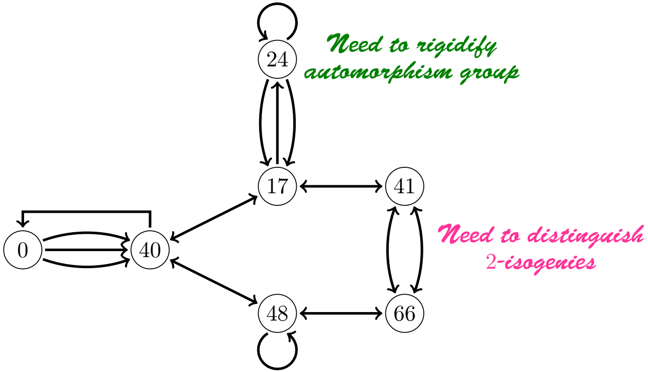
There are multiple reasons to add level structure to our construction:

- 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

L.COLÒ UWAT

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 $\mathcal{Cl}(\mathcal{O}, \Gamma)$).

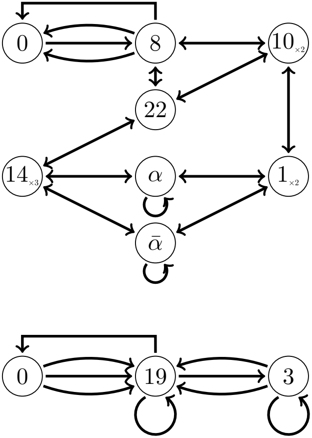
ADDING LEVEL STRUCTURE

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 $\mathcal{C}\ell(\mathcal{O}, \Gamma)$).
- q-modular polynomial of higher level are smaller.

ISOGENY GRAPHS WITH LEVEL STRUCTURE

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 $\psi(\Gamma(P,Q)) = \Gamma(P',Q')$.

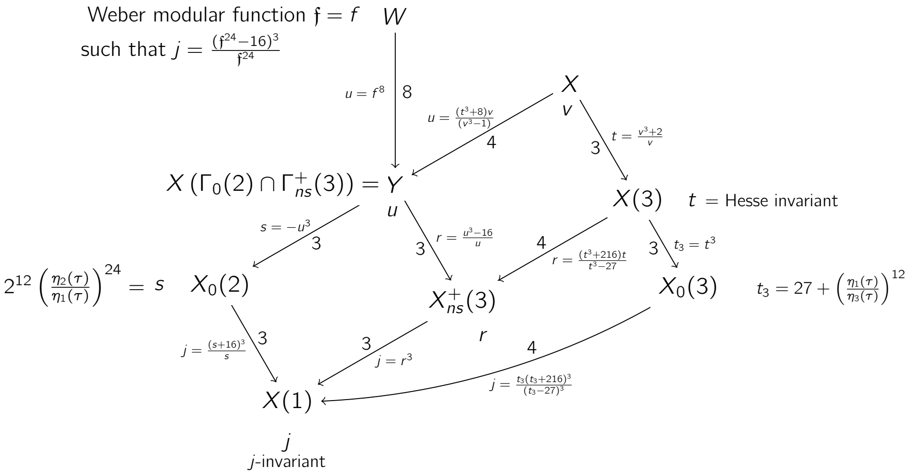


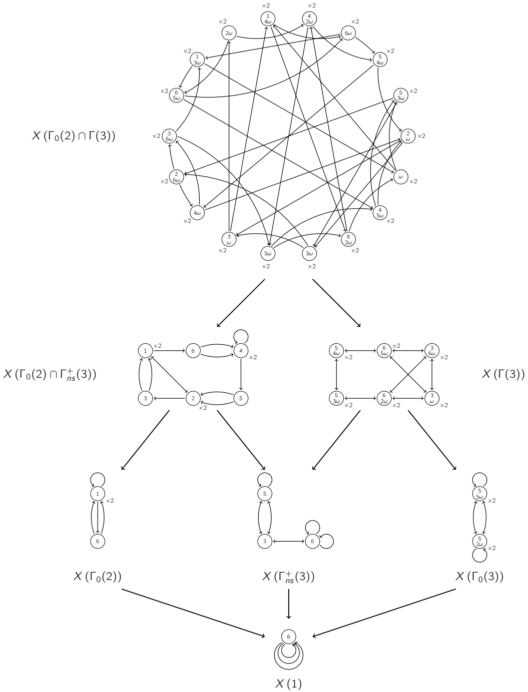
Eg. $\Gamma_0(N)$-structures.
Vertices (E, G) with $G \leq E[N]$ of order N
$\mathrm{End}(E,G) = \{\alpha \in \mathrm{End}(E) \mid \alpha(G) \subseteq G\}$ isomorphic to Eichler order.

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.

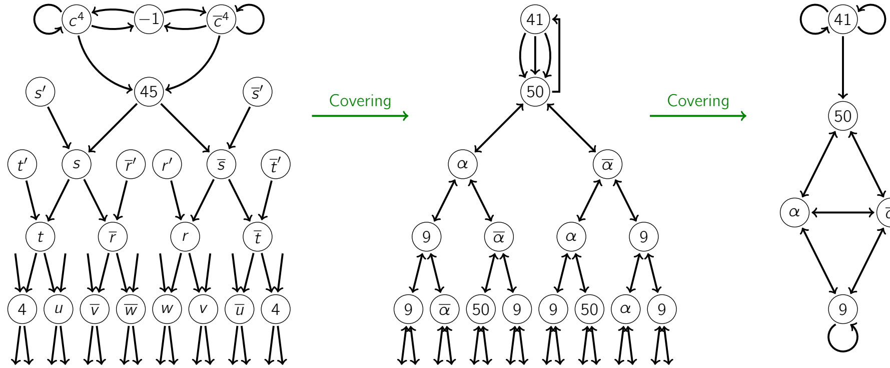
SOME MODULAR CURVES OF INTEREST




$X(\Gamma_0(2) \cap \Gamma(3))$
$X(\Gamma_0(2) \cap \Gamma_{ns}^{+}(3))$
$X(\Gamma(3))$
$X(\Gamma_0(2))$
$X(\Gamma_{ns}^{+}(3))$
$X(\Gamma_0(3))$
$X(1)$

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.



Weber Modular Polynomials

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

FORMAL ORIENTATIONS

FORMAL GROUP LAWS

Let Ω be any commutative ring with multiplicative identity 1 and $\Omega[\![\tau]\!]$ its ring of formal power series.

Definition

A formal group law $\mathcal{F}$ defined over Ω is a power series $F \in \Omega[\![X, Y]\!]$ such that

- $F(X, 0) = X$
- $F(X, Y) = F(Y, X)$
- $F(X, F(Y, Z)) = F(F(X, Y), Z)$

Notice that this implies that

$$F(X, Y) = X + Y + XYG(X, Y) \qquad G \in \Omega[\![X, Y]\!]$$

FORMAL GROUPS

Generally a formal group law is just a group operation with no underlying group. However, if the ring Ω is local and complete and the variables are assigned values from the maximal ideal $\mathfrak{m}$ of Ω, then the power series defining the formal group will converge in Ω, thus giving rise to a group.

Definition

The formal group associated to $\mathcal{F}/\Omega$, denoted $\mathcal{F}(\Omega)$ or $\mathcal{F}(\mathfrak{m})$, is the set $\mathfrak{m}$ together with the group operation

$$x \oplus_{\mathcal{F}} y = F(x, y) \qquad \forall x, y \in \mathfrak{m}$$

For example, if R is a commutative ring with 1 and $\Omega = R[\![\tau]\!]$, then $\mathfrak{m} = \tau R[\![\tau]\!]$ and a formal group law is a power series $F \in R[\![X, Y]\!]$ with zero constant term that makes $(\tau R[\![\tau]\!], \oplus_F)$ an abelian group.

EXAMPLES OF FORMAL GROUPS

Proposition

Let $(G, +)$ be an abelian group with identity 0_G. Suppose there is a one-to-one map $T : \tau R[\![\tau]\!] \to G$ such that $T(0) = 0_G$, and a power series $F \in R[\![X, Y]\!]$ with zero constant term such that

$$T(g) + T(h) = T(F(g, h)) \quad \forall g, h \in \tau R[\![\tau]\!]$$

Then F defines a formal group law.

Example. If $G = R[\![\tau]\!]$ under addition, and T is the inclusion $\tau R[\![\tau]\!] \hookrightarrow G$, $F(X, Y) = X + Y$ defines the additive group law.
Example. If $G = R[\![\tau]\!]^\times$ under multiplication, and T is the $g \mapsto 1 + g$, then

$$T(g)T(h) = (1 + g)(1 + h) = 1 + g + h + gh = T(g + h + gh)$$

and $F(X, Y) = X + Y + XY$ defines the multiplicative formal group law.
Example. If E is an elliptic curve over $L = \mathrm{Frac}(R[\![\tau]\!])$ we can construct a map $\tau R[\![\tau]\!] \to E(L)$ and find a power series defining a formal group law.

HOMOMORPHISMS OF FORMAL GROUPS

Definition

If $\mathcal{F}$ and $\mathcal{F}'$ are formal group laws, then a homomorphism from $\mathcal{F} \to \mathcal{F}'$ is a power series $U \in \tau R[\![\tau]\!]$ such that

$$U(F(X, Y)) = F'(U(X), U(Y))$$

In other words, U is such that $g \mapsto U(g)$ defines a homomorphism between the underlying groups.

Let $\mathcal{F}_1, \mathcal{F}_2$ be two formal group laws associated with the power series $F_1, F_2 \in R[\![X, Y]\!]$ and with maps T_1, T_2 to the abelian groups G_1, G_2. We can prove that if there are a group homomorphism $\psi : G_1 \to G_2$ and a power series $U \in \tau R[\![\tau]\!]$ such that

$$\psi(T_1(g)) = T_2(U(g))$$

then U is a homomorphism of formal group (laws).

HOMOMORPHISMS OF FORMAL GROUPS - EXAMPLES

$$\begin{array}{ccc} \tau R[\![\tau]\!] & \xrightarrow{\;T_1\;} & G_1 \\ {\scriptstyle U}\big\downarrow & & \big\downarrow{\scriptstyle \psi} \\ \tau R[\![\tau]\!] & \xrightarrow[\;T_2\;]{} & G_2 \end{array}$$

Example. Let $G_1 = G_2 = G$, $T_1 = T_2 = T$, $F_1 = F_2 = F$, and $\psi(g) = ng$, $n \in \mathbb{Z}$. Then $U = [n]$ is defined recursively by $[0] = 0$, $[1] = \tau$ and $[i+1]U = [i]\tau \oplus_F \tau$.

Example. For the additive formal group law, T is the inclusion $\tau R[\![\tau]\!] \hookrightarrow R[\![\tau]\!]$ and we get $ng = \psi(T(g)) = T(U(g)) = [n](g)$. So that $[n](\tau) = n\tau$.

Example. For the multiplicative formal group law we have $\psi(T(g)) = (1+g)^n$ and $T(U(g)) = 1 + [n]g$ so that

$$[n](\tau) = \sum_{i=1}^{n} \binom{n}{i} \tau^i$$

PARAMETRIZATION OF AN ELLIPTIC CURVE

Let E be an elliptic curve over a field K. We embed E in $\mathbb{P}^2_K$ as a Weierstrass curve

$$W(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3$$

with $O = (0:1:0)$. We choose local parameters at O: $z = -X/Y$ and $w = -Z/Y$. In particular, the pair (z,w) satisfy an algebraic relation

$$f_E(z,w) = z^3 + a_2z^2w + a_4zw^2 + a_6w^3 - w + (a_1z + a_3w)w$$

which can be used for Hensel lifting

$$w(z) = z^3 + a_1z^4 + (a_1^2 + a_2)z^5 + \dots$$

to a local point at O.

Lemma

We have $W(\tau, -1, w(\tau)) = 0$ in $R[\![\tau]\!]$. If $f, g \in \tau R[\![\tau]\!]$ and $W(f, -1, g) = 0$ then $g = w \circ f$.

FORMAL GROUP LAW OF AN ELLIPTIC CURVE

L.COLÒ UWAT

Let E be an elliptic curve over a field K. Let L be the quotient field of $K[\![\tau]\!]$. We can consider points in $E(L)$. Let R be a subring of K containing 1 and all the a_i's.

We construct a formal group law by embedding $\tau R[\![\tau]\!]$ into $E(L)$ and stealing its group law.

Consider points of the form $(z, 1, w) \in E(K)$. We have an embedding

$$T : \tau R[\![\tau]\!] \hookrightarrow E(L) \qquad f \mapsto (f, -1, w(f))$$

and we can find a power series F which gives rise to a formal group law.

$$F(X, Y) = X + Y - a_1 XY - a_2(X^2 Y + XY^2) + \text{higher terms}$$

Let $(R, \mathfrak{m})$ be any complete local K-algebra. We let $\widehat{E}$ be the formal completion of E at O. Then we have an isomorphism

$$\mathfrak{m} \xrightarrow{\cong} \widehat{E}(R) \qquad z \mapsto (z, w(z))$$

where $\mathfrak{m}$ is equipped with the group structure $z_1 \oplus z_2 = F_E(z_1, z_2)$.

FORMAL HOMOMORPHISMS ARISING FROM ISOGENIES

An isogeny of elliptic curves over K gives rise to a homomorphism of the corresponding formal group laws over K.

Let $I : E \to E'$ be an isogeny over K given by

$$I(X, Y, Z) = (f_1(X, Y, Z), f_2(X, Y, Z), f_3(X, Y, Z))$$

We get

$$\frac{f_1(X, Y, Z)}{f_2(X, Y, Z)} = \frac{f_1(z, -1, s)}{f_2(z, -1, s)} \in \mathfrak{m}$$

and we can expand $U = f_1/f_2$ as a power series, i.e., $U(\tau) = \sum_{i=1}^{+\infty} u_i \tau^i$.

Proposition

Let E, E', E'' be elliptic curves over K and F, F', F'' the associated formal group laws. If $I : E \to E'$ is an isogeny, then $U \in \mathrm{Hom}(F, F')$. This defines an embedding $\mathrm{Isog}(E, E') \hookrightarrow \mathrm{Hom}(F, F)$. If $I' : E' \to E''$ and I' corresponds to $U' \in \mathrm{Hom}(F', F'')$ then $I' \circ I$ corresponds to $U' \circ U \in \mathrm{Hom}(F, F'')$.

FORMAL ARITHMETIC - EXAMPLE

Let F be the formal group law over R of E. Let $g \in \tau R[\![\tau]\!]$.

$$[-1]T(g) = [-1](g, -1, w(g)) = \left(\frac{-g}{1 - a_1 g - a_3 w(g)}, -1, \frac{-w(g)}{1 - a_1 g - a_3 w(g)} \right)$$

and by the Lemma above this is $T(\frac{-g}{1-a_1 g - a_3 w(g)})$. This means that

$$\widehat{[-1]} = \frac{-\tau}{1 - a_1\tau - a_3 w(\tau)} = -\tau \sum_{n=0}^{+\infty} (a_1\tau + a_3 w)^n$$

A similar calculation for [2] yields

$$\widehat{[2]} = 2\tau + \text{higher terms}$$

More in general, for any $n \in \mathbb{Z}$, formal scalar multiplication $\widehat{[n]}$ satisfies:

$$\widehat{[n]} = nz + \text{higher terms}$$

In particular, by reversion of power series, if n is invertible in K, then the inverse of $[n]$ is well-defined:

$$\widehat{[n]}^{-1} = \frac{1}{n} z + \cdots$$

It follows that $\mathbb{Z}_{(p)} \subseteq \text{End}(\widehat{E})$.

N.B. Here we are indeed identifying z with (z, w) under $\mathfrak{m} \cong \widehat{E}(R)$ we hereafter write simply $\widehat{\alpha}(\tau) = \alpha_1 z + \alpha_2 z^2 + \ldots$ for a formal morphism $\widehat{\alpha}$.

FORMAL ISOGENIES

Let $\alpha : E \to F$ be an isogeny of elliptic curves over K, whose degree n is invertible in K, let β be its dual isogeny, and let

$$\widehat{\alpha} : \widehat{E} \longrightarrow \widehat{F},$$

be its formal completion, given by $\widehat{\alpha}(z) = \alpha_1 z + \alpha_2 z^2 + \cdots$.

Since $\beta \circ \alpha = [n]$, we have

$$\widehat{\beta}(z) = \beta_1 z + \cdots = \frac{n}{\alpha_1} z + \cdots$$

and $\widehat{\alpha}$ is invertible in $\mathrm{Hom}(\widehat{E}, \widehat{F})$, with inverse:

$$\widehat{\alpha}^{-1}(z) = \widehat{[n]}^{-1} \circ \widehat{\beta}(z) = \frac{1}{\alpha_1} z + \cdots$$

The isogeny is *normalized* if $\alpha_1 = 1$.

FORMAL ENDOMORPHISM RINGS

It follows that for $p = \mathrm{char}(k) > 0$, we have

$$\mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} \mathrm{End}(E) \subseteq \mathrm{End}(\widehat{E})$$

and more generally $\mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} \mathrm{Hom}(E, F) \subseteq \mathrm{Hom}(\widehat{E}, \widehat{F})$. In fact the formal endomorphism ring contains the completion:

$$\mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} \mathrm{End}(E) \subseteq \mathrm{End}(E)_{\mathfrak{P}} \subseteq \mathrm{End}(\widehat{E}),$$

of the endomorphism ring at the prime

$$\mathfrak{P} = \mathrm{Hom}(E^{\sigma}, E)\pi \subset \mathrm{End}(E),$$

where $\pi : E \to E^{\sigma}$ is the Frobenius p-isogeny.

$$\mathrm{End}(E)_{\mathfrak{P}} \cong \begin{cases} \mathbb{Z}_p & \text{if } E \text{ is ordinary, or} \\ \mathcal{O}_{\mathfrak{P}} & \text{if } E \text{ is supersingular,} \end{cases}$$

where $\mathcal{O}_{\mathfrak{P}}$ is the maximal $\mathbb{Z}_p$-order of the nonsplit quaternion algebra over $\mathbb{Q}_p$.

FORMAL ISOGENY PULLBACK

We use the principle that a formal isogeny of degree coprime to p is invertible to equip an elliptic curve E with formal quaternionic multiplication.

Suppose the $p \equiv 11 \bmod 12$, and let E_0 and E_1 be elliptic curves oriented by

$$\mathbb{Z}[j] \cong \mathbb{Z}[\zeta_3] \text{ and } \mathbb{Z}[i] \cong \mathbb{Z}[\zeta_4],$$

respectively. Let $\alpha : E_0 \to E$ and $\beta : E_1 \to E$ be (smooth) isogenies of degree coprime to p.

$$j \circlearrowright E_0 \xrightarrow{\quad\alpha\quad} \cdots \longrightarrow \bullet \longrightarrow E \longleftarrow \bullet \longleftarrow \cdots \xleftarrow{\quad\beta\quad} E_1 \circlearrowleft i$$

We define:

$$\widehat{j} = \widehat{\alpha} \circ \widehat{j} \circ \widehat{\alpha}^{-1} \text{ and } \widehat{i} = \widehat{\beta} \circ \widehat{i} \circ \widehat{\beta}^{-1} \text{ in } \mathrm{End}(\widehat{E}).$$

Then we have an effective subring $\mathbb{Z}_{(p)}[\widehat{i}, \widehat{j}] \subseteq \mathrm{End}(\widehat{E})$.

ORIENTATIONS OF SUPERSINGULAR FORMAL GROUPS

Let $E_0 \xrightarrow{\phi_0} E_1 \xrightarrow{\phi_1} \cdots \xrightarrow{\phi_{n-1}} E_n$ be an ℓ-isogeny chain. The formal group functor $\mathcal{F}$ induces a formal ℓ-isogeny chain:

$$\mathcal{F}(E_0) \xrightarrow{\mathcal{F}(\phi_0)} \mathcal{F}(E_1) \xrightarrow{\mathcal{F}(\phi_1)} \cdots \xrightarrow{\mathcal{F}(\phi_{n-1})} \mathcal{F}(E_n),$$

and given an endomorphism ψ of E_0, we define $\mathcal{F}(\psi)_0 = \mathcal{F}(\psi)$ and recursively, for each i, a formal endomorphism $\mathcal{F}(\psi)_{i+1}$ of $\mathcal{F}(E_{i+1})$:

$$\mathcal{F}(\psi)_{i+1} = \mathcal{F}([\ell])^{-1} \circ \mathcal{F}(\phi_i) \circ \mathcal{F}(\psi)_i \circ \mathcal{F}(\hat{\phi}_i).$$

We derive conditions under which an endomorphism ϕ of E_0 induces an integral formal endomorphism of $\mathcal{F}(E_i)$.

EFFECTIVE FORMAL ENDOMORPHISM RING

The problem remains to effectively cut out ℓ-torsion subgroups using formal endomorphisms: Given $\widehat{\alpha}$, determine $\ker(\widehat{\alpha}) \cap E[\ell]$, or more generally a map to $\mathbb{M}_2(\mathbb{F}_\ell) = \mathrm{End}(E[\ell])$.

Since formal endomorphisms operate locally at O, one needs an algorithm for extending $\widehat{\alpha}$ to $\widehat{E} \times E[\ell] \to \widehat{E} \times E[\ell]$.

In order to extend formal endomorphisms, we need instead a formal canonical lift to $\mathbb{Z}_p$ (characteristic 0) and interpolation.

WORK IN PROGRESS

THANK YOU FOR YOUR ATTENTION

REFERENCES FOR THE FORMAL GROUP SECTION

- Antonia W. Bluher, *Formal groups, elliptic curves, and some theorems of Couveignes*, 1998.
- Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Ch IV.
- David Kohel's talk at SIAM Conference:
  https://videocollege.tue.nl/Mediasite/Channel/siam-2023-event/watch/6d2dbd97b4d649ab8b0c52c06070db501d