MARSEILLE, 26 SEPTEMBER 2019

L.COLÒ I2M

ORIENTING SUPERSINGULAR ISOGENY GRAPHS

LEONARDO COLÒ & DAVID KOHEL

Institut de Mathématiques de Marseille

Séminaire ATI - Arithmétique et Théorie de l'Information

Isogeny graphs

Definition

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

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

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

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

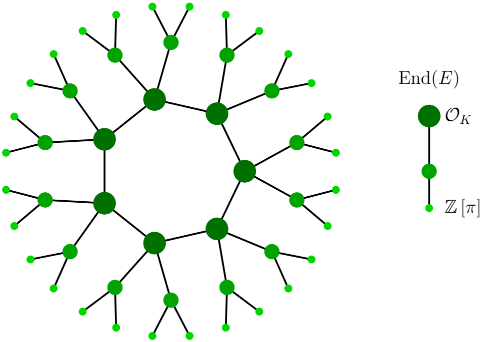
The ℓ-isogeny graph of E is $(\ell + 1)$-regular (as a directed multigraph). In characteristic 0, if $\mathsf{End}(E) = \mathbb{Z}$, then this graph is a tree.

ORDINARY ISOGENY GRAPHS: VOLCANOES

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

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

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



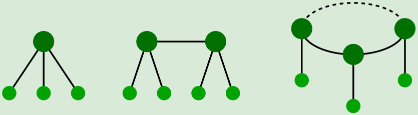
STRUCTURE OF VOLCANOES

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

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

Crater

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



$\left(\frac{\Delta_K}{\ell}\right) = -1$ $\quad$ $\left(\frac{\Delta_K}{\ell}\right) = 0$ $\quad$ $\left(\frac{\Delta_K}{\ell}\right) = +1$

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

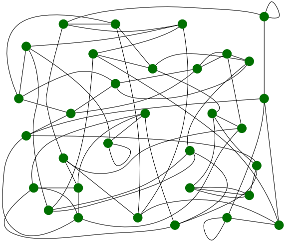
SUPERSINGULAR ISOGENY GRAPHS

L.COLÒ I2M

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

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

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



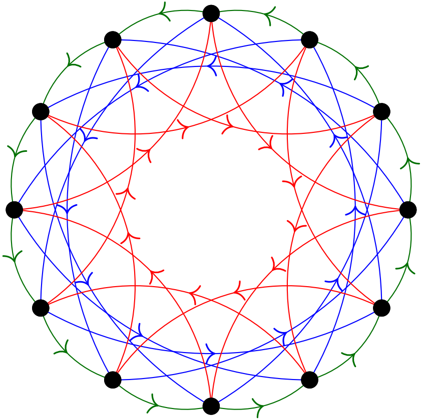
For this reason, supersingular isogeny graphs have been proposed for

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

ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

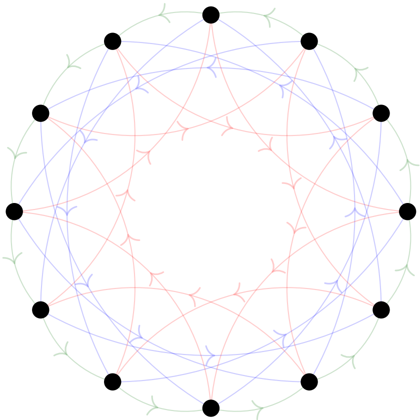
Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$



Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

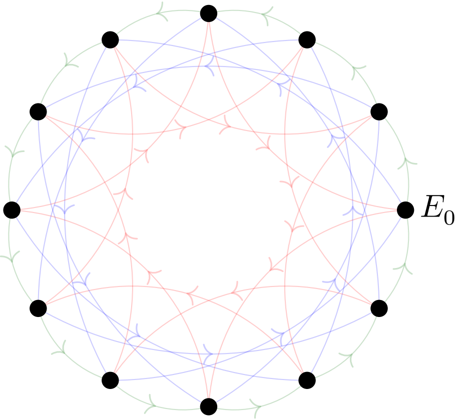
$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$



ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$



ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

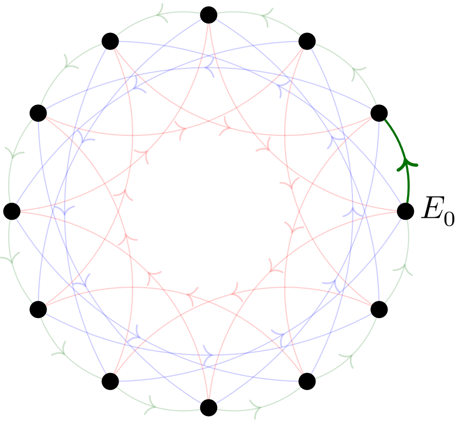
Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

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

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



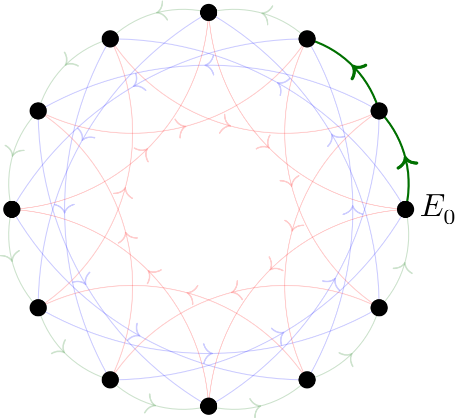
Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.
Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

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

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



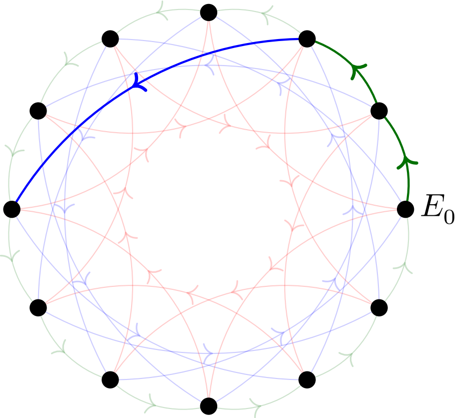
Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

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

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

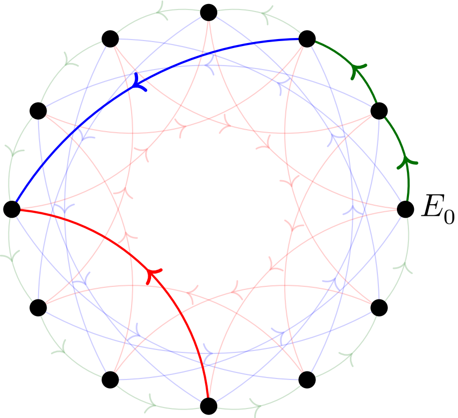
Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

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

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



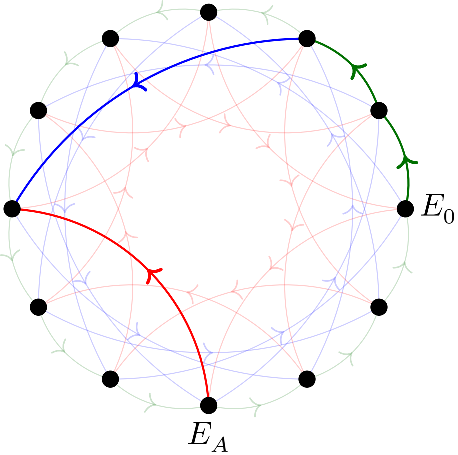
Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

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

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



Ordinary protocol - Couveignes & Rostovtsev-Stolbunov, 2006

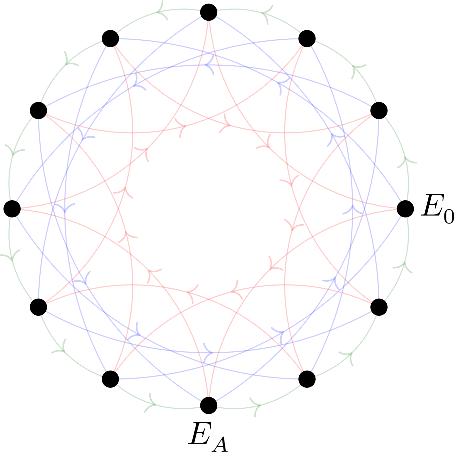
Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

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

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



Bob

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

$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

Ordinary protocol - Couveignes & Rostovtsev-Stolbunov, 2006

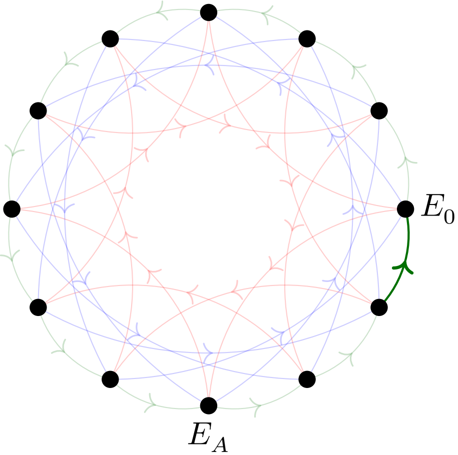
Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

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

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



Bob

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

$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

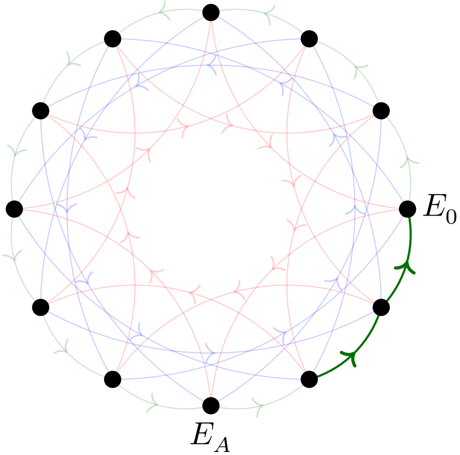
Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

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

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



Bob

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

$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

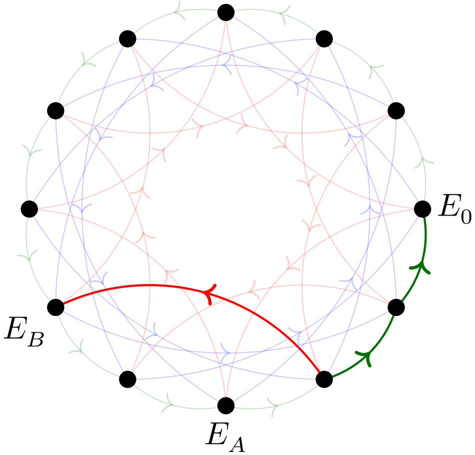
Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

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

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



Bob

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

$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

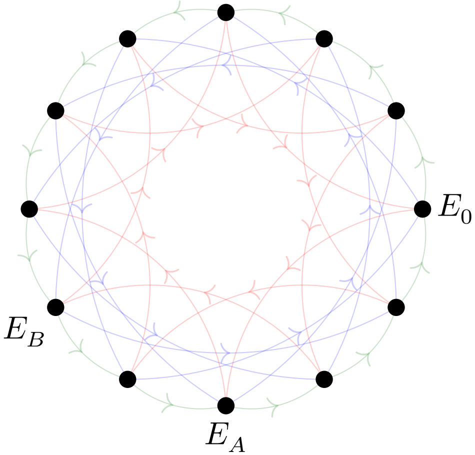
Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

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

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



Bob

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

$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

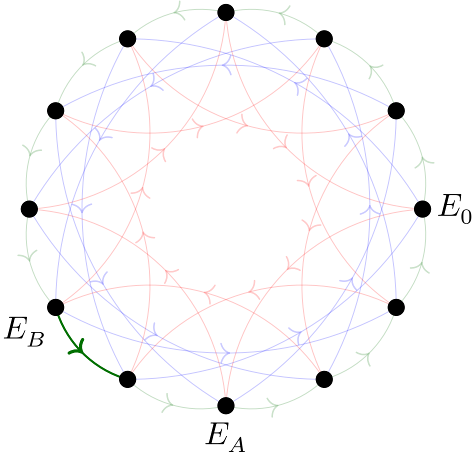
Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.
Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

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

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



Bob

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

$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

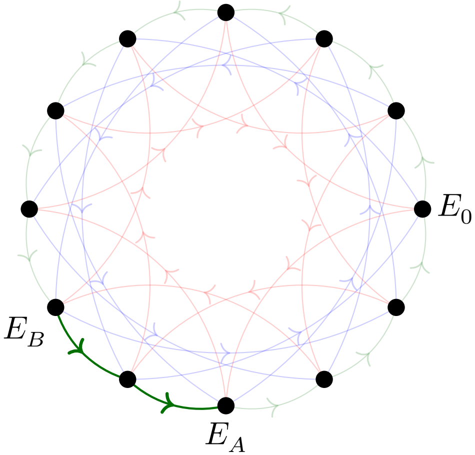
Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

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

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



Bob

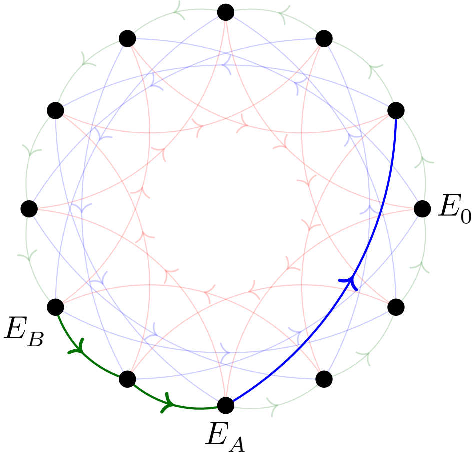
$\rho_B = (-2, 0, 1)$

$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice
$\rho_A = (2, 1, -1)$
$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



Bob
$\rho_B = (-2, 0, 1)$
$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

L.COLÒ I2M

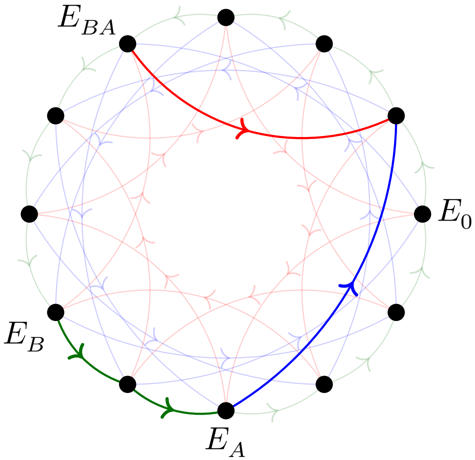
Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

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

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



Bob

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

$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

Ordinary protocol - Couveignes & Rostovtsev-Stolbunov, 2006

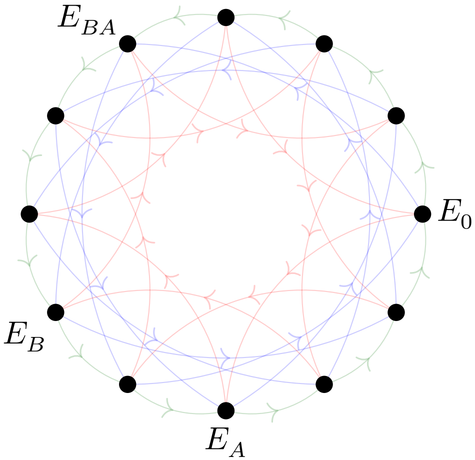
Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

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

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



Bob

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

$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

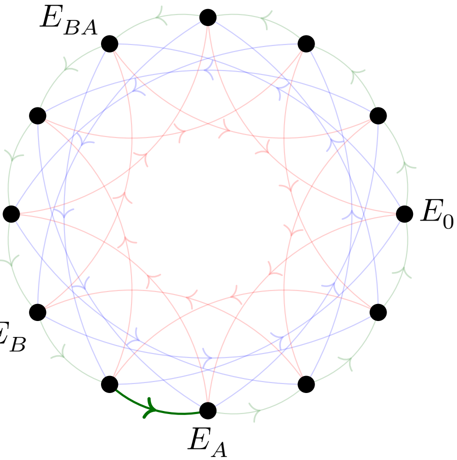
Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

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

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



Bob

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

$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

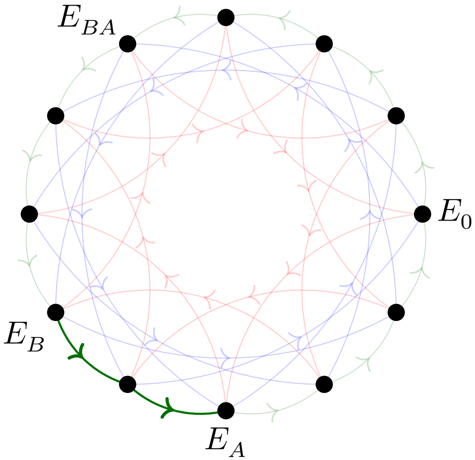
Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

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

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



Bob

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

$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

Ordinary protocol - Couveignes & Rostovtsev-Stolbunov, 2006

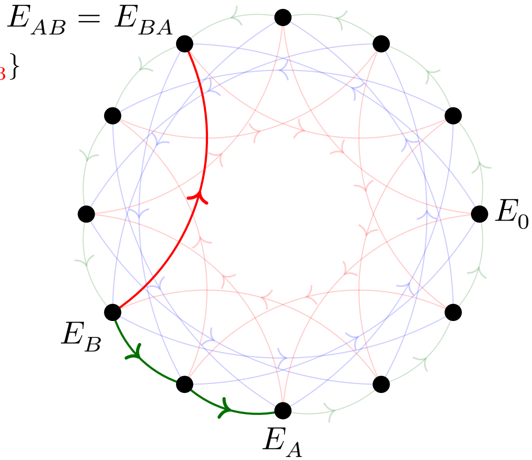
Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

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

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



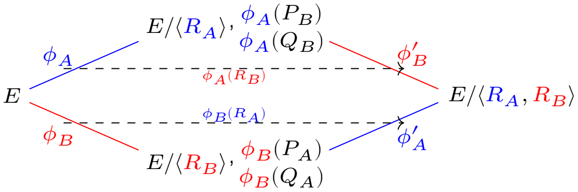
Bob

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

$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

Supersingular isogeny Diffie-Hellman

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



CSIDH - Castryck, Lange, Martindale, Panny & Renes, 2018

L.COLÒ I2M

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

Commutative Supersingular isogeny Diffie-Hellman

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

MOTIVATING OSIDH

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

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

Motivation

- Generalize CSIDH.
- Key space of SIDH: in order to have the two key spaces of similar size, we need to take $\ell_A^a \approx \ell_B^b \approx \sqrt{p}$. This implies that the space of choices for the secret key is limited to a fraction of the whole set of supersingular j-invariants over $\mathbb{F}_{p^2}$.
- A feature shared by SIDH and CSIDH is that the isogenies are constructed as quotients of rational torsion subgroups. The need for rational points limits the choice of the prime p

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 inclusion $\iota : \mathcal{O} \hookrightarrow \mathrm{End}(E)$, and a *$K$-orientation* is an inclusion $\iota : K \hookrightarrow \mathrm{End}^0(E) = \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$. 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.

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 ELLIPTIC CURVES AND VOLCANOES

As we have seen, one feature of the ℓ-isogeny graphs of CM elliptic curves is that in each component, depending on whether ℓ is split, inert, or ramified in K, there is a cycle of vertices, unique vertex, or adjacent pair of vertices which have ℓ-maximal endomorphism ring.

Chains of ℓ-isogenies leading away from these ℓ-maximal vertices have successively (and strictly) smaller endomorphism rings, by a power of ℓ.

This lets us define the depth of a CM elliptic curve E (i.e. vertex) in the ℓ-isogeny graph as the valuation of the index $[\mathcal{O}_K : \mathrm{End}(E)]$ at ℓ, which measures the distance to an ℓ-maximal vertex.

Consequently, we obtain a notion of depth at ℓ in the K-oriented supersingular ℓ-isogeny graph.

We also recover the notion of horizontal, ascending and descending isogenies.

CLASS GROUP ACTION

- $\mathrm{SS}(p) = \{$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$\}$.
- $\mathrm{SS}_{\mathcal{O}}^{pr}(p)$ =subset of primitive $\mathcal{O}$-oriented curves.

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

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

Proposition

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

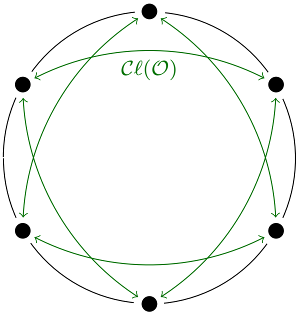
In particular, for fixed primitive $\mathcal{O}$-oriented E, we obtain a bijection of sets:

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

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

VORTEX

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

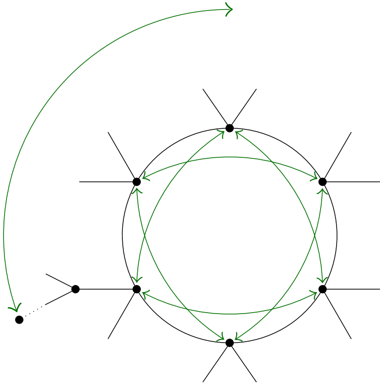


Instead of considering the union of different isogeny graphs, we focus on one single crater and we think of all the other primes as acting on it: the resulting object is a single isogeny circle rotating under the action of $\mathcal{C}\ell(\mathcal{O})$.

WHIRLPOOL

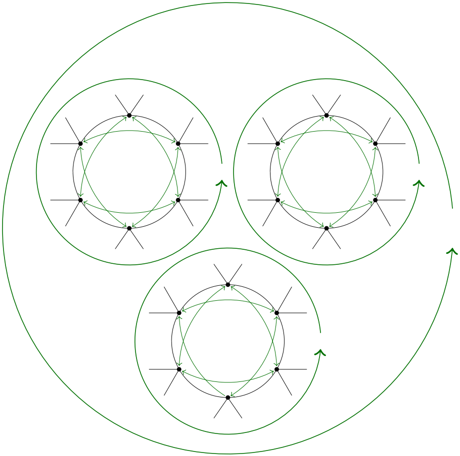
The action of $\mathcal{C}\ell(\mathcal{O})$ extends to the union $\bigcup_i SS_{\mathcal{O}_i}(p)$ over all superorders $\mathcal{O}_i$ containing $\mathcal{O}$ via the surjections $\mathcal{C}\ell(\mathcal{O}) \to \mathcal{C}\ell(\mathcal{O}_i)$.

We define a *whirlpool* to be a complete isogeny volcano acted on by the class group. We would like to think at isogeny graphs as moving objects.



WHIRLPOOL

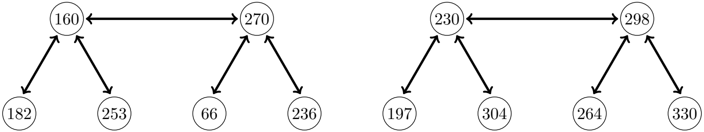
Actually, we would like to take the ℓ-isogeny graph on the full $\mathcal{C}\ell(\mathcal{O}_K)$-orbit. This might be composed of several ℓ-isogeny orbits (craters), although the class group is transitive.



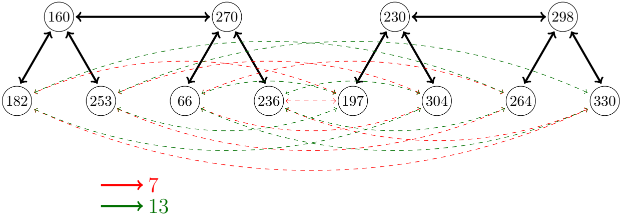
WHIRLPOOL: AN EXAMPLE

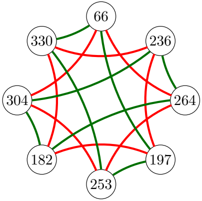
The set of multiple ℓ-volcanoes is called ℓ-cordillera.

Example. $p = 353, \ell = 2$, elliptic curves with 344 $\mathbb{F}_{353}$-rational points.



A whirlpool is the union of the two, shuffled by the class group of $\mathbb{Z}[2\sqrt{-82}]$.





ISOGENY CHAINS

L.COLÒ I2M

Definition

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

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

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

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

Lemma

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

PUSHING ISOGENIES ALONG A CHAIN

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

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

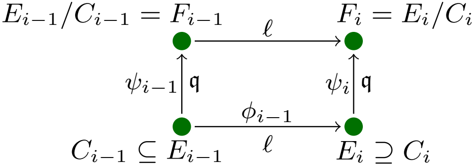
If $\mathfrak{q}$ is a split prime in $\mathcal{O}_K$ over $q \neq \ell, p$, then the isogeny

$$\psi_0 : E_0 \to F_0 = E_0/E_0\left[\mathfrak{q}\right]$$

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

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

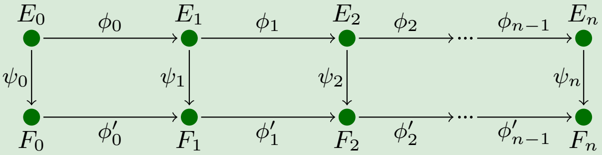
and defining $F_i = E_i/C_i$.



LADDERS

Definition

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



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

We say that an ℓ-ladder is ascending (or descending, or horizontal) if the ℓ-isogeny chain (E_i, ϕ_i) is ascending (or descending, or horizontal, respectively).

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

EFFECTIVE ENDOMORPHISM RINGS AND ISOGENIES

L. COLÒ I2M

We say that a subring of End(E) is effective if we have explicit polynomials or rational functions which represent its generators.

Examples. $\mathbb{Z}$ in End(E) is effective. Effective imaginary quadratic subrings $\mathcal{O} \subset$ End(E), are the subrings $\mathcal{O} = \mathbb{Z}[\pi]$ generated by Frobenius

In the Couveignes-Rostovtsev-Stolbunov constructions, or in the CSIDH protocol, one works with $\mathcal{O} = \mathbb{Z}[\pi]$.

- For large finite fields, the class group of $\mathcal{O}$ is large and the primes $\mathfrak{q}$ in $\mathcal{O}$ have no small generators.
  Factoring the division polynomial $\psi_q(x)$ to find the kernel polynomial of degree $(q-1)/2$ for $E[\mathfrak{q}]$ becomes relatively expensive.
- In SIDH, the ordinary protocol of De Feo, Smith, and Kieffer, or CSIDH, the curves are chosen such that the points of $E[\mathfrak{q}]$ are defined over a small degree extension κ/k, and working with rational points in $E(\kappa)$.
- We propose the use of an effective CM order $\mathcal{O}_K$ of class number 1.
  The kernel polynomial can be computed directly without need for a splitting field for $E[\mathfrak{q}]$, and the computation of a generator isogeny is a one-time precomputation.

MODULAR APPROACH

The use of modular curves for efficient computation of isogenies has an established history (see Elkies)

Modular Curve

The modular curve $\mathtt{X}(1) \simeq \mathbb{P}^1$ classifies elliptic curves up to isomorphism, and the function j generates its function field.

The modular polynomial $\Phi_m(X, Y)$ defines a correspondence in $\mathtt{X}(1) \times \mathtt{X}(1)$ such that $\Phi_m(j(E), j(E')) = 0$ if and only if there exists a cyclic m-isogeny ϕ from E to E', possibly over some extension field.

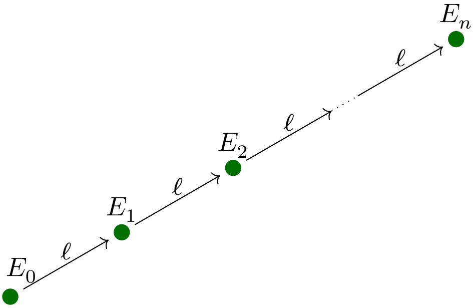
Definition

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

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

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

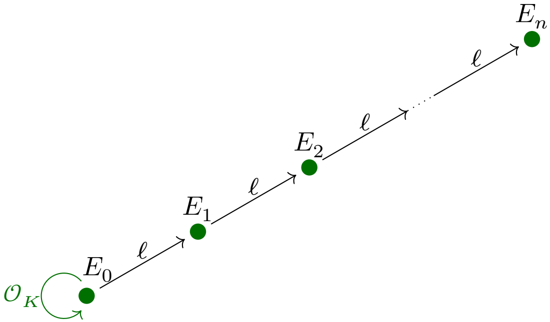
We consider an elliptic curve E_0 with an effective endomorphism ring (eg. $j_0 = 0, 1728$) and a chain of ℓ-isogenies.



OSIDH - Introduction

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

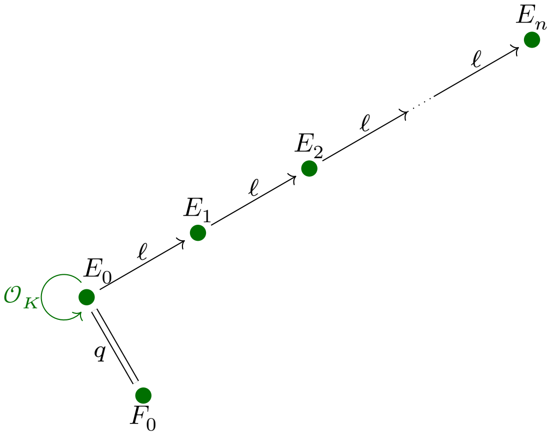
- For $\ell = 2$ (or 3) a suitable candidate for $\mathcal{O}_K$ could be the Gaussian integers $\mathbb{Z}[i]$ or the Eisenstein integers $\mathbb{Z}[\omega]$.



L.COLÒ I2M

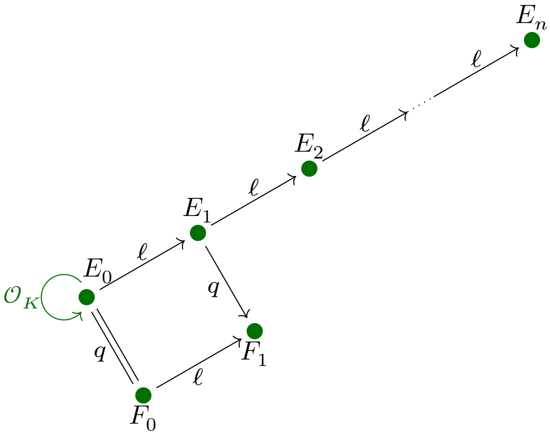
We consider an elliptic curve E_0 with an effective endomorphism ring (eg. $j_0 = 0, 1728$) and a chain of ℓ-isogenies.

- Horizontal isogenies must be endomorphisms



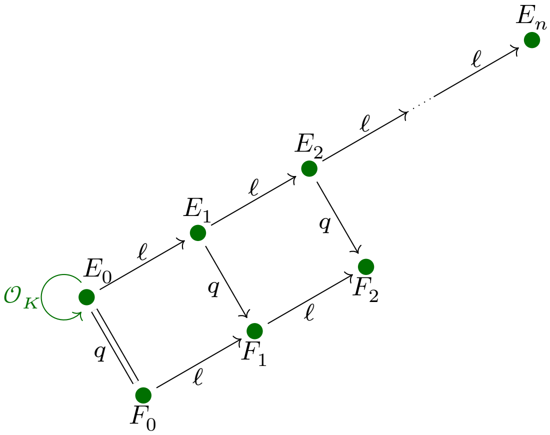
We consider an elliptic curve E_0 with an effective endomorphism ring (eg. $j_0 = 0, 1728$) and a chain of ℓ-isogenies.

- We push forward our q-orientation obtaining F_1.



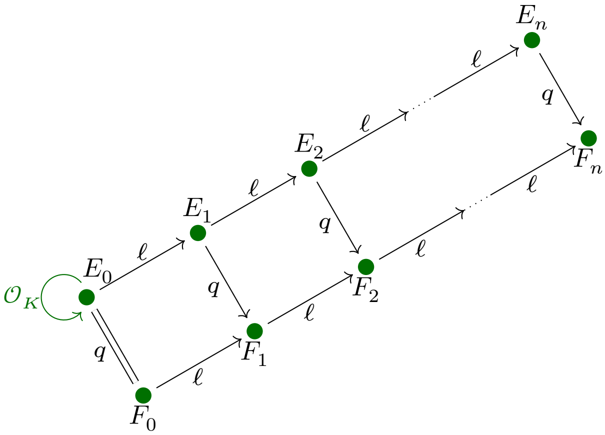
We consider an elliptic curve E_0 with an effective endomorphism ring (eg. $j_0 = 0, 1728$) and a chain of ℓ-isogenies.

- We repeat the process for F_2.

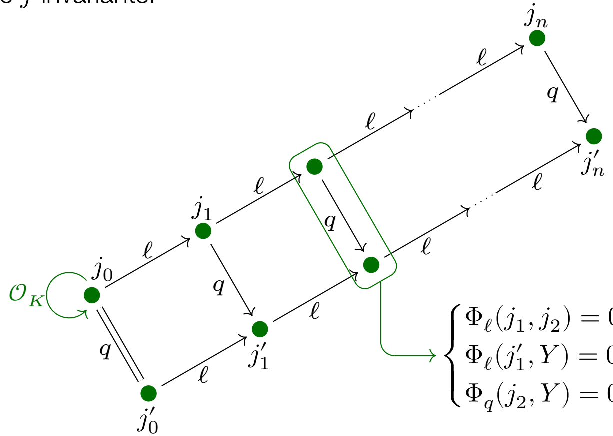


We consider an elliptic curve E_0 with an effective endomorphism ring (eg. $j_0 = 0, 1728$) and a chain of ℓ-isogenies.

- And again till F_n.



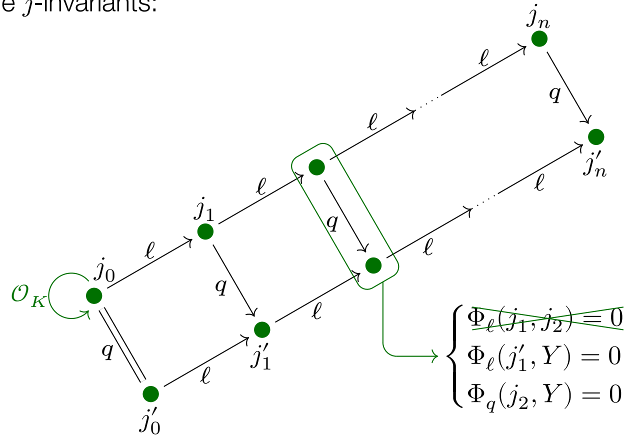
If we look at modular polynomials $\Phi_\ell(X,Y)$ and $\Phi_q(X,Y)$ we realize that all we need are the j-invariants:



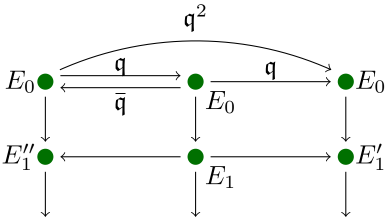
$$\begin{cases} \Phi_\ell(j_1, j_2) = 0 \\ \Phi_\ell(j'_1, Y) = 0 \\ \Phi_q(j_2, Y) = 0 \end{cases}$$

L.COLÒ I2M

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



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



$E_i' \neq E_i''$ 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

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

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

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

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

A FIRST NAIVE PROTOCOL

L.COLÒ I2M

PUBLIC DATA: A chain of ℓ-isogenies $E_0 \to E_1 \to ... \to E_n$		
	ALICE	**BOB**

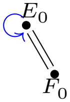
A FIRST NAIVE PROTOCOL

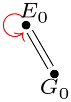
L.COLÒ I2M

PUBLIC DATA: A chain of ℓ-isogenies $E_0 \to E_1 \to ... \to E_n$

ALICE **BOB**

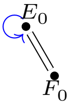
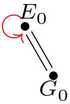
Choose a primitive $\mathcal{O}_K$-orientation of E_0





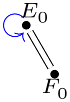
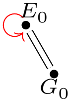
A FIRST NAIVE PROTOCOL

PUBLIC DATA: A chain of ℓ-isogenies $E_0 \to E_1 \to ... \to E_n$

	ALICE	**BOB**
Choose a primitive $\mathcal{O}_K$-orientation of E_0		
Push it forward to depth n	$\underbrace{E_0 = F_0 \to F_1 \to ... \to F_n}_{\phi_A}$	$\underbrace{E_0 = G_0 \to G_1 \to ... \to G_n}_{\phi_B}$

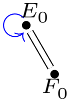
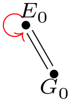
A FIRST NAIVE PROTOCOL

PUBLIC DATA: A chain of ℓ-isogenies $E_0 \to E_1 \to \ldots \to E_n$

	ALICE	**BOB**
Choose a primitive $\mathcal{O}_K$-orientation of E_0		
Push it forward to depth n	$\underbrace{E_0 = F_0 \to F_1 \to \ldots \to F_n}_{\phi_A}$	$\underbrace{E_0 = G_0 \to G_1 \to \ldots \to G_n}_{\phi_B}$
Exchange data	$\{G_i\}_{i=1}^n$	$\{F_i\}_{i=1}^n$

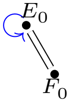
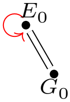
A FIRST NAIVE PROTOCOL

PUBLIC DATA: A chain of ℓ-isogenies $E_0 \to E_1 \to \ldots \to E_n$

	ALICE	**BOB**
Choose a primitive $\mathcal{O}_K$-orientation of E_0		
Push it forward to depth n	$\underbrace{E_0 = F_0 \to F_1 \to \ldots \to F_n}_{\phi_A}$	$\underbrace{E_0 = G_0 \to G_1 \to \ldots \to G_n}_{\phi_B}$
Exchange data	$\{G_i\}_{i=1}^n$	$\{F_i\}_{i=1}^n$
Compute shared secret	Compute $\phi_A \cdot \{G_i\}$	Compute $\phi_B \cdot \{F_i\}$

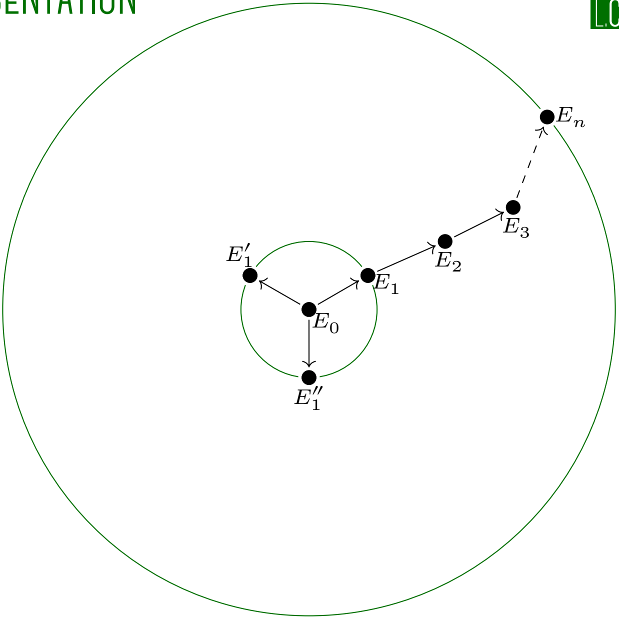
A FIRST NAIVE PROTOCOL

PUBLIC DATA: A chain of ℓ-isogenies $E_0 \to E_1 \to ... \to E_n$

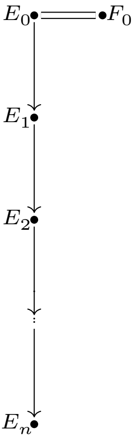
	ALICE	**BOB**
Choose a primitive $\mathcal{O}_K$-orientation of E_0		
Push it forward to depth n	$\underbrace{E_0 = F_0 \to F_1 \to ... \to F_n}_{\phi_A}$	$\underbrace{E_0 = G_0 \to G_1 \to ... \to G_n}_{\phi_B}$
Exchange data	$\{G_i\}_{i=1}^n$	$\{F_i\}_{i=1}^n$
Compute shared secret	Compute $\phi_A \cdot \{G_i\}$	Compute $\phi_B \cdot \{F_i\}$

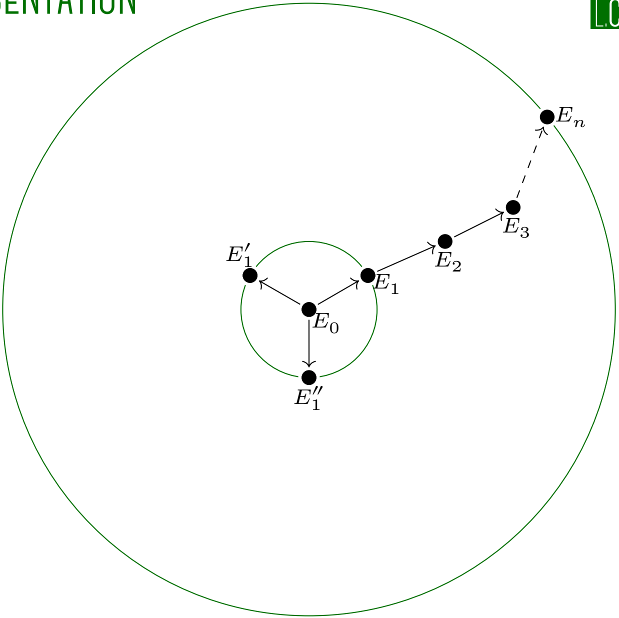
In the end, Alice and Bob will share a new chain $E_0 \to H_1 \to ... \to H_n$

GRAPHIC REPRESENTATION

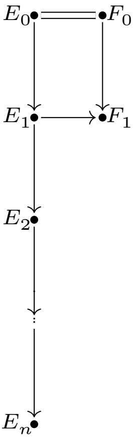


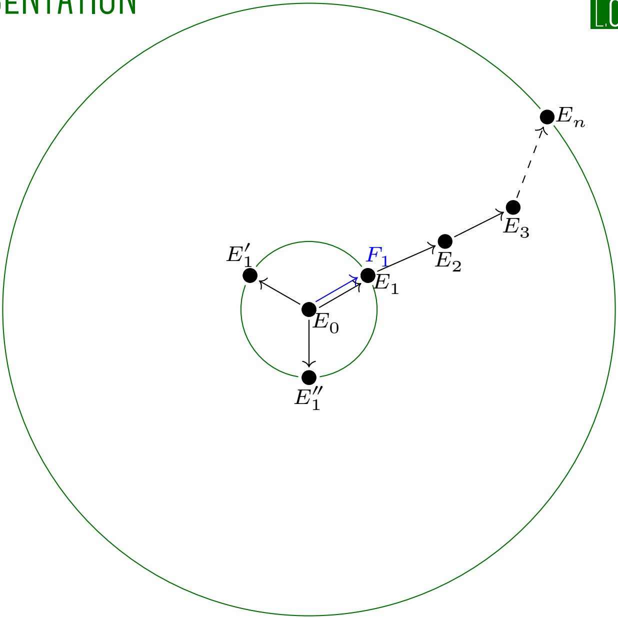
GRAPHIC REPRESENTATION



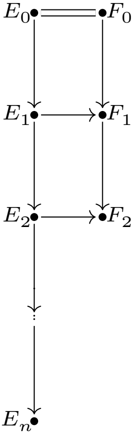


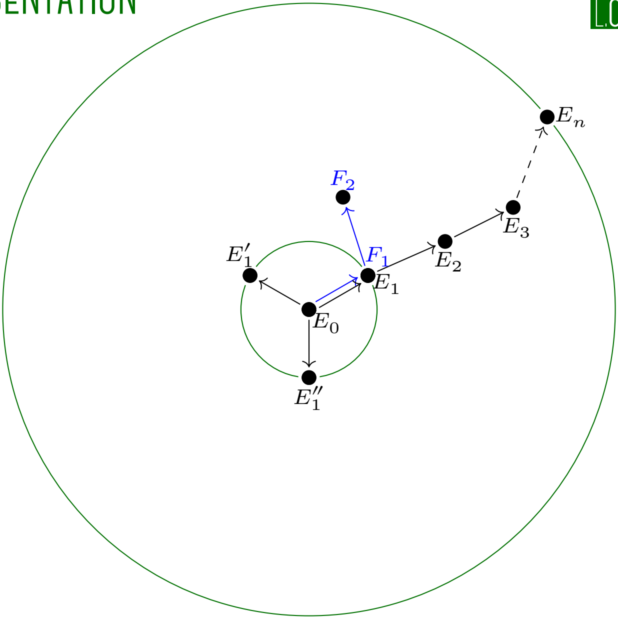
GRAPHIC REPRESENTATION



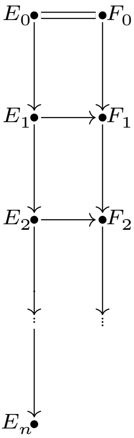


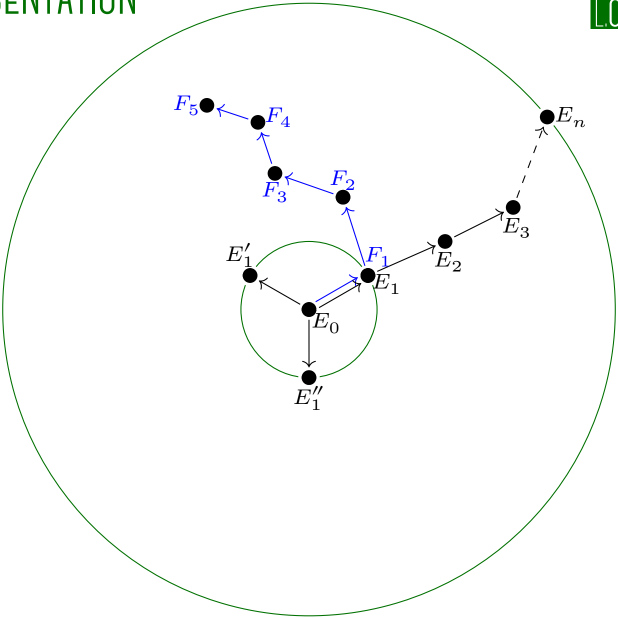
GRAPHIC REPRESENTATION





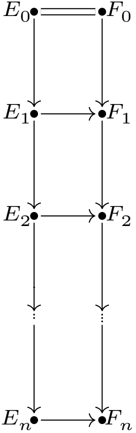
GRAPHIC REPRESENTATION

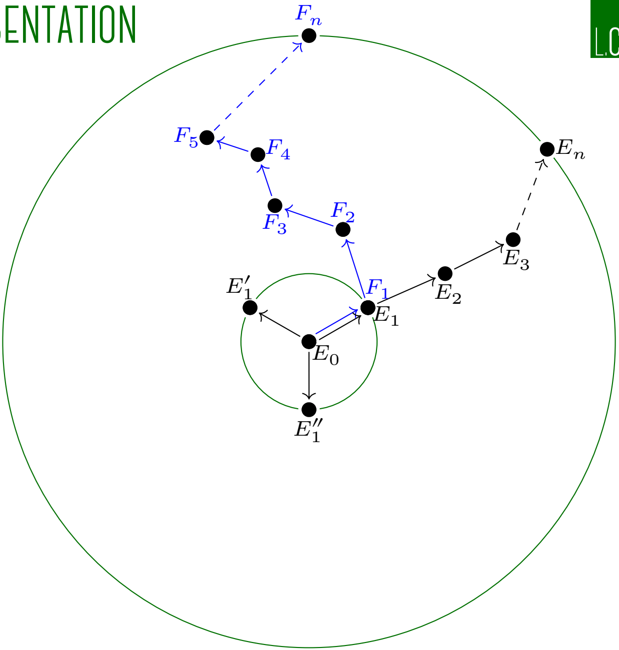




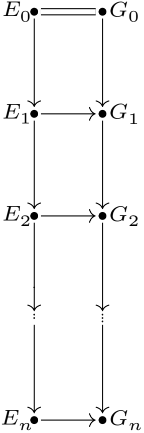
GRAPHIC REPRESENTATION

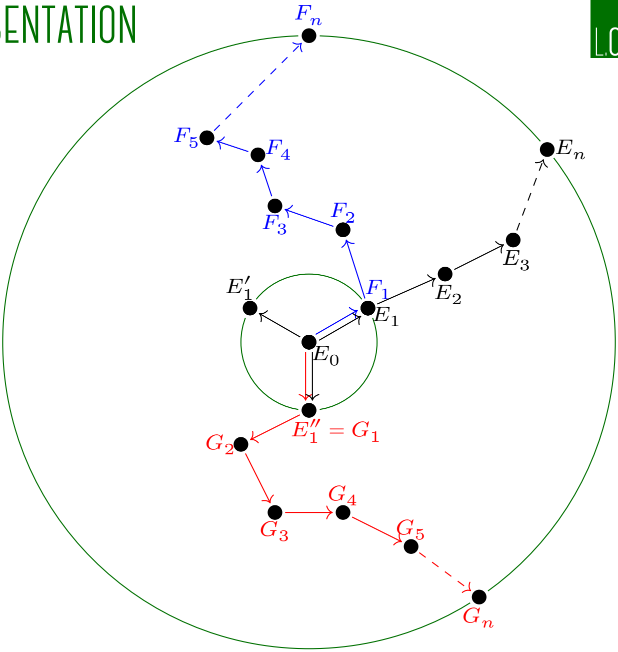
L.COLÒ I2M



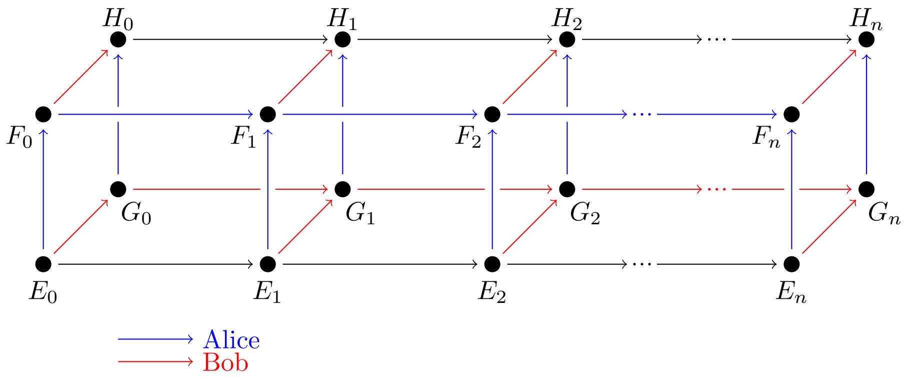


GRAPHIC REPRESENTATION





GRAPHIC REPRESENTATION



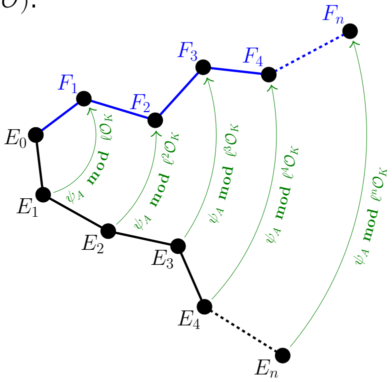
A FIRST NAIVE PROTOCOL - WEAKNESS

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

From the short exact sequence of class groups:

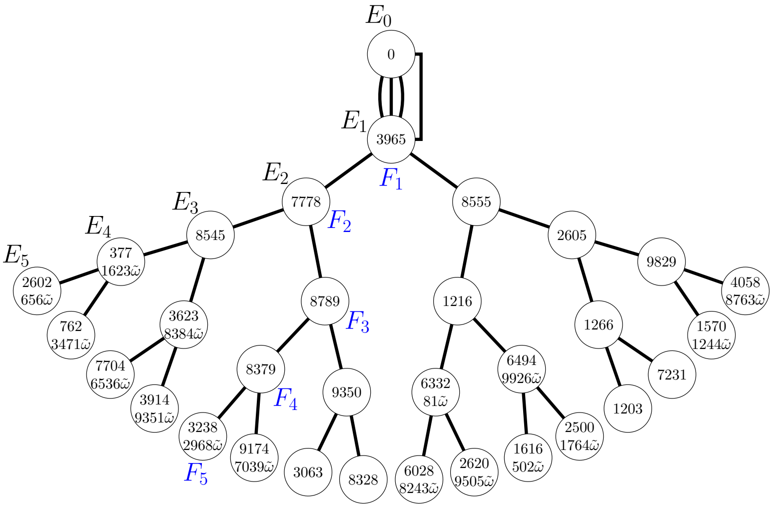
$$1 \to \frac{(\mathcal{O}_K/\ell^n\mathcal{O}_K)^\times}{\mathcal{O}_K^\times(\mathbb{Z}/\ell^n\mathbb{Z})^\times} \to \mathcal{C}\ell(\mathcal{O}) \to \mathcal{C}\ell(\mathcal{O}_K) \to 1$$

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



AN EXAMPLE: COMPUTE SUCCESSIVE APPROXIMATIONS

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



AN EXAMPLE: COMPUTE SUCCESSIVE APPROXIMATIONS

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

Input: The j-invariants of two elliptic curves E and E' over $\mathbb{F}_{p^2}$ known to be q-isogenous.
Output: The ideal $[\mathfrak{a}] \in \{[\mathfrak{q}], [\overline{\mathfrak{q}}]\}$ such that $[\mathfrak{a}] * j(E) = j(E')$.

---

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

    Return $\mathfrak{q}$.

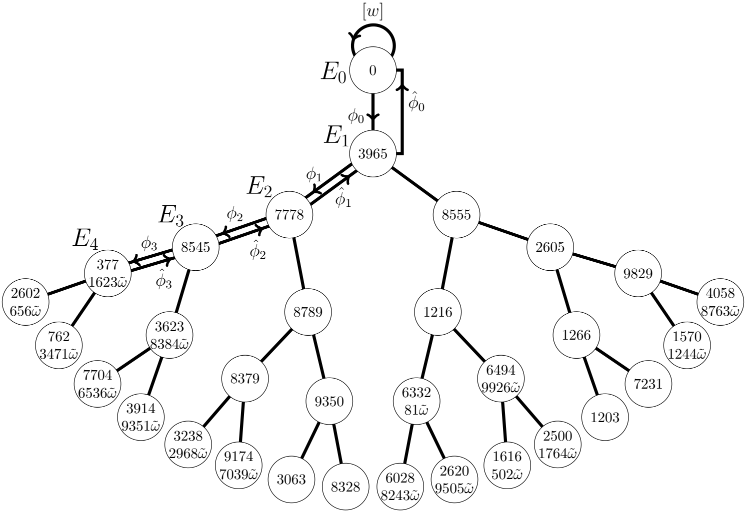
    Else

    Return $\overline{\mathfrak{q}}$.

AN EXAMPLE: COMPUTE SUCCESSIVE APPROXIMATIONS

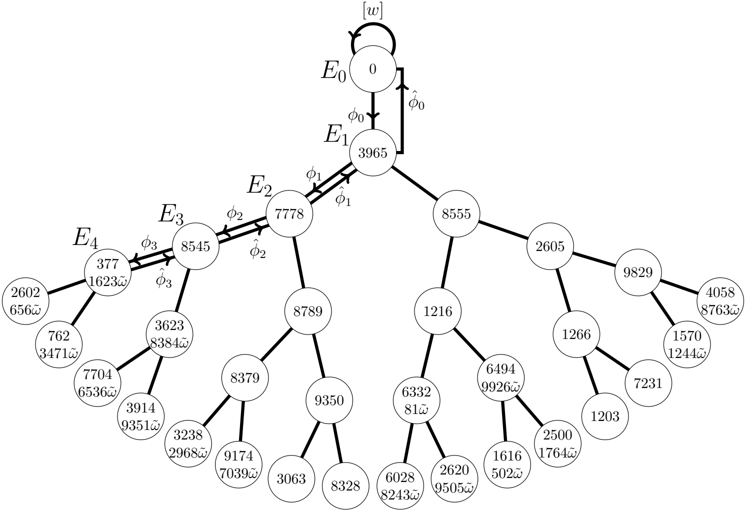
The action of $\ell^i \omega$ on E_i will be given by the composition

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



AN EXAMPLE: COMPUTE SUCCESSIVE APPROXIMATIONS

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



Computing successive approximations

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

1. $\beta \equiv 1$ mod ℓ^m so that $\beta_* E_i = F_i = E_i$ for all $i \leq m$;

2. $\beta_* E_{m+1} = F_{m+1}$;

3. β is smooth with small exponents (n order to determine the action of β modulo ℓ^{m+1} effectively).

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

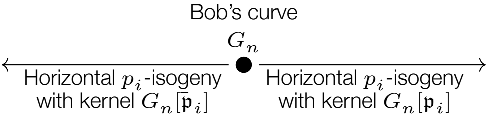
1'. $\beta \equiv \alpha$ mod ℓ^k so that $\beta_* E_{k+1} = F_{k+1}$.

Towards a more secure OSIDH protocol

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

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

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



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

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

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

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

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

OSIDH PROTOCOL

L.COLÒ I2M

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

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

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

	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 $E_0 \to E_1 \to \ldots \to E_n$ 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
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 $H_n = E_n / E_n\left[\mathfrak{p}_1^{e_1+d_1} \cdot \ldots \cdot \mathfrak{p}_t^{e_t+d_t}\right]$

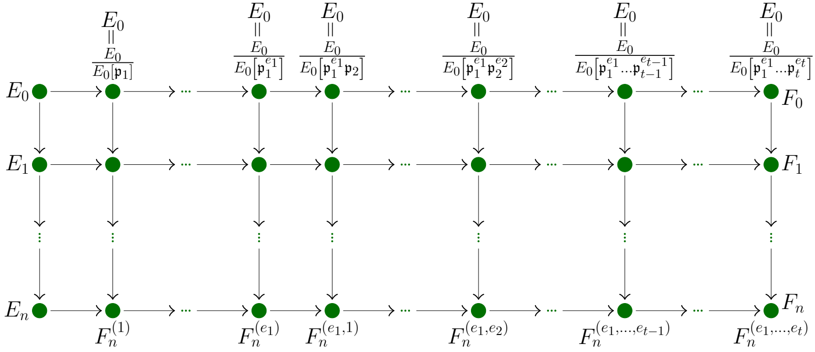
OSIDH PROTOCOL - GRAPHIC REPRESENTATION I

L.COLÒ I2M

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

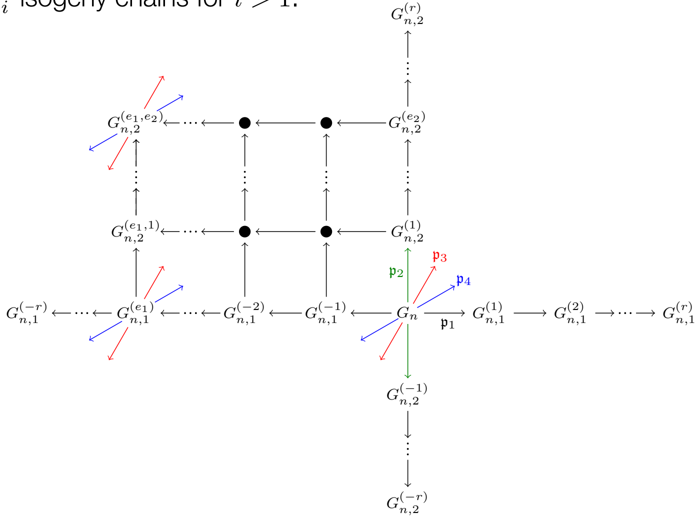
$$F_n = \frac{E_n}{E_n\left[\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_t^{e_t}\right]}$$

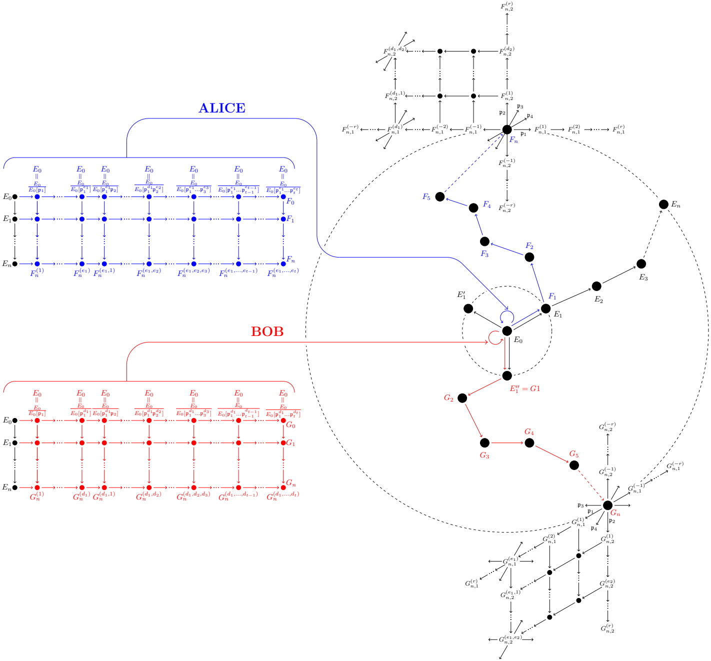
by means of constructing the following commutative diagram



OSIDH PROTOCOL - GRAPHIC REPRESENTATION II

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




ALICE
BOB
E_0
E_1
E_2
E_3
E_n
E'_1
$E''_1 = G1$
F_1
F_2
F_3
F_4
F_5
F_n
G_2
G_3
G_4
G_5
G_n

OSIDH PROTOCOL - AN EXAMPLE

$p = 10007$

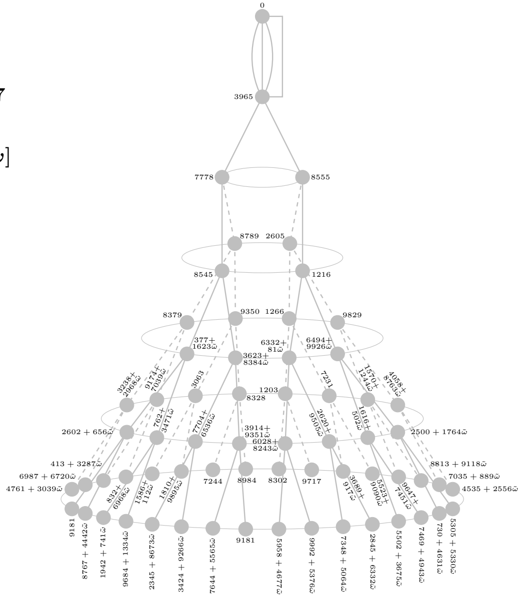
$\ell = 2$

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

$\ell_1 = 13$

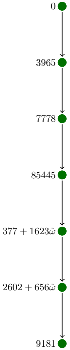
$\ell_2 = 31$

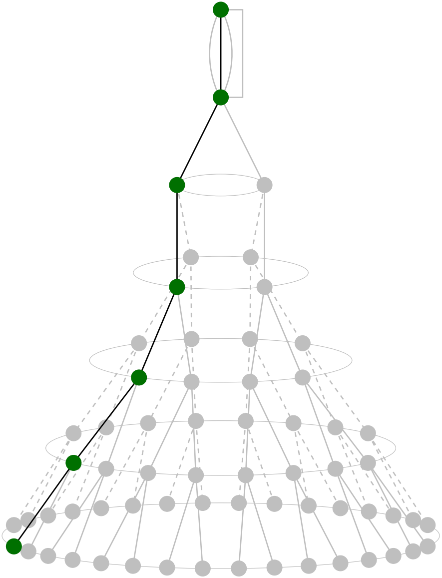
$\ell_3 = 43$



OSIDH PROTOCOL - AN EXAMPLE

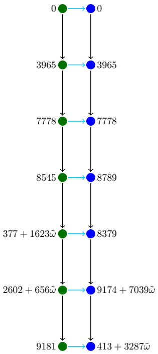
Alice secret key: $\mathfrak{l}_1^5\mathfrak{l}_2^3\mathfrak{l}_3^2$

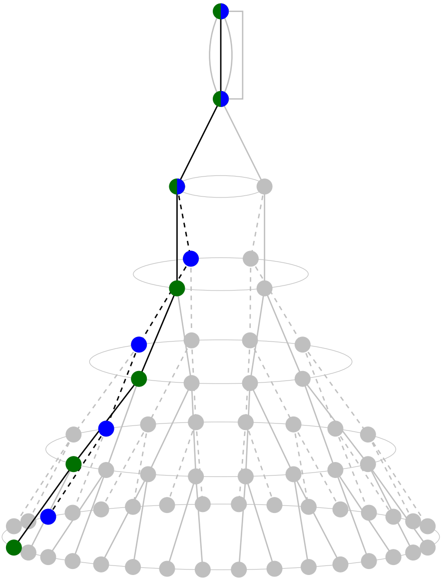




OSIDH PROTOCOL - AN EXAMPLE

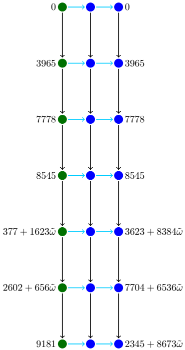
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$

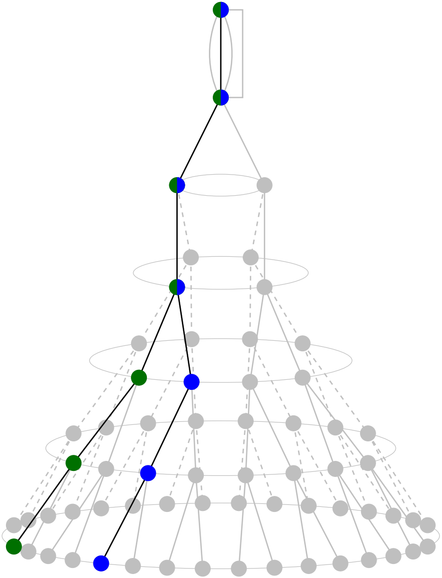




OSIDH PROTOCOL - AN EXAMPLE

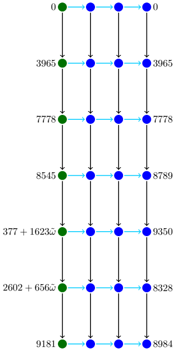
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$

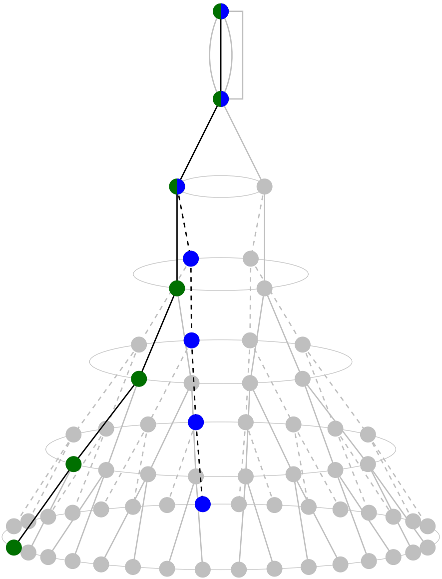




OSIDH PROTOCOL - AN EXAMPLE

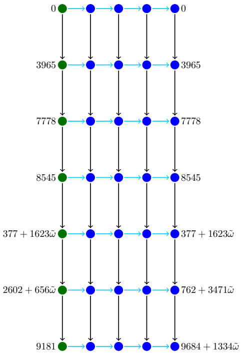
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$

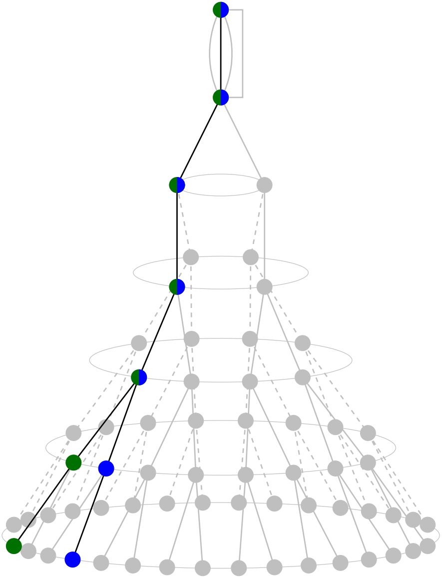




OSIDH PROTOCOL - AN EXAMPLE

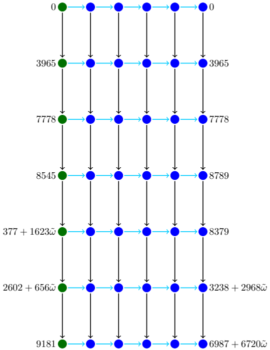
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$

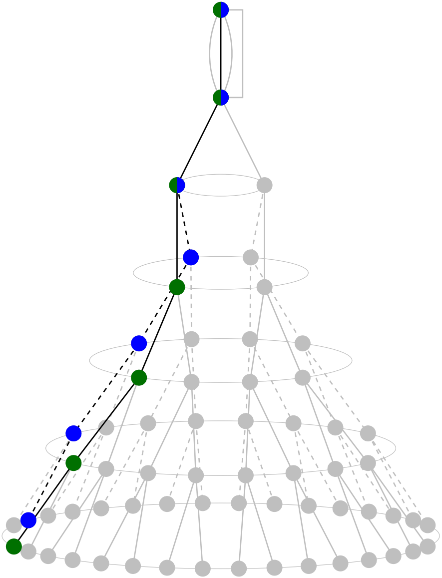




OSIDH PROTOCOL - AN EXAMPLE

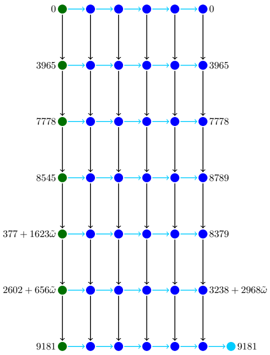
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$

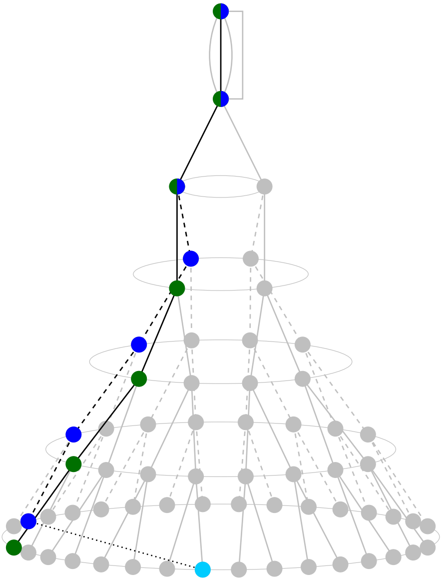




OSIDH PROTOCOL - AN EXAMPLE

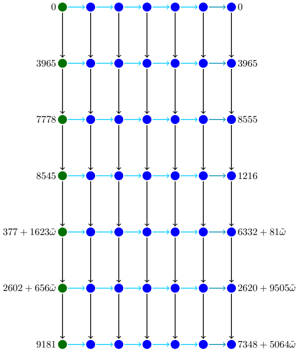
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$

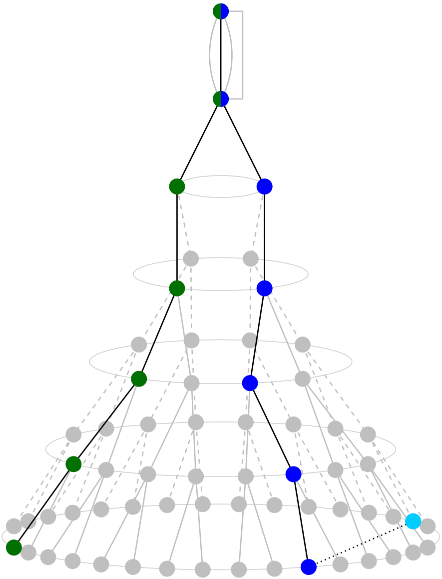




OSIDH PROTOCOL - AN EXAMPLE

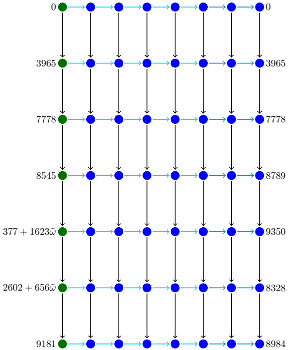
Alice secret key: $\mathfrak{l}_1^5\mathfrak{l}_2^3\mathfrak{l}_3^2$

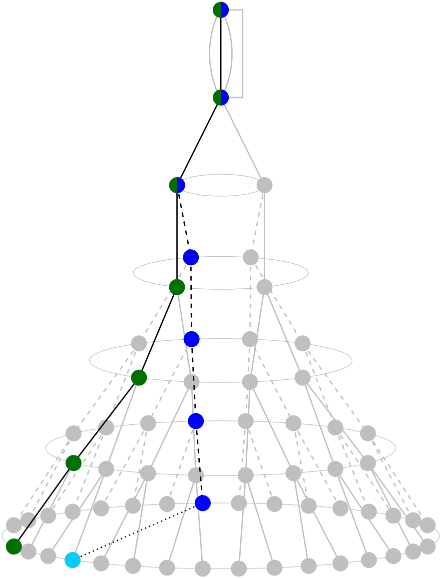




OSIDH PROTOCOL - AN EXAMPLE

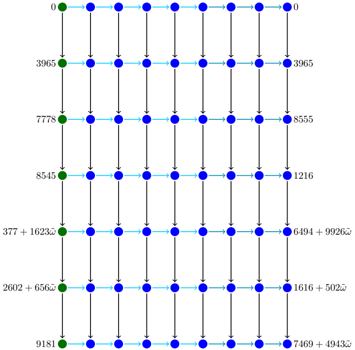
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$

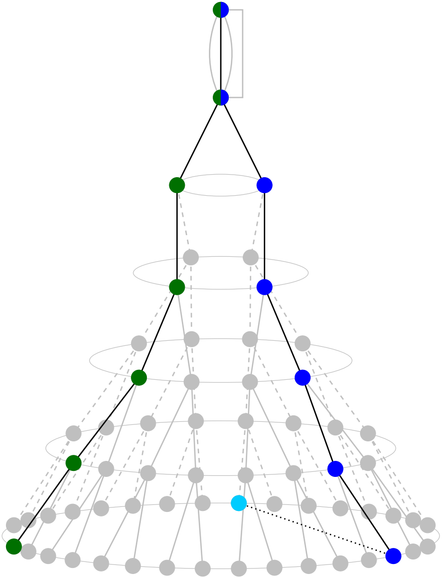




OSIDH PROTOCOL - AN EXAMPLE

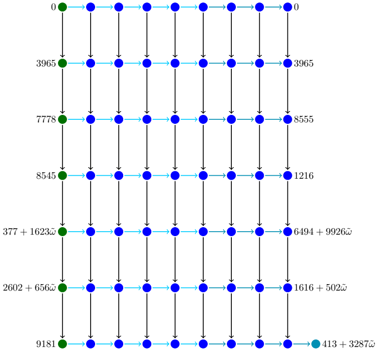
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$

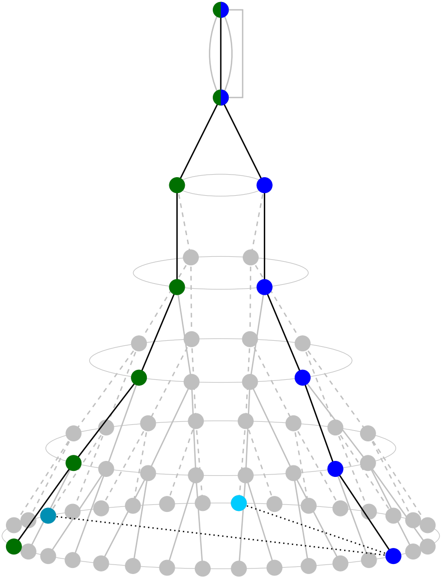




OSIDH PROTOCOL - AN EXAMPLE

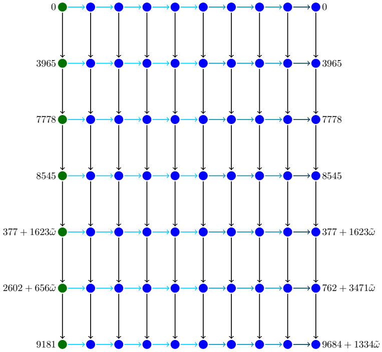
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$

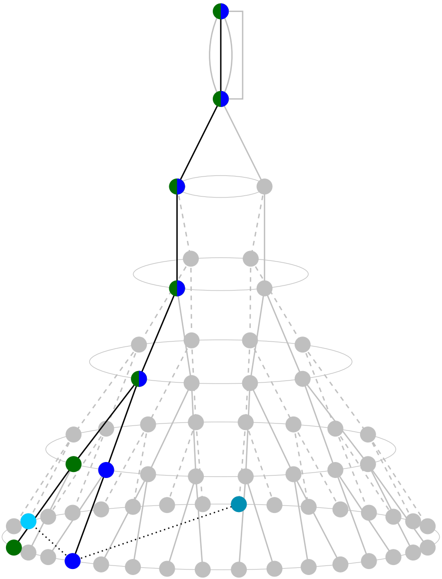




OSIDH PROTOCOL - AN EXAMPLE

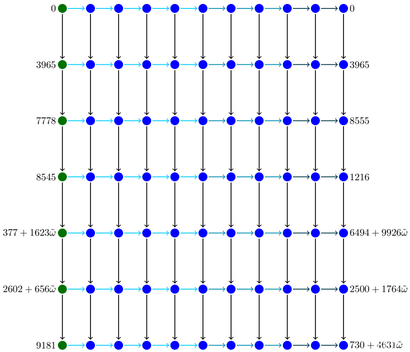
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$

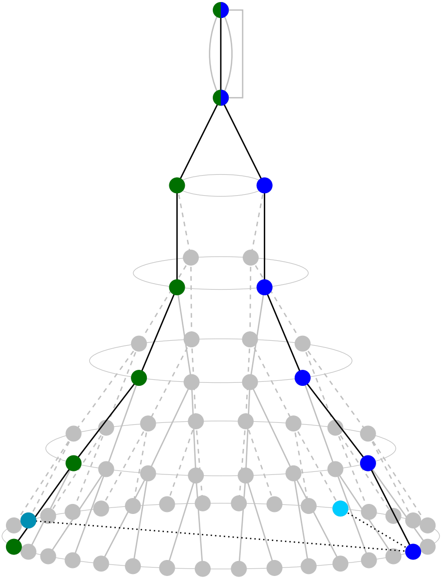




OSIDH PROTOCOL - AN EXAMPLE

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

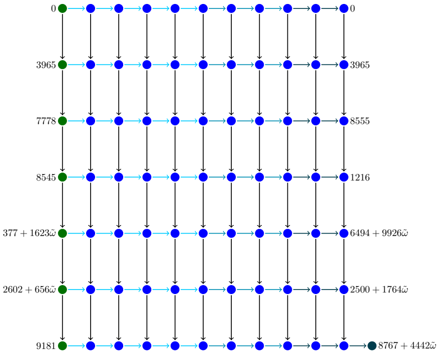


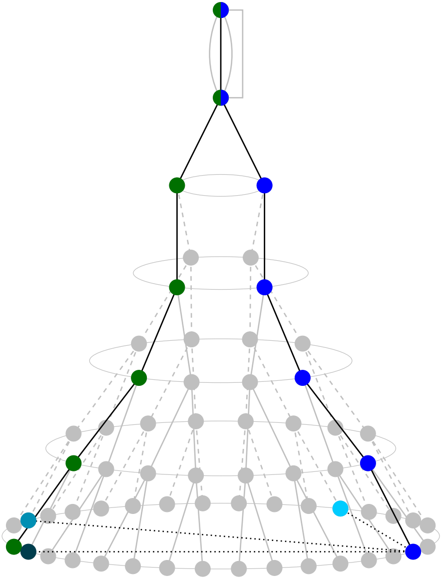


OSIDH PROTOCOL - AN EXAMPLE

L.COLÒ I2M

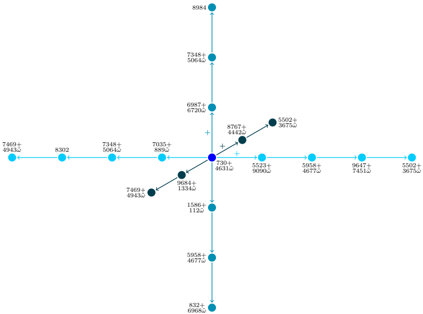
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$

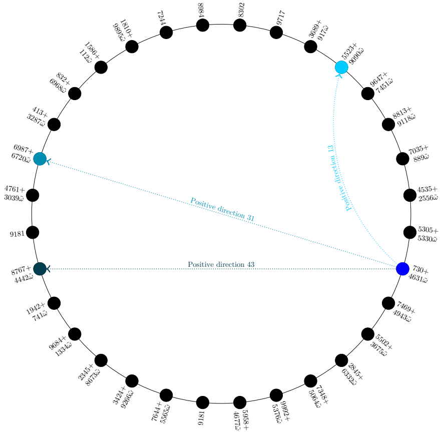




OSIDH PROTOCOL - AN EXAMPLE

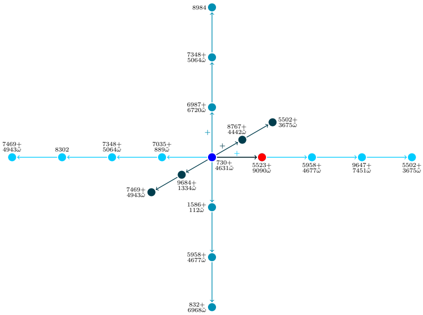
Bob secret key: $\mathfrak{l}_1^3 \mathfrak{l}_2 \mathfrak{l}_3^2$

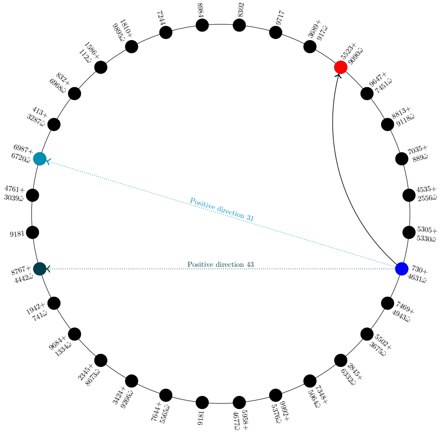




OSIDH PROTOCOL - AN EXAMPLE

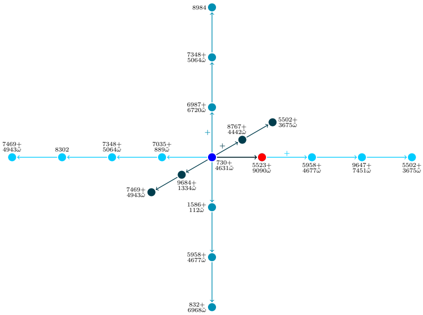
Bob secret key: $\mathfrak{l}_1^3\mathfrak{l}_2\mathfrak{l}_3^2$

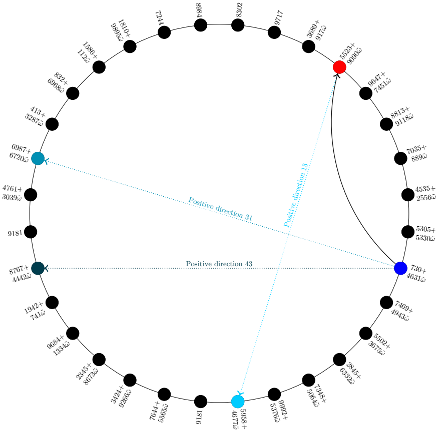




OSIDH PROTOCOL - AN EXAMPLE

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

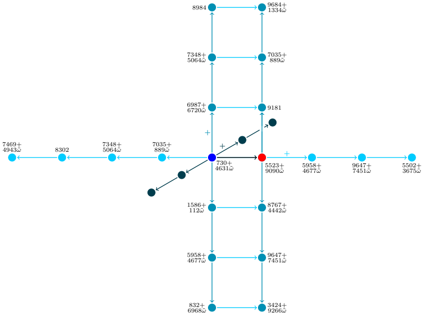


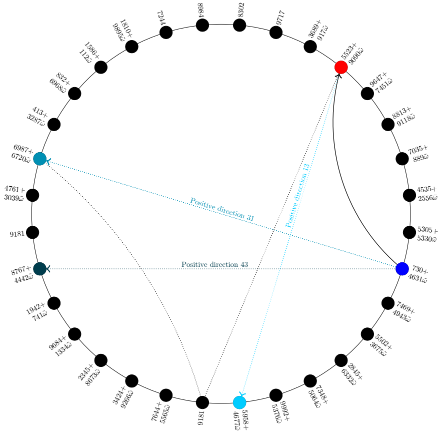


OSIDH PROTOCOL - AN EXAMPLE

L.COLÒ I2M

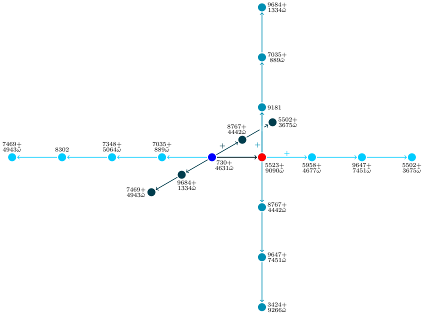
Bob secret key: $\mathfrak{l}_1^3 \mathfrak{l}_2 \mathfrak{l}_3^2$

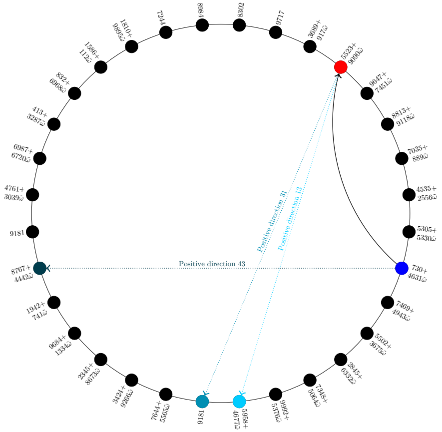




L.COLÒ I2M

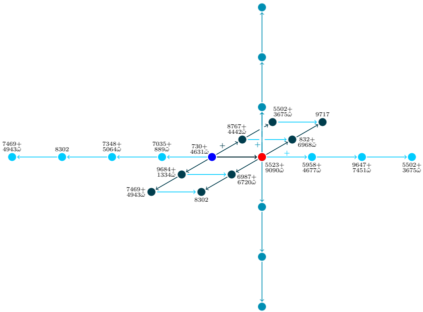
Bob secret key: $\mathfrak{l}_1^3\mathfrak{l}_2\mathfrak{l}_3^2$

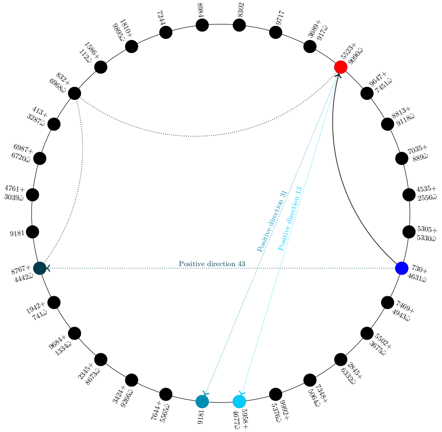




OSIDH PROTOCOL - AN EXAMPLE

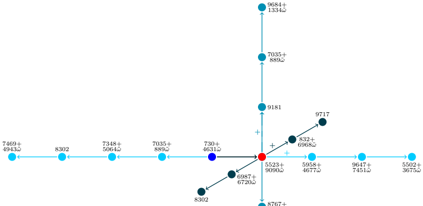
Bob secret key: $\mathfrak{l}_1^3\mathfrak{l}_2\mathfrak{l}_3^2$

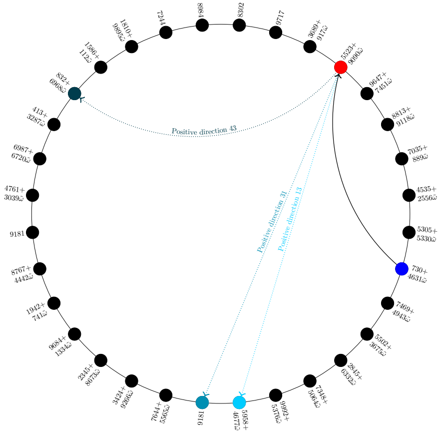




OSIDH PROTOCOL - AN EXAMPLE

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

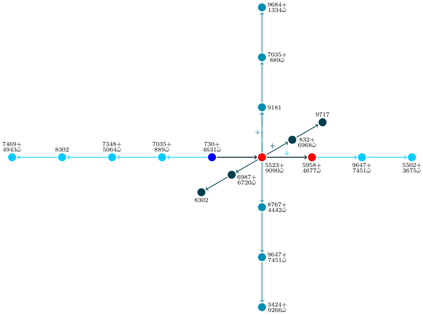


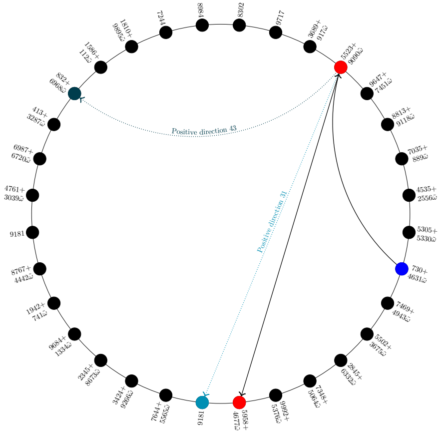


OSIDH PROTOCOL - AN EXAMPLE

L.COLÒ I2M

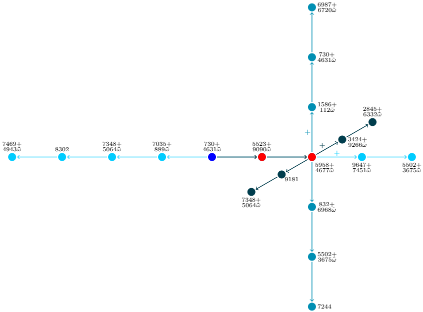
Bob secret key: $\mathfrak{l}_1^3 \mathfrak{l}_2 \mathfrak{l}_3^2$

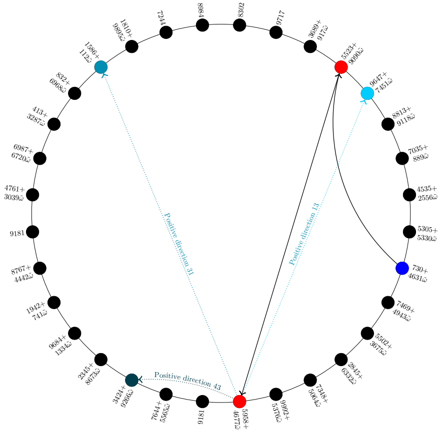




OSIDH PROTOCOL - AN EXAMPLE

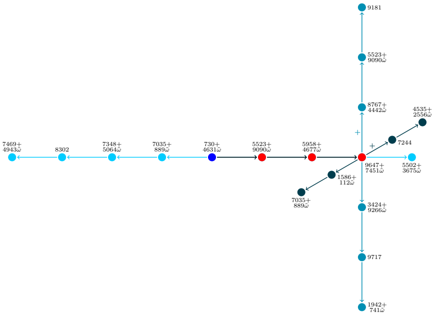
Bob secret key: $\mathfrak{l}_1^3\mathfrak{l}_2\mathfrak{l}_3^2$

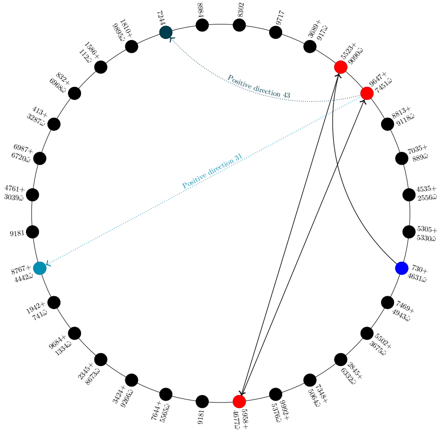




OSIDH PROTOCOL - AN EXAMPLE

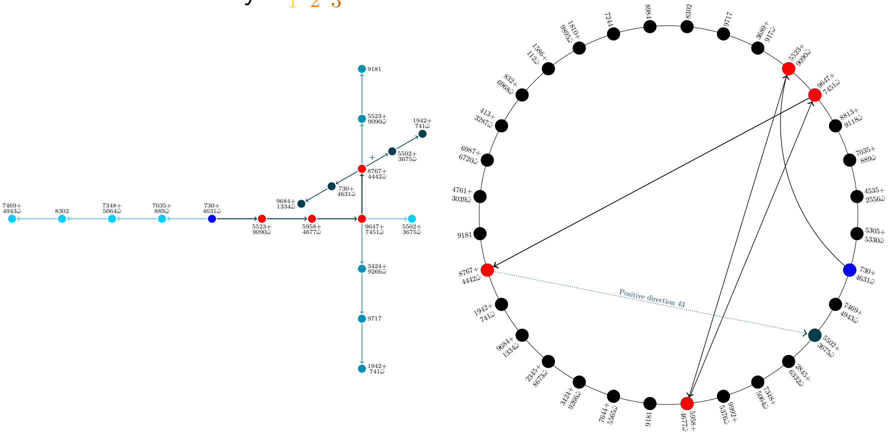
Bob secret key: $\mathfrak{l}_1^3\mathfrak{l}_2\mathfrak{l}_3^2$





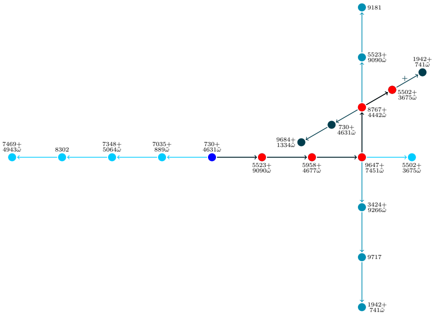
OSIDH PROTOCOL - AN EXAMPLE

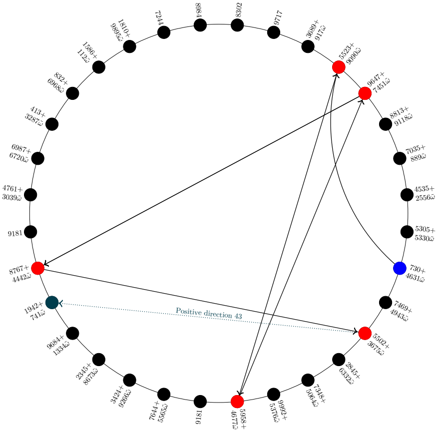
Bob secret key: $\mathfrak{l}_1^3\mathfrak{l}_2\mathfrak{l}_3^2$



OSIDH PROTOCOL - AN EXAMPLE

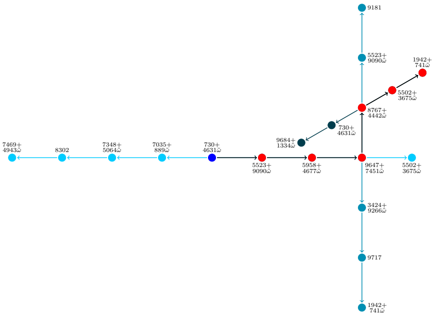
Bob secret key: $\mathfrak{l}_1^3 \mathfrak{l}_2 \mathfrak{l}_3^2$

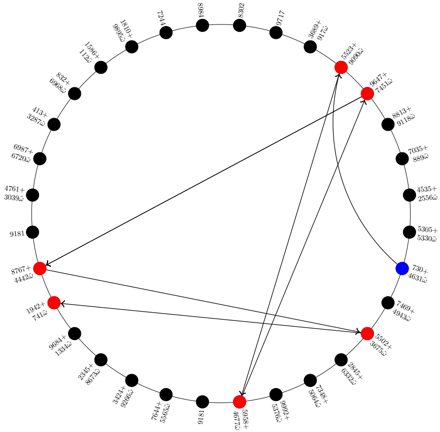




OSIDH PROTOCOL - AN EXAMPLE

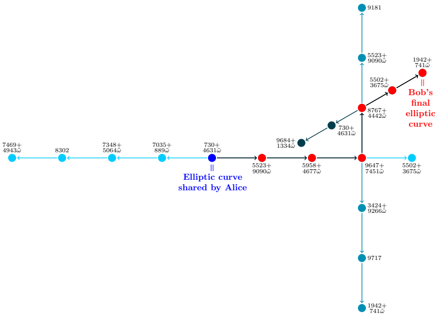
Bob secret key: $\mathfrak{l}_1^3 \mathfrak{l}_2 \mathfrak{l}_3^2$

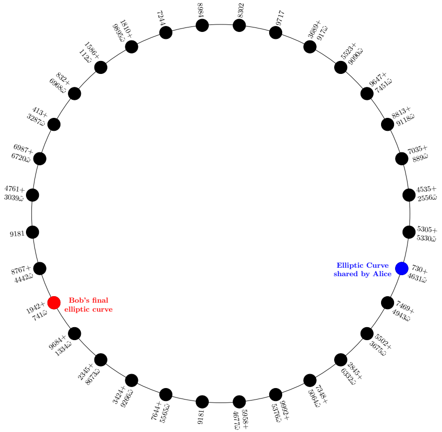




OSIDH PROTOCOL - AN EXAMPLE

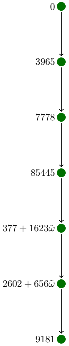
Bob secret key: $\mathfrak{l}_1^3 \mathfrak{l}_2 \mathfrak{l}_3^2$

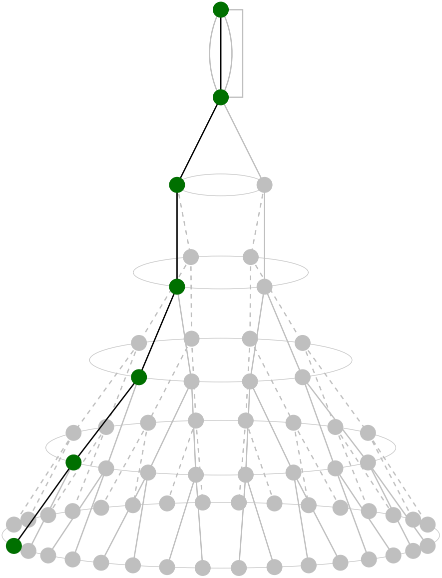




OSIDH PROTOCOL - AN EXAMPLE

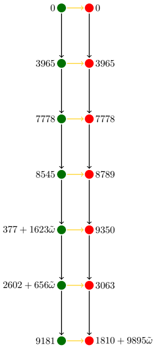
Bob secret key: $\mathfrak{l}_1^3 \mathfrak{l}_2 \mathfrak{l}_3^2$

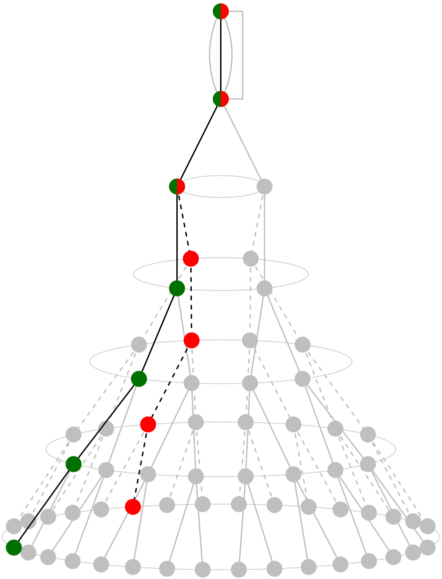




OSIDH PROTOCOL - AN EXAMPLE

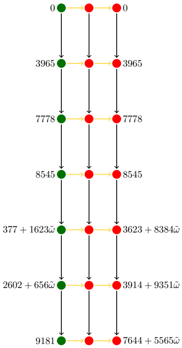
Bob secret key: $\mathfrak{l}_1^3 \mathfrak{l}_2 \mathfrak{l}_3^2$

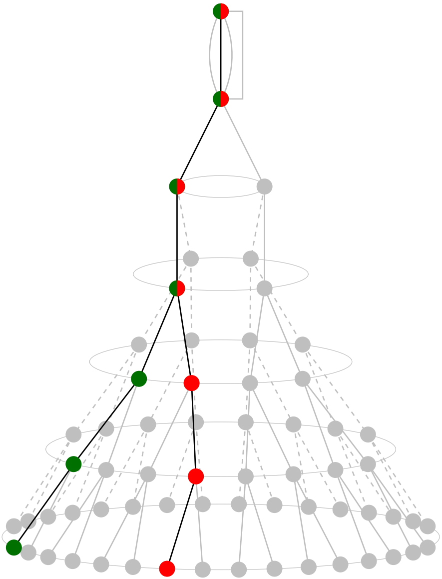




OSIDH PROTOCOL - AN EXAMPLE

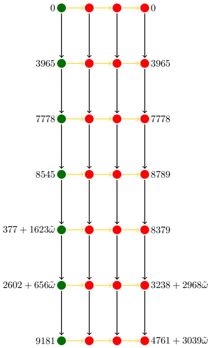
Bob secret key: $\mathfrak{l}_1^3 \mathfrak{l}_2 \mathfrak{l}_3^2$

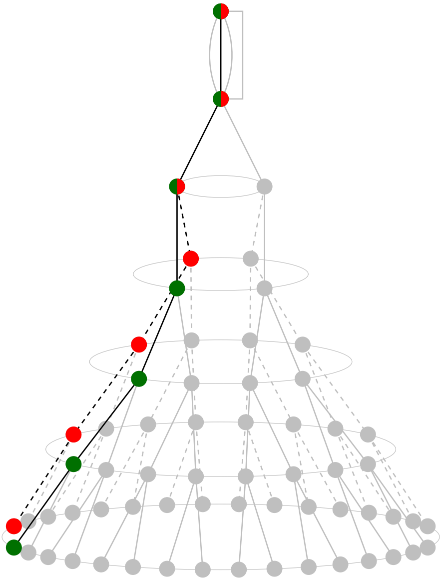




OSIDH PROTOCOL - AN EXAMPLE

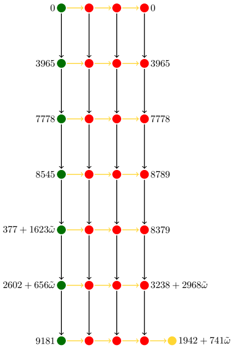
Bob secret key: $\mathfrak{l}_1^3 \mathfrak{l}_2 \mathfrak{l}_3^2$

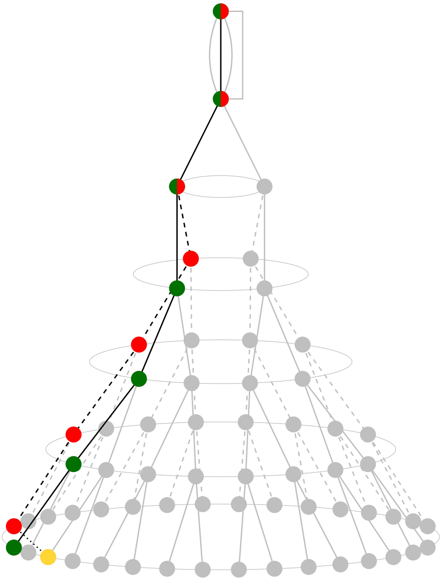




OSIDH PROTOCOL - AN EXAMPLE

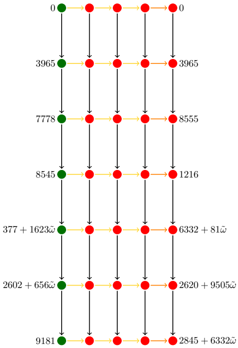
Bob secret key: $\mathfrak{l}_1^3\mathfrak{l}_2\mathfrak{l}_3^2$

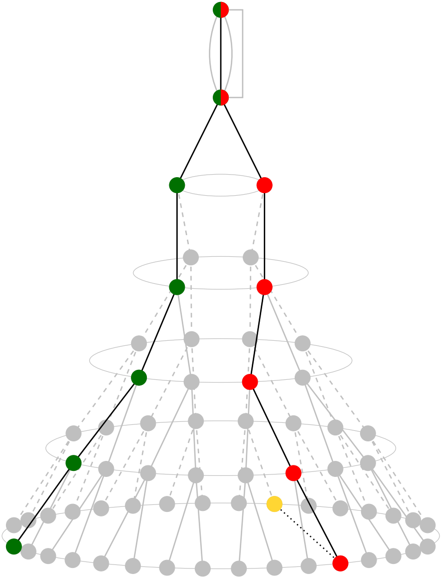




OSIDH PROTOCOL - AN EXAMPLE

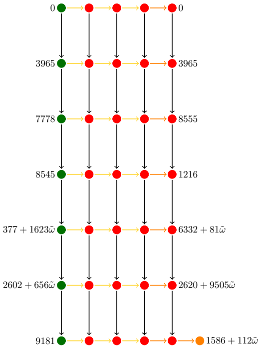
Bob secret key: $\mathfrak{l}_1^3\mathfrak{l}_2\mathfrak{l}_3^2$

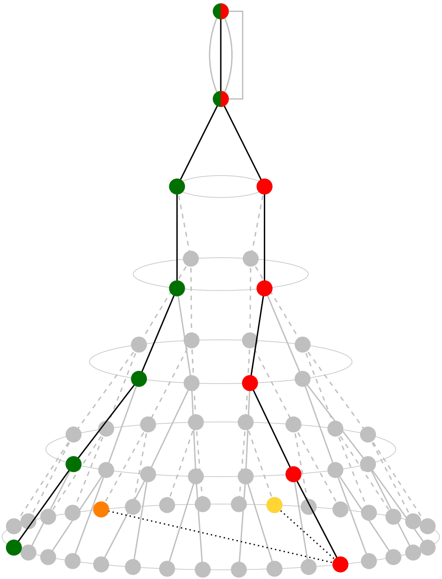




OSIDH PROTOCOL - AN EXAMPLE

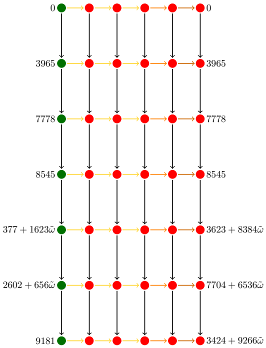
Bob secret key: $\mathfrak{l}_1^3 \mathfrak{l}_2 \mathfrak{l}_3^2$

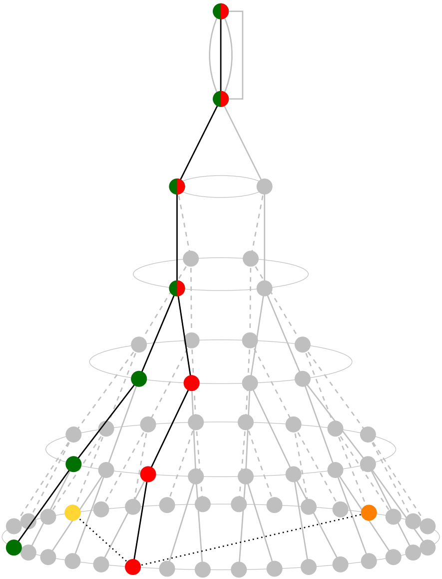




OSIDH PROTOCOL - AN EXAMPLE

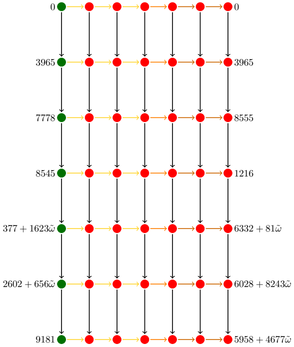
Bob secret key: $\mathfrak{l}_1^3 \mathfrak{l}_2 \mathfrak{l}_3^2$

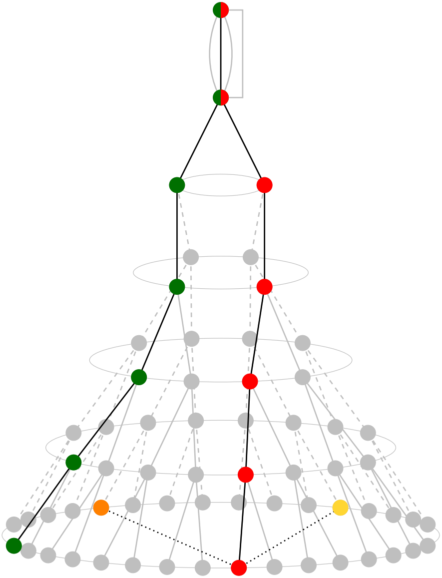




OSIDH PROTOCOL - AN EXAMPLE

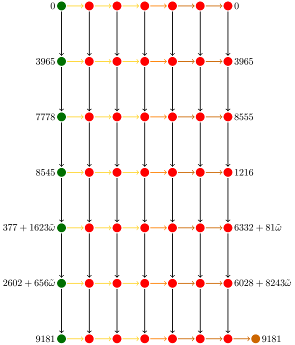
Bob secret key: $\mathfrak{l}_1^3\mathfrak{l}_2\mathfrak{l}_3^2$

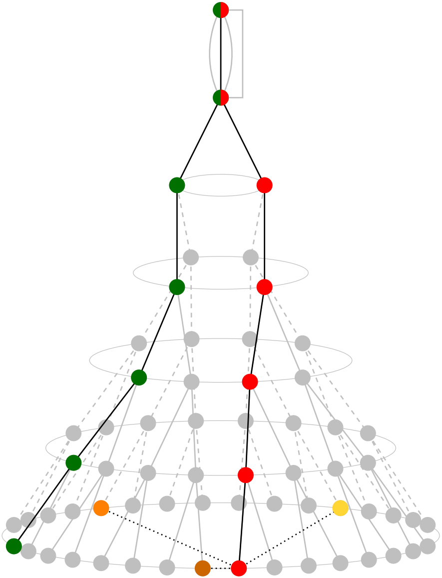




OSIDH PROTOCOL - AN EXAMPLE

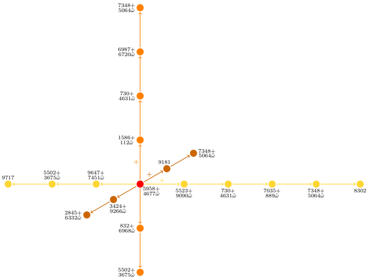
Bob secret key: $\mathfrak{l}_1^3 \mathfrak{l}_2 \mathfrak{l}_3^2$

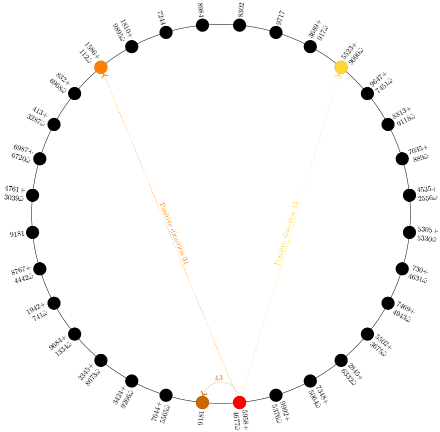




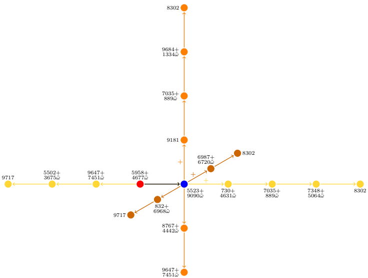
L.COLÒ I2M

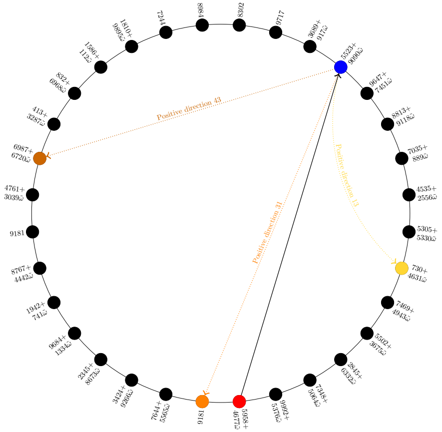
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$





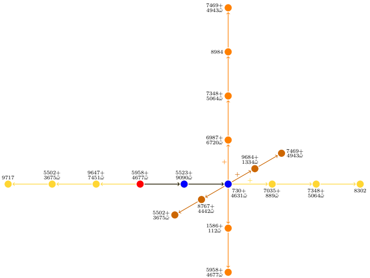
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$

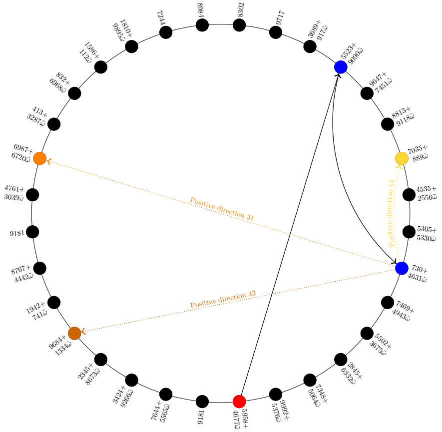




OSIDH PROTOCOL - AN EXAMPLE

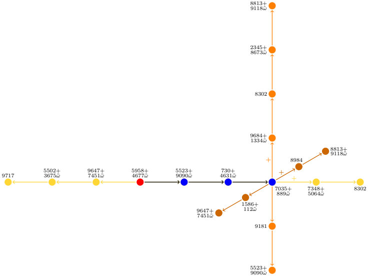
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$

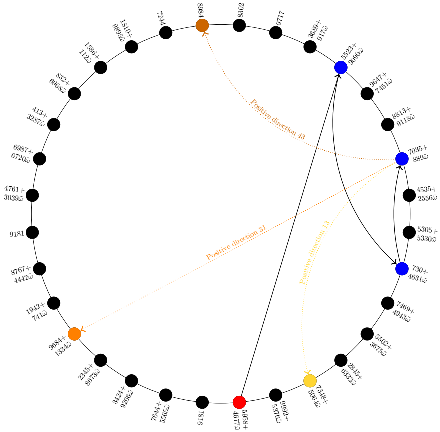




OSIDH PROTOCOL - AN EXAMPLE

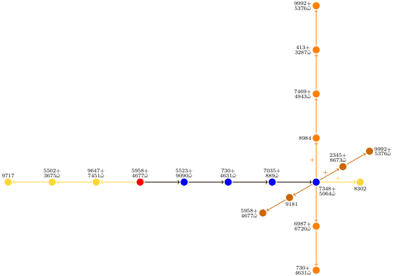
Alice secret key: $\overleftarrow{\mathfrak{l}}_1^5 \overleftarrow{\mathfrak{l}}_2^3 \overleftarrow{\mathfrak{l}}_3^2$

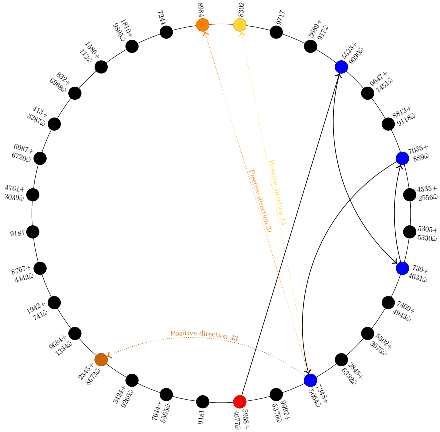




OSIDH PROTOCOL - AN EXAMPLE

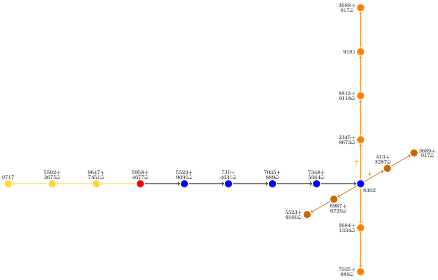
Alice secret key: $\mathfrak{l}_1^5\,\mathfrak{l}_2^3\,\mathfrak{l}_3^2$

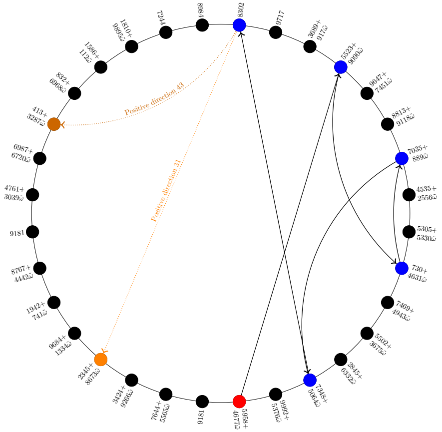




OSIDH PROTOCOL - AN EXAMPLE

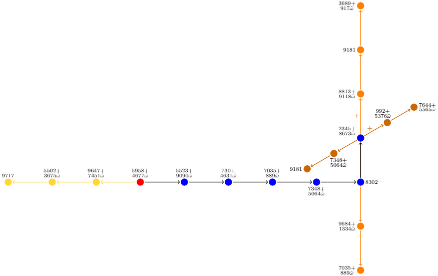
Alice secret key: $\mathfrak{l}_1^5\mathfrak{l}_2^3\mathfrak{l}_3^2$

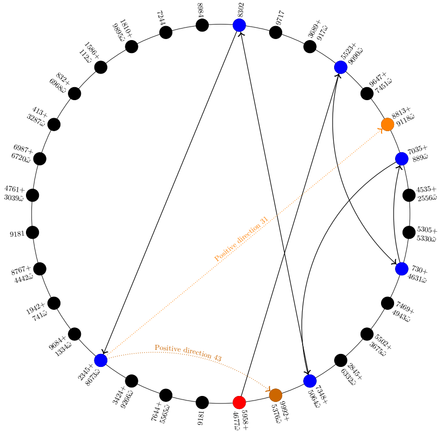




OSIDH PROTOCOL - AN EXAMPLE

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

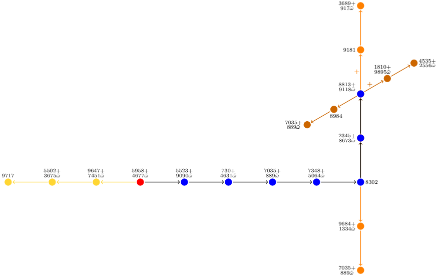


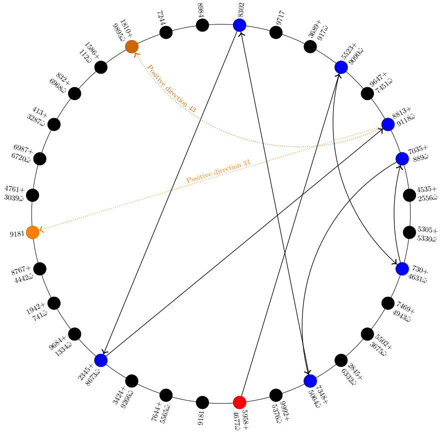


OSIDH PROTOCOL - AN EXAMPLE

L.COLÒ I2M

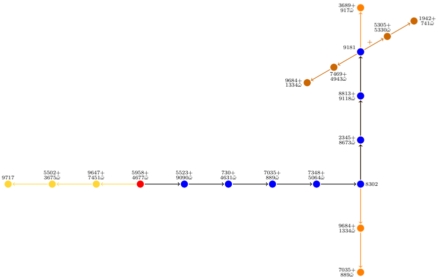
Alice secret key: $\mathfrak{l}_1^5\,\mathfrak{l}_2^3\,\mathfrak{l}_3^2$

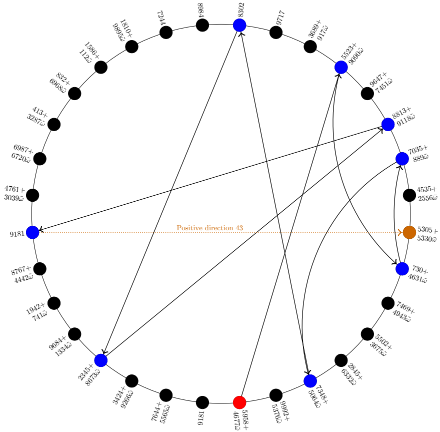




OSIDH PROTOCOL - AN EXAMPLE

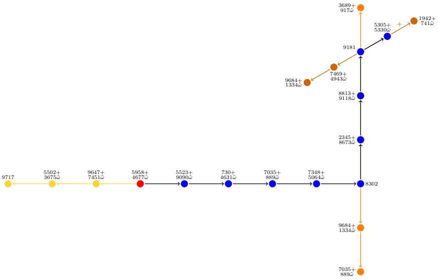
Alice secret key: $\mathfrak{l}_1^5\,\mathfrak{l}_2^3\,\mathfrak{l}_3^2$

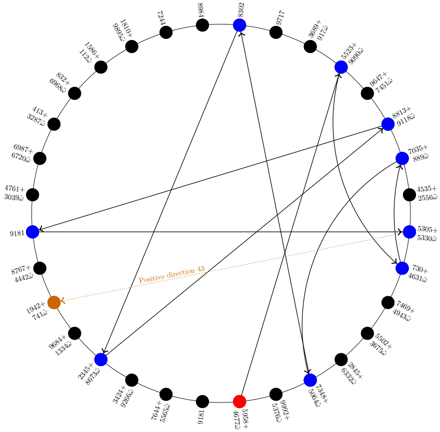




OSIDH PROTOCOL - AN EXAMPLE

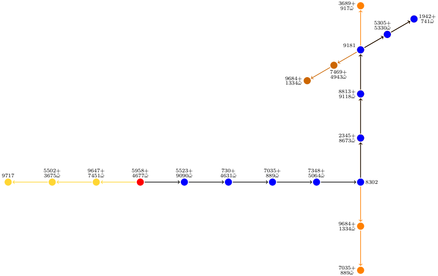
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$

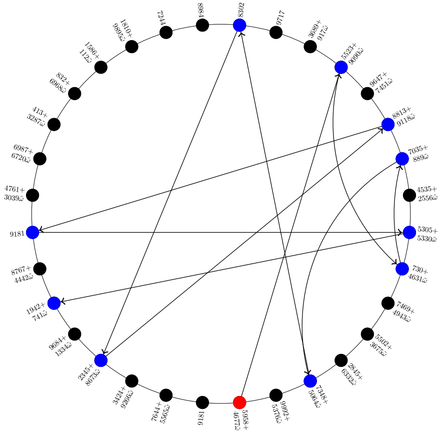




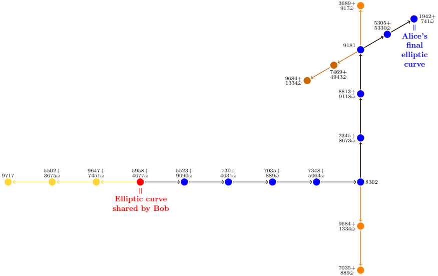
OSIDH PROTOCOL - AN EXAMPLE

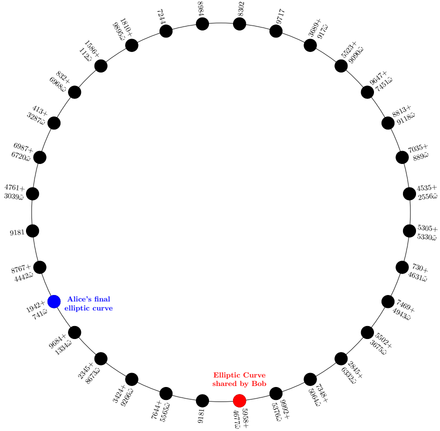
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$





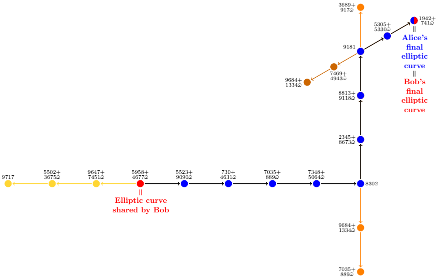
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$

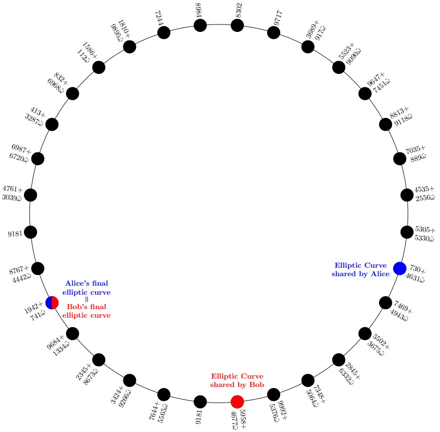




OSIDH PROTOCOL - AN EXAMPLE

L.COLÒ I2M





Endomorphism ring problem

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

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

Endomorphism ring transfer problem

Given an isogeny chain

$$E_0 \longrightarrow E_1 \longrightarrow ... \longrightarrow E_n$$

and End(E_0), determine End(E_n).

HARD PROBLEMS

Endomorphism Generators Problem

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

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

Suppose $S = \{(\mathfrak{q}, n)\} = \{(\mathfrak{q}_1, n_1), \dots, (\mathfrak{q}_t, n_t)\}$ where $\mathfrak{q}_1, \dots, \mathfrak{q}_t$ are pairwise distinct primes such that

$$\begin{aligned}[0, \dots, n_1] \times \dots \times [0, \dots, n_t] &\longrightarrow \mathcal{C}\ell(\mathcal{O}) \\ (e_1, \dots, e_t) &\longrightarrow [\mathfrak{q}_1^{e_1} \cdot \dots \cdot \mathfrak{q}_t^{e_t}]\end{aligned}$$

is injective. Then, the problem should remain difficult.
We can reformulate this in a way that allows $(\bar{\mathfrak{q}}_i, n_i) \in S$:

$$\begin{aligned}[-n_1, \dots, n_1] \times \dots \times [-n_t, \dots, n_t] &\longrightarrow \mathcal{C}\ell(\mathcal{O}) \\ (e_1, \dots, e_t) &\longrightarrow [\mathfrak{q}_1^{e_1} \cdot \dots \cdot \mathfrak{q}_t^{e_t}]\end{aligned}$$

is injective. If $e_i < 0$, then $\mathfrak{q}_i^{e_i}$ corresponds to $(\bar{\mathfrak{q}}_i)^{|e_i|}$.

SECURITY PARAMETERS - CHAIN LENGTH I

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

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

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

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

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

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

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

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

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

SECURITY PARAMETERS - CHAIN LENGTH II

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

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

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

- Units

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

- Number of Supersingular curves

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

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

SECURITY PARAMETERS - DEGREE OF PRIVATE WALKS

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

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

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

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

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

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

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

$$\log_p\left(\text{deg}(\psi_A)\right) \geq \lambda$$

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

We choose exponents $(e_1, \ldots, e_r)$ in the space $I_1 \times \ldots \times I_r \subset \mathbb{Z}^r$ where $I_j = [-m_j, m_j]$, defining ψ_A with kernel $E[\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}]$.
As we said, we want the map

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

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

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

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

for fixed $m = m_j$ this yields

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

CONCLUSIONS

By imposing the data of an orientation by an imaginary quadratic ring $\mathcal{O}$, we obtain an augmented category of supersingular curves on which the class group $\mathcal{C}\ell(\mathcal{O})$ acts faithfully and transitively.

This idea is already implicit in the CSIDH protocol, in which supersingular curves over $\mathbb{F}_p$ are oriented by the Frobenius subring $\mathbb{Z}[\pi] \cong \mathbb{Z}[\sqrt{-p}]$.

In contrast we consider an elliptic curve E_0 oriented by a CM order $\mathcal{O}_K$ of class number one. To obtain a nontrivial group action, we consider ℓ-isogeny chains, on which the class group of an order $\mathcal{O}$ of large index ℓ^n in $\mathcal{O}_K$ acts.

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

We define a new oriented supersingular isogeny Diffie-Hellman (OSIDH) protocol, which has fewer restrictions on the proportion of supersingular curves covered and on the torsion group structure of the underlying curves.

Moreover, the group action can be carried out effectively solely on the sequences of modular points (such as j-invariants) on a modular curve, thereby avoiding expensive isogeny computations, and is further amenable to speedup by precomputations of endomorphisms on the base curve E_0.

Future directions:

- Security analysis and setting security parameters.
- Comparison with earlier protocols.
- Implementation and algorithmic optimization.
- Use of canonical liftings.

Future directions:

- Security analysis and setting security parameters.
- Comparison with earlier protocols.
- Implementation and algorithmic optimization.
- Use of canonical liftings.

MERCI POUR VOTRE ATTENTION