GARDANNE, 12 DECEMBER 2019

ORIENTING SUPERSINGULAR ISOGENY GRAPHS

LEONARDO COLÒ & DAVID KOHEL

Institut de Mathématiques de Marseille

Séminaire de Gardanne

ELLIPTIC CURVES

Definition

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

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

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

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

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

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

ISOMORPHISMS OF ELLIPTIC CURVES

Isomorphisms

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

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

Isomorphisms between elliptic curves are group isomorphisms.

Isomorphism classes are described by an invariant:

j-invariant

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

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

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

GROUP STRUCTURE

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

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

Torsion structure

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

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

If the $p > 0$, then

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

ISOGENIES

They are relationships between isomorphisms classes of elliptic curves.

Isogenies

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

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

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

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

ATTRIBUTES OF ISOGENIES

Let $\phi : E \to E'$ be an isogeny defined over a field k, char$(k) = p$. We define $k(E), k(E')$ to be the function fields of E and E'; by composing ϕ with elements of $k(E')$ we obtain a subfield $\phi^*(k(E'))$ of $k(E)$.

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

$$\phi \circ \hat{\phi} = [\mathtt{deg}\ \phi]_{E'} \qquad \hat{\phi} \circ \phi = [\mathtt{deg}\ \phi]_{E}$$

THEOREMS ON ISOGENIES

Theorem

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

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

Theorem (Tate)

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

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

ENDOMORPHISMS

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

Endomorphism ring

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

The endomorphism ring always contains a copy of $\mathbb{Z}$ in the form of the multiplication by m maps.
If k is a finite field we also have the Frobenius endomorphism.

Theorem (Hasse)

Let E be an elliptic curve defined over a finite field with q elements. Its Frobenius endomorphism satisfies a quadratic equation $\pi^2 - t\pi + q = 0$ for some $|t| \leq 2\sqrt{q}$, called the trace of π.

THEOREMS ON ENDOMORPHISMS

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

Theorem (Deuring)

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

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

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

Theorem (Serre-Tate)

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

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.

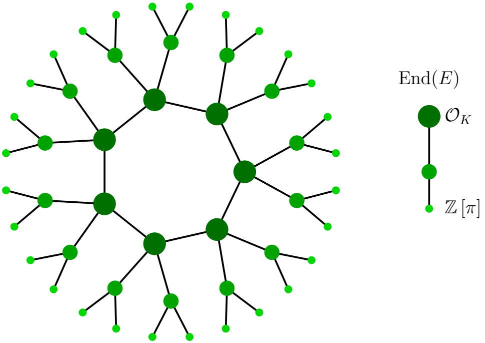
The ℓ-isogeny graph of E is $(\ell + 1)$-regular (as a directed multigraph). In characteristic 0, if End$(E) = \mathbb{Z}$, then this graph is a tree.

ORDINARY ISOGENY GRAPHS: VOLCANOES

Let $\mathrm{End}(E) = \mathcal{O} \subseteq K$. The class group $\mathrm{Cl}(\mathcal{O})$ 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.



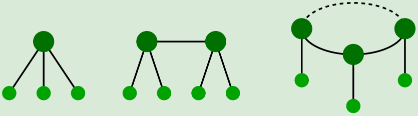
STRUCTURE OF VOLCANOES

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:



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

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

SUPERSINGULAR ISOGENY GRAPHS

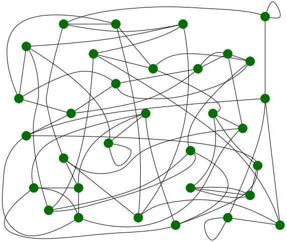
The supersingular isogeny graphs are remarkable because the vertex sets are finite : there are $(p+1)/12 + \epsilon_p$ curves. Moreover

- 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

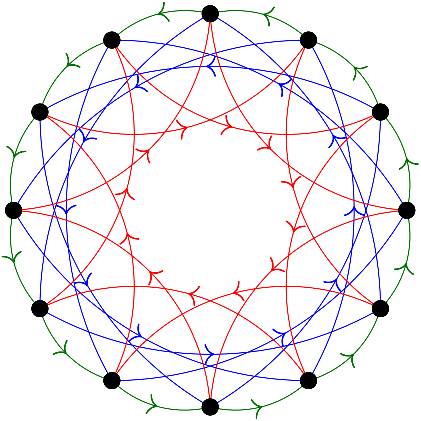
- cryptographic hash functions (Goren–Lauter),
- post-quantum SIDH key exchange protocol.



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 $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

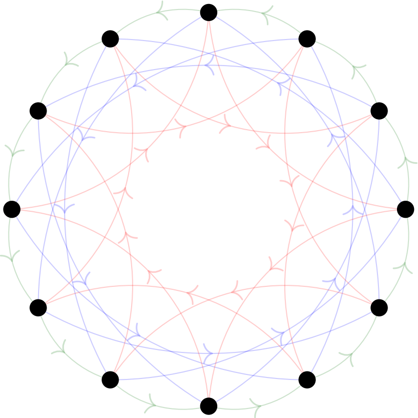
$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$



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 $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

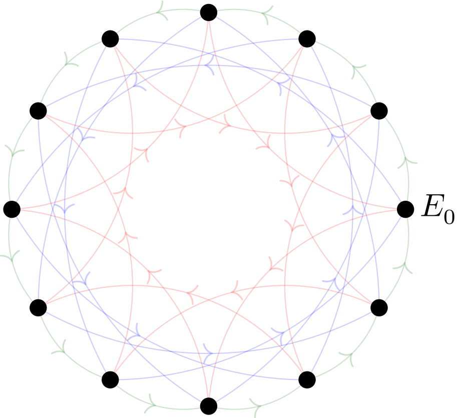
$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$



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 $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

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



Ordinary protocol - Couveignes & Rostovtsev-Stolbunov, 2006

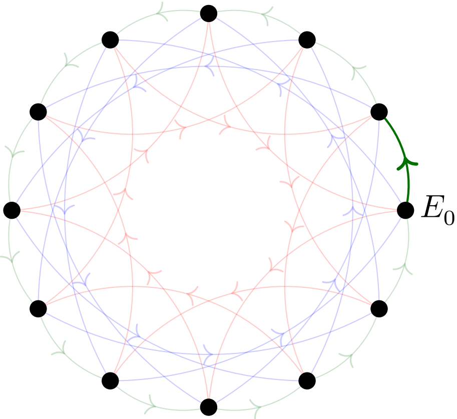
Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right)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

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

Alice

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

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



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.

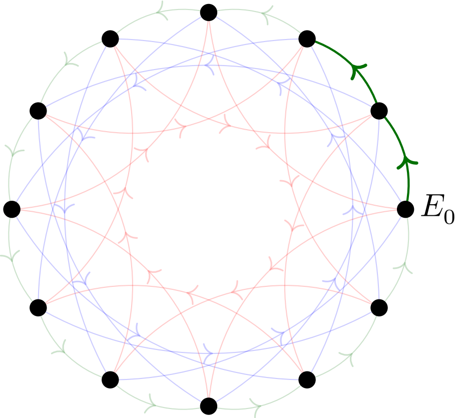
Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

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

Alice

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

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



Ordinary protocol - Couveignes & Rostovtsev-Stolbunov, 2006

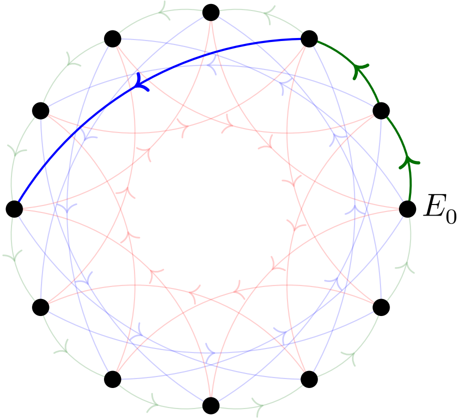
Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right)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

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

Alice

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

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



Ordinary protocol - Couveignes & Rostovtsev-Stolbunov, 2006

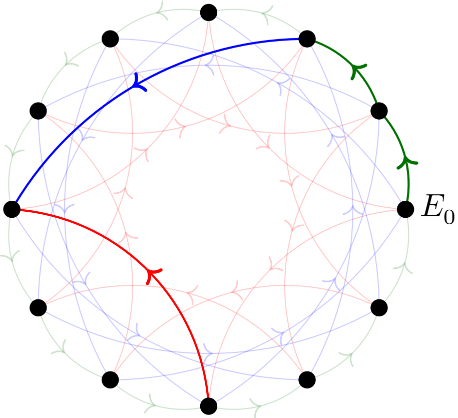
Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right)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

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

Alice

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

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



ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

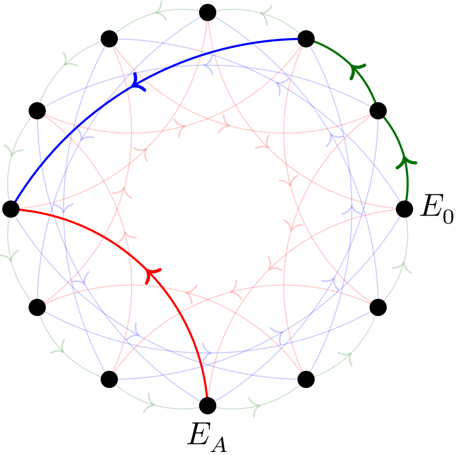
Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right)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

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

Alice

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

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



Ordinary protocol - Couveignes & Rostovtsev-Stolbunov, 2006

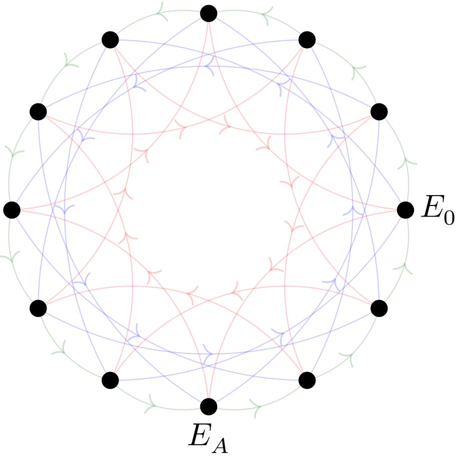
Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right)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

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

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

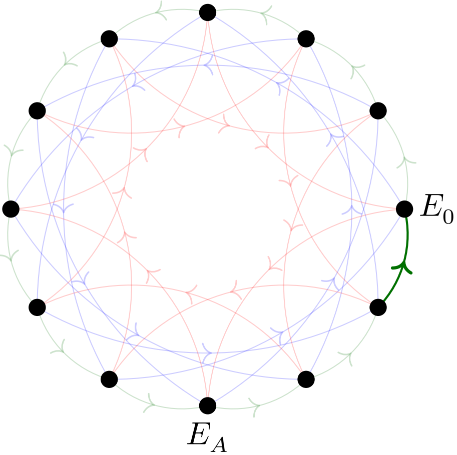
Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right)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

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

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

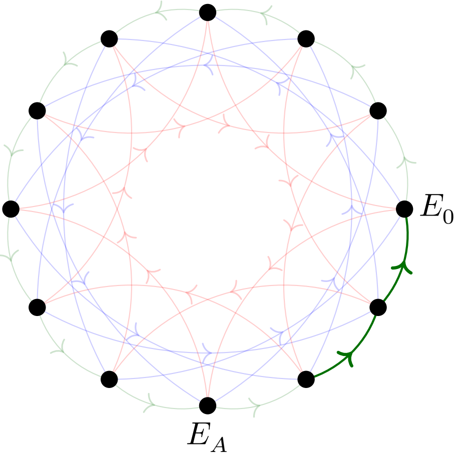
Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right)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

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

Alice

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

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



Bob

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

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

ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

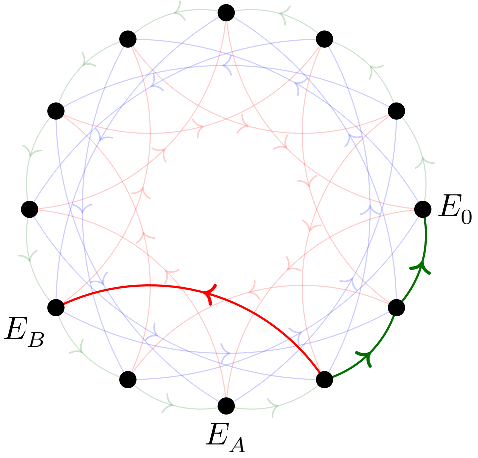
Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.
Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right)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

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

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

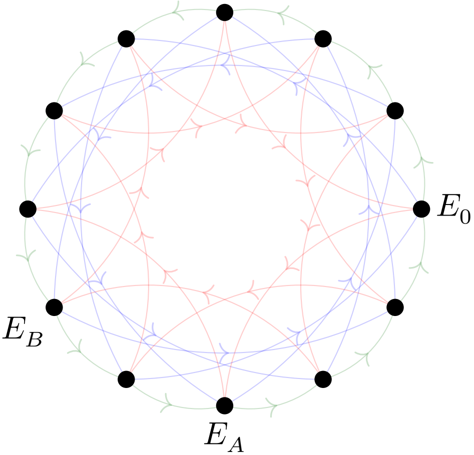
Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.
Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right)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

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

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

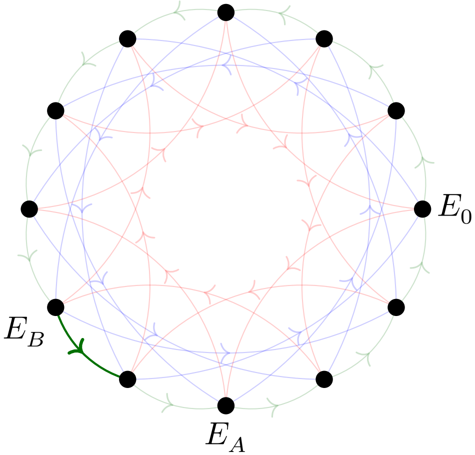
Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right)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

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

Alice

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

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



Bob

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

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

Ordinary protocol - Couveignes & Rostovtsev-Stolbunov, 2006

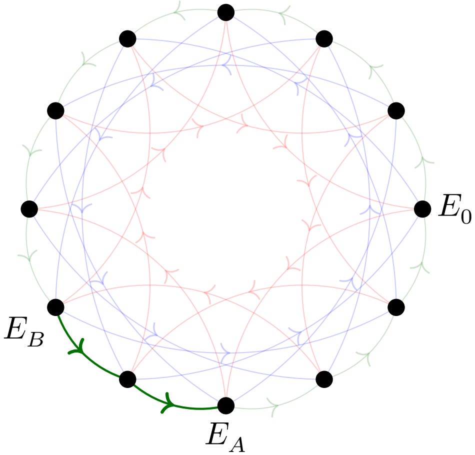
Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.
Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right)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

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

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

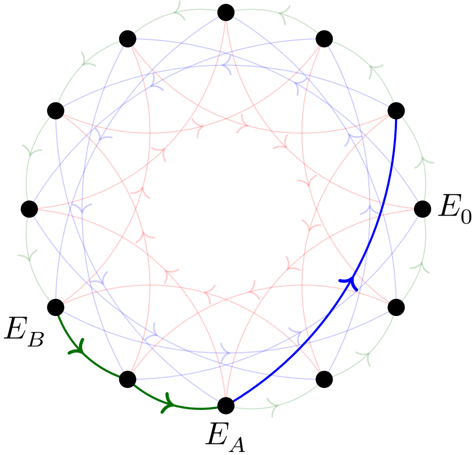
Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right)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

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

Alice

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

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



Bob

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

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

ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

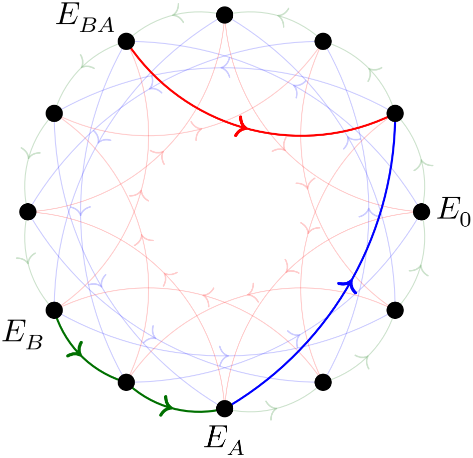
Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right)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

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

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

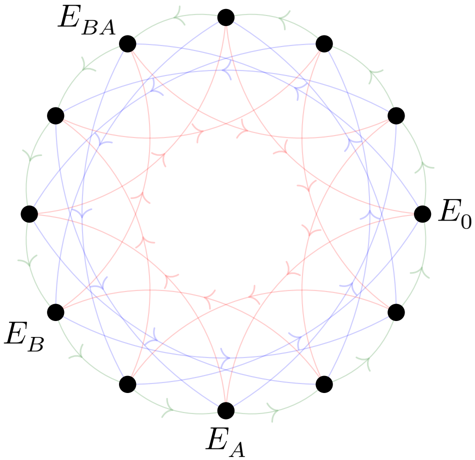
Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right)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

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

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

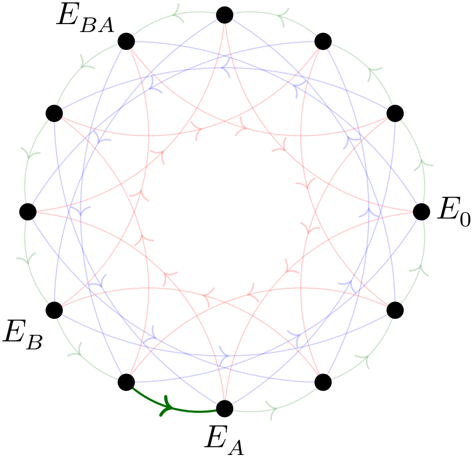
Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right)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

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

Alice

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

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



Bob

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

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

ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

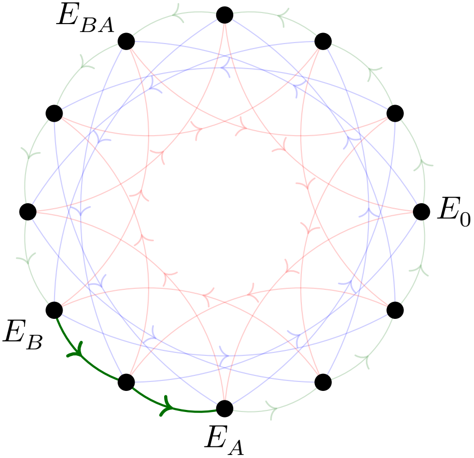
Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right)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

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

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.

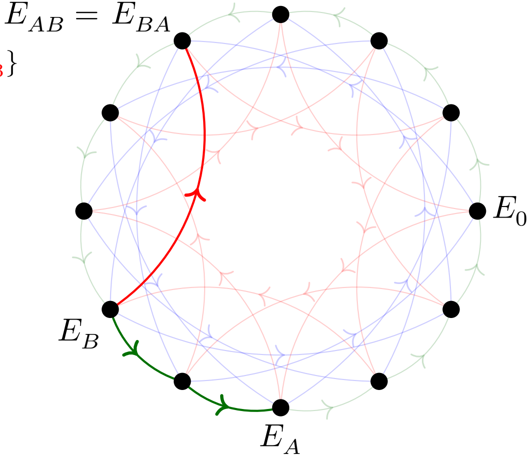
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

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

Alice

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

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



Bob

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

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

SIDH - L. De Feo & D. Jao, 2011

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:** $E/E\langle R_A,R_B\rangle=E_B/\langle\phi_B(R_A)\rangle=E_A/\langle\phi_A(R_B)\rangle$.

$$\begin{tikzcd}
 & E/\langle R_A\rangle,\ \begin{matrix}\phi_A(P_B)\\ \phi_A(Q_B)\end{matrix} \arrow[dr, dash, "\phi'_B"] & \\
E \arrow[ur, dash, "\phi_A"] \arrow[dr, dash, "\phi_B"'] \arrow[rr, dashed, shift left=2, "\phi_A(R_B)"'] \arrow[rr, dashed, shift right=2, "\phi_B(R_A)"] & & E/\langle R_A,R_B\rangle \\
 & E/\langle R_B\rangle,\ \begin{matrix}\phi_B(P_A)\\ \phi_B(Q_A)\end{matrix} \arrow[ur, dash, "\phi'_A"'] &
\end{tikzcd}$$

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

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

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 $\iota : K \hookrightarrow \mathsf{End}^0(E)$ determines a K-orientation $\phi_*(\iota) : K \hookrightarrow \mathsf{End}^0(F)$ 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

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

The set 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.

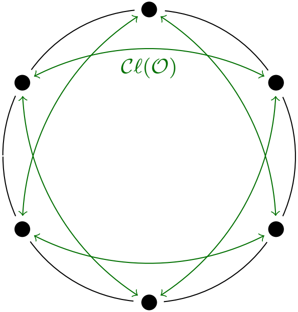
In particular, for fixed primitive $\mathcal{O}$-oriented E, we obtain a bijection of sets:

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

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 $[\mathfrak{a}] = [\mathfrak{q}_1^{e_1} \cdot \dots \cdot \mathfrak{q}_r^{e_r}]$, 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 $\mathcal{C}\ell(\mathcal{O})$.

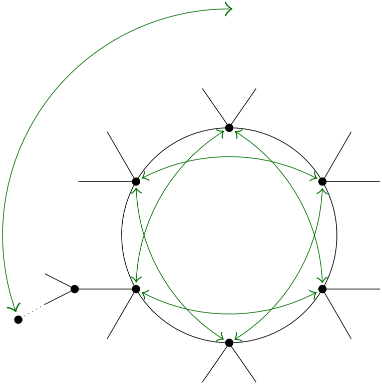


Instead of considering the union of different isogeny graphs, we focus on one single crater and we think of all the other primes as acting on it: the resulting object is a single isogeny circle rotating under the action of $\mathcal{C}\ell(\mathcal{O})$.

WHIRLPOOL

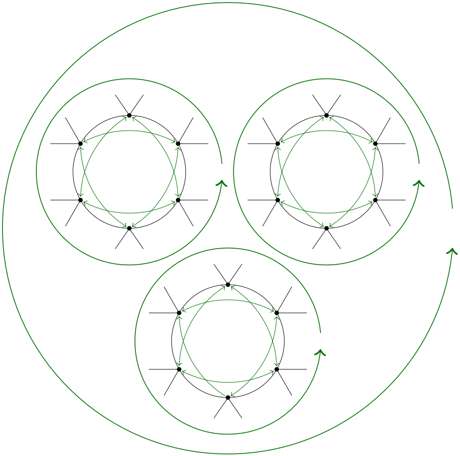
The action of $\mathcal{C}\ell(\mathcal{O})$ extends to the union $\bigcup_i SS_{\mathcal{O}_i}(p)$ over all superorders $\mathcal{O}_i$ containing $\mathcal{O}$ via the surjections $\mathcal{C}\ell(\mathcal{O}) \to \mathcal{C}\ell(\mathcal{O}_i)$.

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

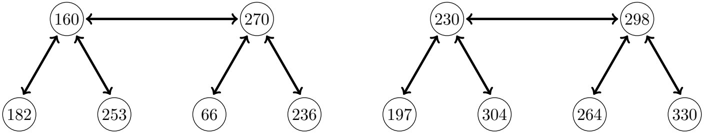
Actually, we would like to take the ℓ-isogeny graph on the full $\mathcal{C}\ell(\mathcal{O}_K)$-orbit. This might be composed of several ℓ-isogeny orbits (craters), although the class group is transitive.



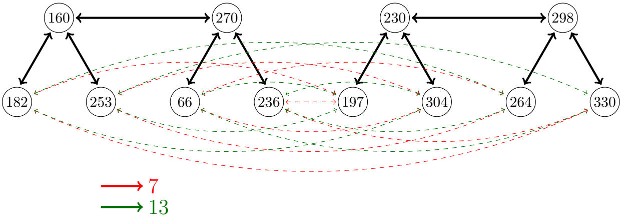
WHIRLPOOL - AN EXAMPLE

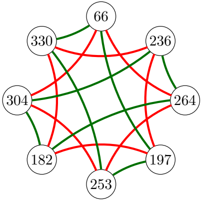
The set of multiple ℓ-volcanoes is called ℓ-cordillera.

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

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 $F_i = E_i/C_i$.

$$\begin{tikzcd}
E_{i-1}/C_{i-1} = F_{i-1} \arrow[r, "\ell"] & F_i = E_i/C_i \\
C_{i-1} \subseteq E_{i-1} \arrow[u, "\psi_{i-1}", "\mathfrak{q}"'] \arrow[r, "\phi_{i-1}", "\ell"'] & E_i \supseteq C_i \arrow[u, "\psi_i", "\mathfrak{q}"']
\end{tikzcd}$$

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 $\psi_i : E_i \to F_i$

$$\begin{tikzcd}
E_0 \arrow[r, "\phi_0"] \arrow[d, "\psi_0"'] & E_1 \arrow[r, "\phi_1"] \arrow[d, "\psi_1"'] & E_2 \arrow[r, "\phi_2"] \arrow[d, "\psi_2"'] & \cdots \arrow[r, "\phi_{n-1}"] & E_n \arrow[d, "\psi_n"'] \\
F_0 \arrow[r, "\phi_0'"'] & F_1 \arrow[r, "\phi_1'"'] & F_2 \arrow[r, "\phi_2'"'] & \cdots \arrow[r, "\phi_{n-1}'"'] & F_n
\end{tikzcd}$$

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).

FORGETFUL MAP

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

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

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

$$\mathsf{SS}_{\mathcal{O}_i}(p) \subset \mathsf{SS}_{\mathcal{O}_{i+1}}(p) = \mathsf{SS}_{\mathcal{O}_i}(p) \cup \mathsf{SS}^{pr}_{\mathcal{O}_{i+1}}(p)$$
$$\Downarrow$$
$$\mathsf{SS}_{\mathcal{O}_K}(p) \subset \mathsf{SS}_{\mathcal{O}_1}(p) \subset \cdots \subset \mathsf{SS}_{\mathcal{O}_i}(p) \subset \cdots$$

equipped with forgetful maps

$$\mathsf{SS}_{\mathcal{O}_i}(p) \to \mathsf{SS}(p)$$
$$[(E, \mathcal{O}_i)] \to j(E)$$

Question

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

Forgetful map - First results

Proposition

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

$p = 1013$

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

$p = 1019$

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

EFFECTIVE ENDOMORPHISM RINGS AND ISOGENIES

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

Examples. $\mathbb{Z}$ in $\mathrm{End}(E)$ is effective. Effective imaginary quadratic subrings $\mathcal{O} \subset \mathrm{End}(E)$, 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

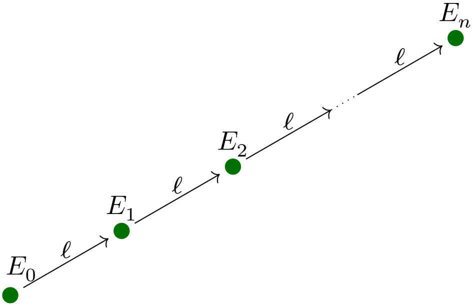
A *modular ℓ-isogeny chain* of length n over k is a finite sequence $(j_0, j_1, \dots, j_n)$ in k such that $\Phi_\ell(j_i, j_{i+1}) = 0$ for $0 \le i < n$.
A *modular ℓ-ladder* of length n and degree q over k is a pair of modular ℓ-isogeny chains

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

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

OSIDH - Introduction

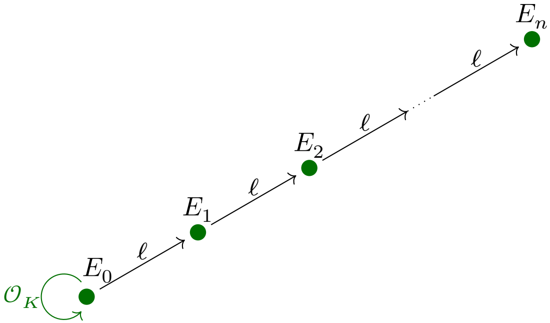
We consider an elliptic curve E_0 with an effective endomorphism ring (eg. $j_0 = 0, 1728$) and a chain of ℓ-isogenies.



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.

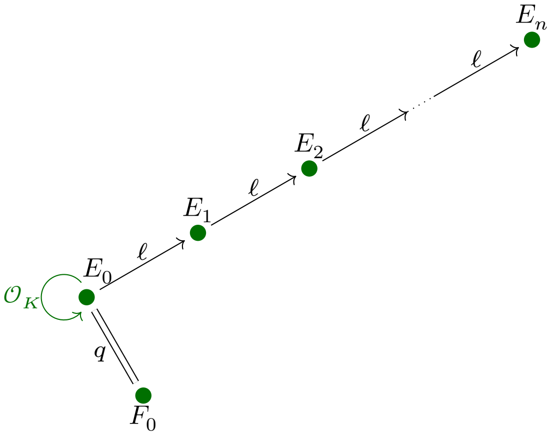
- For $\ell = 2$ (or 3) a suitable candidate for $\mathcal{O}_K$ could be the Gaussian integers $\mathbb{Z}[i]$ or the Eisenstein integers $\mathbb{Z}[\omega]$.



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.

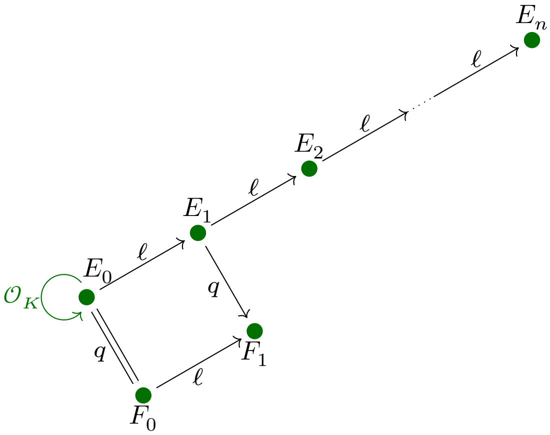
- Horizontal isogenies must be endomorphisms



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.

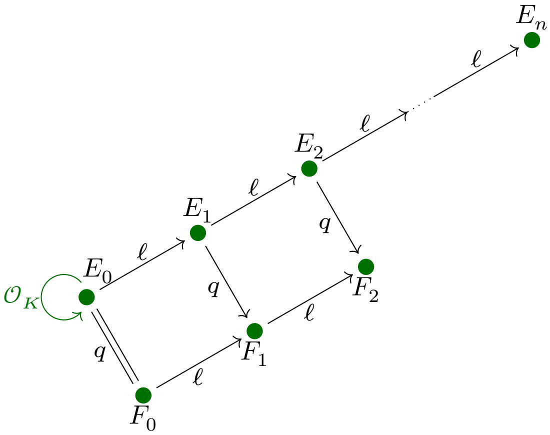
- We push forward our q-orientation obtaining F_1.



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.

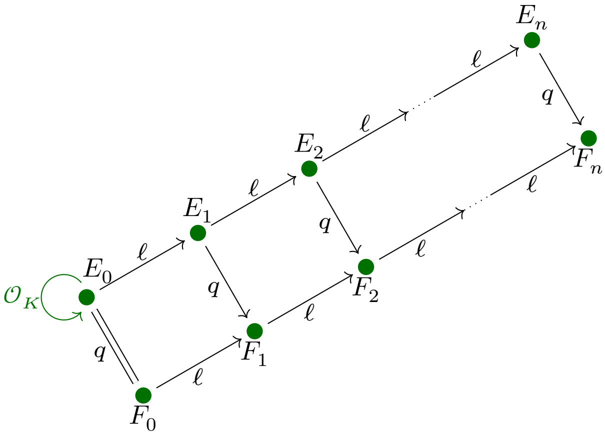
- We repeat the process for F_2.



OSIDH - Introduction

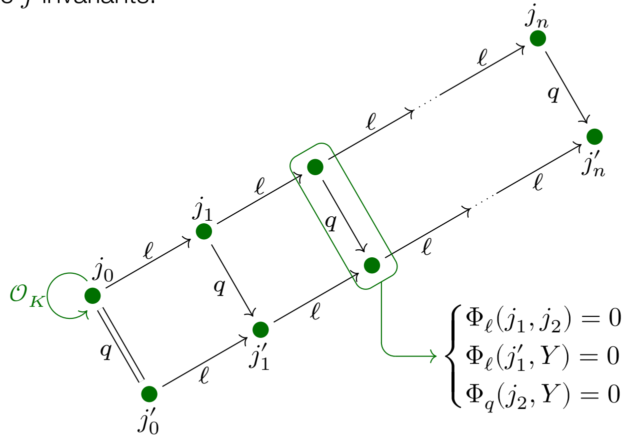
We consider an elliptic curve E_0 with an effective endomorphism ring (eg. $j_0 = 0, 1728$) and a chain of ℓ-isogenies.

- And again till F_n.



OSIDH - Introduction & Modular Approach

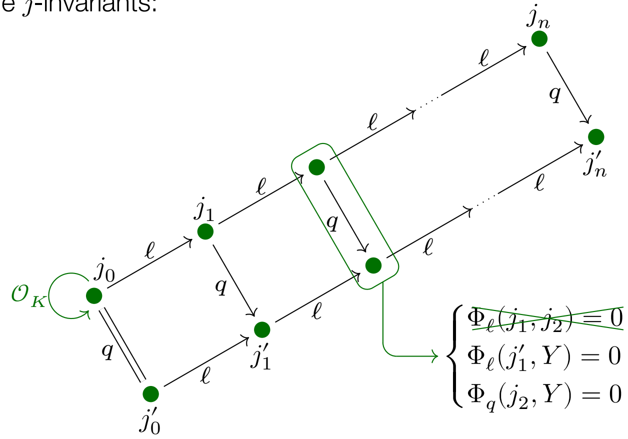
If we look at modular polynomials $\Phi_\ell(X,Y)$ and $\Phi_q(X,Y)$ we realize that all we need are the j-invariants:



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

OSIDH - Introduction & modular approach

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:



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

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

HOW MANY STEPS BEFORE THE IDEALS ACT DIFFERENTLY?

$$\begin{tikzcd}
E_0 \arrow[r, shift left, "\mathfrak{q}"] \arrow[rr, bend left, "\mathfrak{q}^2"] \arrow[d] & E_0 \arrow[l, shift left, "\bar{\mathfrak{q}}"] \arrow[r, "\mathfrak{q}"] \arrow[d] & E_0 \arrow[d] \\
E_1'' \arrow[d] & E_1 \arrow[l] \arrow[r] \arrow[d] & E_1' \arrow[d] \\
{} & {} & {}
\end{tikzcd}$$

$E_i' \neq E_i''$ 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

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

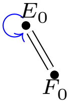
A FIRST NAIVE PROTOCOL

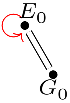
PUBLIC DATA: A chain of ℓ-isogenies $E_0 \to E_1 \to ... \to E_n$

ALICE

BOB

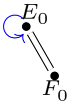
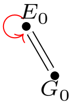
Choose a primitive $\mathcal{O}_K$-orientation of E_0





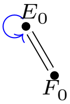
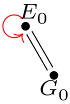
A FIRST NAIVE PROTOCOL

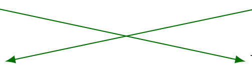
PUBLIC DATA: A chain of ℓ-isogenies $E_0 \to E_1 \to ... \to E_n$

	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

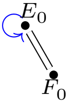
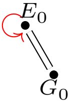
PUBLIC DATA: A chain of ℓ-isogenies $E_0 \to E_1 \to \ldots \to E_n$

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



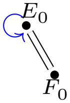
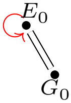
A FIRST NAIVE PROTOCOL

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

	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 $\phi_B \cdot \{F_i\}$

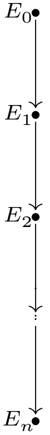
A FIRST NAIVE PROTOCOL

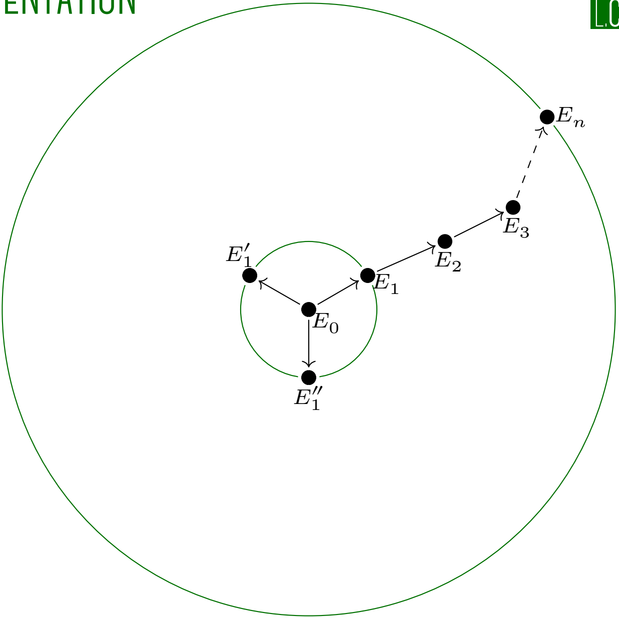
PUBLIC DATA: A chain of ℓ-isogenies $E_0 \to E_1 \to ... \to E_n$

	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 $E_0 \to H_1 \to ... \to H_n$

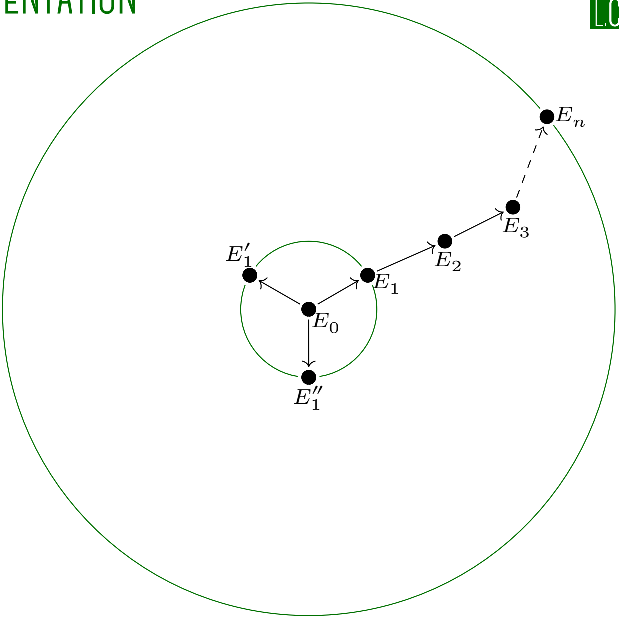
GRAPHIC REPRESENTATION



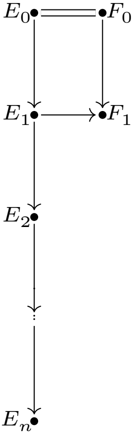


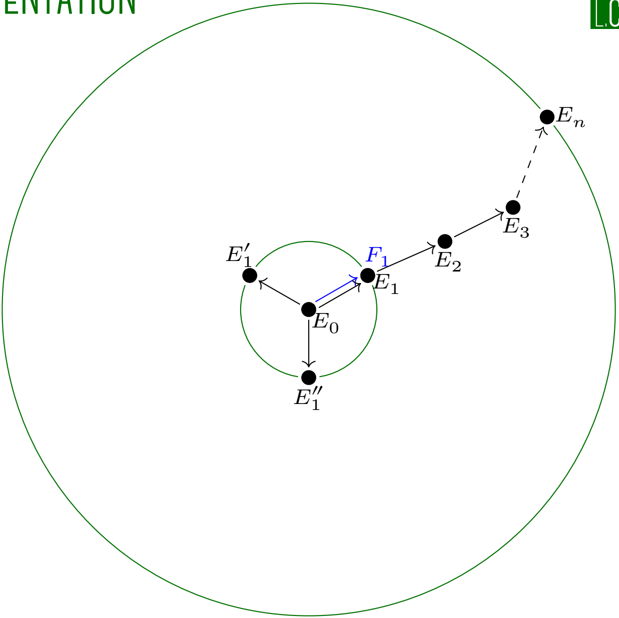
GRAPHIC REPRESENTATION

$$\begin{tikzcd}
E_0 \arrow[r, equal] \arrow[d] & F_0 \\
E_1 \arrow[d] & \\
E_2 \arrow[d] & \\
\vdots \arrow[d] & \\
E_n &
\end{tikzcd}$$



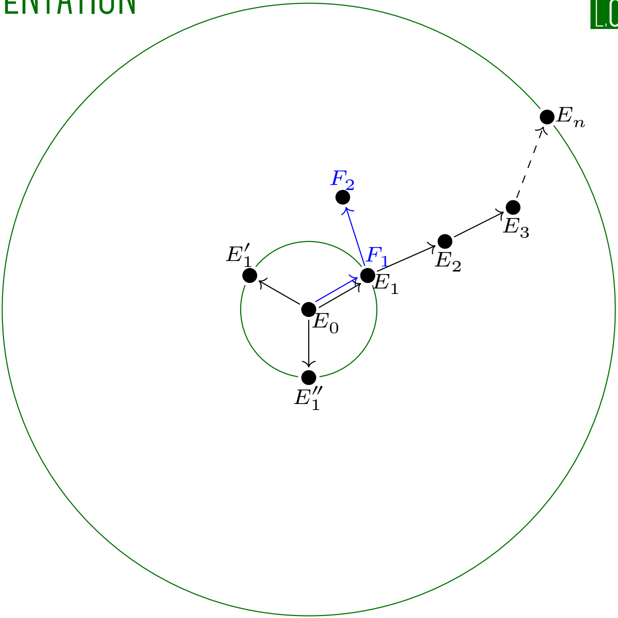
GRAPHIC REPRESENTATION





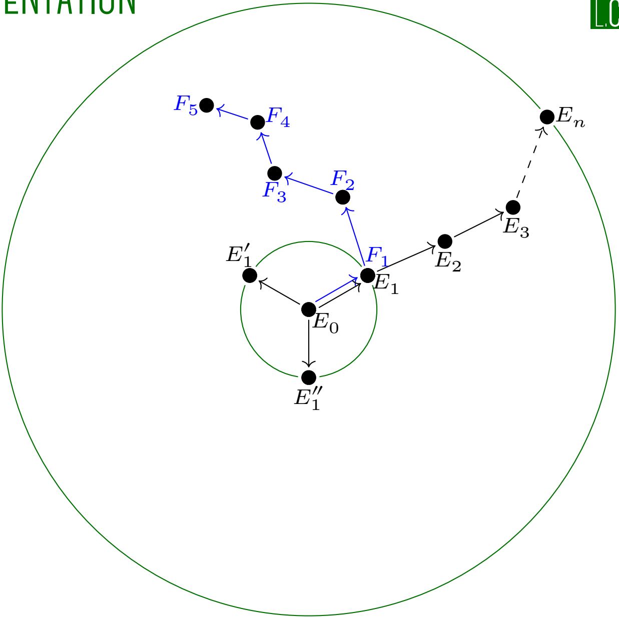
GRAPHIC REPRESENTATION

$$\begin{tikzcd}
E_0 \arrow[r, equal] \arrow[d] & F_0 \arrow[d] \\
E_1 \arrow[r] \arrow[d] & F_1 \arrow[d] \\
E_2 \arrow[r] \arrow[d] & F_2 \\
\vdots \arrow[d] & \\
E_n &
\end{tikzcd}$$



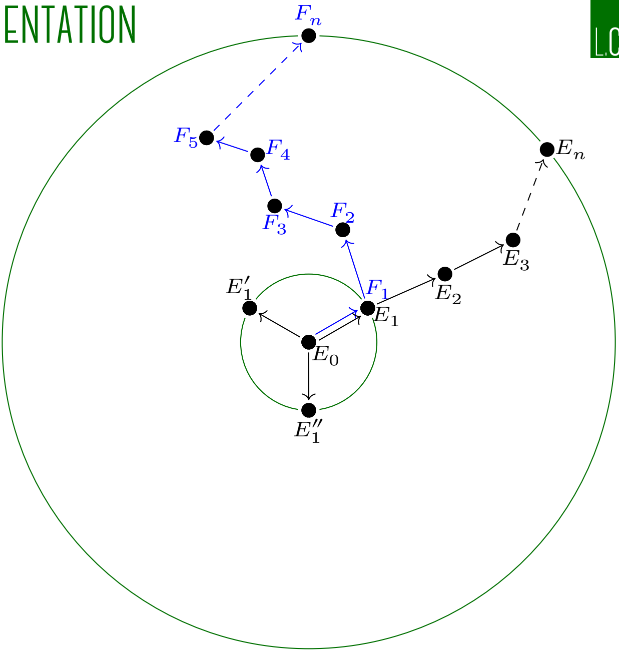
GRAPHIC REPRESENTATION

$$\begin{tikzcd}
E_0 \arrow[r, equal] \arrow[d] & F_0 \arrow[d] \\
E_1 \arrow[r] \arrow[d] & F_1 \arrow[d] \\
E_2 \arrow[r] \arrow[d] & F_2 \arrow[d] \\
\vdots \arrow[d] & \vdots \\
E_n &
\end{tikzcd}$$



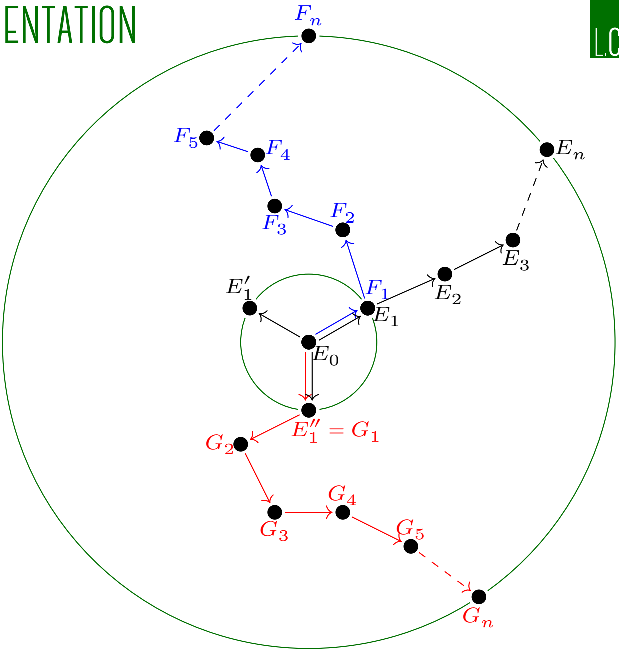
GRAPHIC REPRESENTATION

$$\begin{tikzcd}
E_0 \arrow[r, equal] \arrow[d] & F_0 \arrow[d] \\
E_1 \arrow[r] \arrow[d] & F_1 \arrow[d] \\
E_2 \arrow[r] \arrow[d] & F_2 \arrow[d] \\
\vdots \arrow[d] & \vdots \arrow[d] \\
E_n \arrow[r] & F_n
\end{tikzcd}$$



GRAPHIC REPRESENTATION

$$\begin{tikzcd}
E_0 \arrow[r, equal] \arrow[d] & G_0 \arrow[d] \\
E_1 \arrow[r] \arrow[d] & G_1 \arrow[d] \\
E_2 \arrow[r] \arrow[d] & G_2 \arrow[d] \\
\vdots \arrow[d] & \vdots \arrow[d] \\
E_n \arrow[r] & G_n
\end{tikzcd}$$



Graphic representation

$$\begin{tikzcd}
& H_0 \arrow[rr] & & H_1 \arrow[rr] & & H_2 \arrow[rr] & & \cdots \arrow[rr] & & H_n \\
F_0 \arrow[ur, red] \arrow[rr, blue] & & F_1 \arrow[ur, red] \arrow[rr, blue] & & F_2 \arrow[ur, red] \arrow[rr, blue] & & {\color{blue}\cdots} \arrow[rr, blue] & & F_n \arrow[ur, red] & \\
& G_0 \arrow[uu, blue] \arrow[rr, red] & & G_1 \arrow[uu, blue] \arrow[rr, red] & & G_2 \arrow[uu, blue] \arrow[rr, red] & & {\color{red}\cdots} \arrow[rr, red] & & G_n \arrow[uu, blue] \\
E_0 \arrow[uu, blue] \arrow[ur, red] \arrow[rr] & & E_1 \arrow[uu, blue] \arrow[ur, red] \arrow[rr] & & E_2 \arrow[uu, blue] \arrow[ur, red] \arrow[rr] & & \cdots \arrow[rr] & & E_n \arrow[uu, blue] \arrow[ur, red] &
\end{tikzcd}$$

⟶ Alice

⟶ Bob

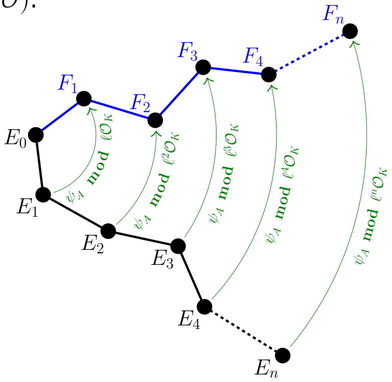
A FIRST NAIVE PROTOCOL - WEAKNESS

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

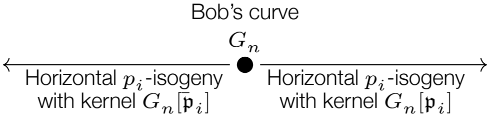

F_n
F_3
F_4
F_1
F_2
E_0
ψ_A mod $\ell\mathcal{O}_K$
ψ_A mod $\ell^2\mathcal{O}_K$
ψ_A mod $\ell^3\mathcal{O}_K$
ψ_A mod $\ell^4\mathcal{O}_K$
ψ_A mod $\ell^n\mathcal{O}_K$
E_1
E_2
E_3
E_4
E_n

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 $\mathfrak{p}_i$:



Bob's curve

G_n

Horizontal p_i-isogeny with kernel $G_n[\bar{\mathfrak{p}}_i]$

Horizontal p_i-isogeny with kernel $G_n[\mathfrak{p}_i]$

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

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

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 $[-r, r]$	$(e_1, \dots, e_t)$	$(d_1, \dots, d_t)$

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

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 $E_0 \to E_1 \to \dots \to E_n$ 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 $\forall i$	$F_{n,i}^{(-r)} \leftarrow F_{n,i}^{(-r+1)} \leftarrow \dots \leftarrow F_{n,i}^{(1)} \leftarrow F_n$	$G_{n,i}^{(-r)} \leftarrow G_{n,i}^{(-r+1)} \leftarrow \dots \leftarrow G_{n,i}^{(1)} \leftarrow G_n$
... and their conjugates	$F_n \to F_{n,i}^{(1)} \to \dots \to F_{n,i}^{(r-1)} \to F_{n,1}^{(r)}$	$G_n \to G_{n,i}^{(1)} \to \dots \to G_{n,i}^{(r-1)} \to G_{n,1}^{(r)}$

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

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 $E_0 \to E_1 \to \dots \to E_n$ 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 $j > i$.

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

OSIDH PROTOCOL - GRAPHIC REPRESENTATION I

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

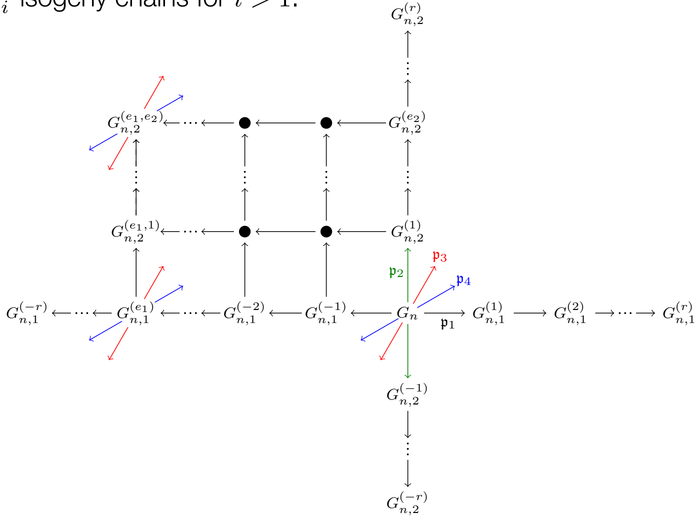
$$F_n = \frac{E_n}{E_n\left[\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_t^{e_t}\right]}$$

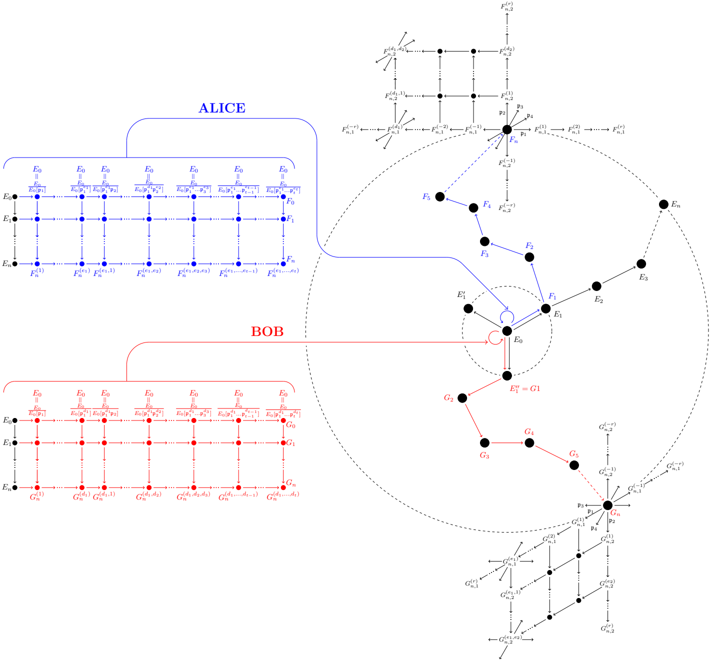
by means of constructing the following commutative diagram

$$\begin{tikzcd}
 & E_0 \arrow[d, equal] & & E_0 \arrow[d, equal] & E_0 \arrow[d, equal] & & E_0 \arrow[d, equal] & & E_0 \arrow[d, equal] & & E_0 \arrow[d, equal] \\
 & \frac{E_0}{E_0[\mathfrak{p}_1]} & & \frac{E_0}{E_0\left[\mathfrak{p}_1^{e1}\right]} & \frac{E_0}{E_0\left[\mathfrak{p}_1^{e1}\mathfrak{p}_2\right]} & & \frac{E_0}{E_0\left[\mathfrak{p}_1^{e1}\mathfrak{p}_2^{e2}\right]} & & \frac{E_0}{E_0\left[\mathfrak{p}_1^{e1}\dots\mathfrak{p}_{t-1}^{et-1}\right]} & & \frac{E_0}{E_0\left[\mathfrak{p}_1^{e1}\dots\mathfrak{p}_t^{et}\right]} \\
E_0 \arrow[r] \arrow[d] & \bullet \arrow[r] \arrow[d] & \cdots \arrow[r] & \bullet \arrow[r] \arrow[d] & \bullet \arrow[r] \arrow[d] & \cdots \arrow[r] & \bullet \arrow[r] \arrow[d] & \cdots \arrow[r] & \bullet \arrow[r] \arrow[d] & \cdots \arrow[r] & F_0 \arrow[d] \\
E_1 \arrow[r] \arrow[d] & \bullet \arrow[r] \arrow[d] & \cdots \arrow[r] & \bullet \arrow[r] \arrow[d] & \bullet \arrow[r] \arrow[d] & \cdots \arrow[r] & \bullet \arrow[r] \arrow[d] & \cdots \arrow[r] & \bullet \arrow[r] \arrow[d] & \cdots \arrow[r] & F_1 \arrow[d] \\
\vdots \arrow[d] & \vdots \arrow[d] & & \vdots \arrow[d] & \vdots \arrow[d] & & \vdots \arrow[d] & & \vdots \arrow[d] & & \vdots \arrow[d] \\
E_n \arrow[r] & \bullet \arrow[r] & \cdots \arrow[r] & \bullet \arrow[r] & \bullet \arrow[r] & \cdots \arrow[r] & \bullet \arrow[r] & \cdots \arrow[r] & \bullet \arrow[r] & \cdots \arrow[r] & F_n \\
 & F_n^{(1)} & & F_n^{(e_1)} & F_n^{(e_1,1)} & & F_n^{(e_1,e_2)} & & F_n^{(e_1,\dots,e_{t-1})} & & F_n^{(e_1,\dots,e_t)}
\end{tikzcd}$$

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_n
$\frac{E_0}{E_0[\mathfrak{p}_1]}$
$\frac{E_0}{E_0[\mathfrak{p}_1^{e_1}]}$
$\frac{E_0}{E_0[\mathfrak{p}_1^{e_1}\mathfrak{p}_2]}$
$\frac{E_0}{E_0[\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}]}$
$\frac{E_0}{E_0[\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_3^{e_3}]}$
$\frac{E_0}{E_0[\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_{t-1}^{e_{t-1}}]}$
$\frac{E_0}{E_0[\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_t^{e_t}]}$
F_0
F_1
F_n
$F_n^{(1)}$
$F_n^{(e_1)}$
$F_n^{(e_1,1)}$
$F_n^{(e_1,e_2)}$
$F_n^{(e_1,e_2,e_3)}$
$F_n^{(e_1,\ldots,e_{t-1})}$
$F_n^{(e_1,\ldots,e_t)}$
$\frac{E_0}{E_0[\mathfrak{p}_1^{d_1}]}$
$\frac{E_0}{E_0[\mathfrak{p}_1^{d_1}\mathfrak{p}_2]}$
$\frac{E_0}{E_0[\mathfrak{p}_1^{d_1}\mathfrak{p}_2^{d_2}]}$
$\frac{E_0}{E_0[\mathfrak{p}_1^{d_1}\cdots\mathfrak{p}_3^{d_3}]}$
$\frac{E_0}{E_0[\mathfrak{p}_1^{d_1}\cdots\mathfrak{p}_{t-1}^{d_{t-1}}]}$
$\frac{E_0}{E_0[\mathfrak{p}_1^{d_1}\cdots\mathfrak{p}_t^{d_t}]}$
G_0
G_1
G_n
$G_n^{(1)}$
$G_n^{(d_1)}$
$G_n^{(d_1,1)}$
$G_n^{(d_1,d_2)}$
$G_n^{(d_1,d_2,d_3)}$
$G_n^{(d_1,\ldots,d_{t-1})}$
$G_n^{(d_1,\ldots,d_t)}$
$F_{n,2}^{(r)}$
$F_{n,2}^{(d_1,d_2)}$
$F_{n,2}^{(d_2)}$
$F_{n,2}^{(d_1,1)}$
$F_{n,2}^{(1)}$
$\mathfrak{p}_3$
$\mathfrak{p}_2$
$\mathfrak{p}_4$
$\mathfrak{p}_1$
$F_{n,1}^{(-r)}$
$F_{n,1}^{(d_1)}$
$F_{n,1}^{(-2)}$
$F_{n,1}^{(-1)}$
$F_{n,1}^{(1)}$
$F_{n,1}^{(2)}$
$F_{n,1}^{(r)}$
F_n
$F_{n,2}^{(-1)}$
$F_{n,2}^{(-r)}$
F_5
F_4
F_3
F_2
F_1
E_n
E_3
E_2
E_1
E_1'
E_0
$E_1'' = G1$
G_2
G_3
G_4
G_5
$G_{n,2}^{(-r)}$
$G_{n,2}^{(-1)}$
$G_{n,1}^{(-r)}$
$G_{n,1}^{(-1)}$
$\mathfrak{p}_3$
$\mathfrak{p}_1$
G_n
$\mathfrak{p}_2$
$\mathfrak{p}_4$
$G_{n,1}^{(1)}$
$G_{n,1}^{(2)}$
$G_{n,2}^{(1)}$
$G_{n,1}^{(e_1)}$
$G_{n,1}^{(r)}$
$G_{n,2}^{(e_2)}$
$G_{n,2}^{(e_1,1)}$
$G_{n,2}^{(r)}$
$G_{n,2}^{(e_1,e_2)}$

OSIDH PROTOCOL - AN EXAMPLE

$p = 10007$

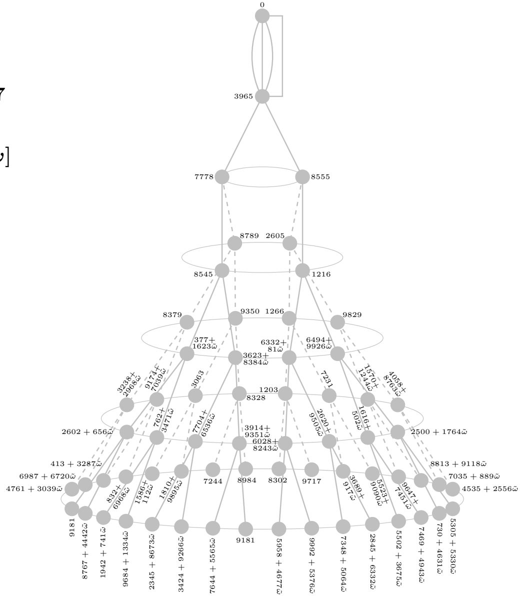
$\ell = 2$

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

$\ell_1 = 13$

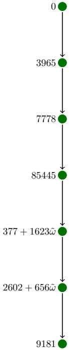
$\ell_2 = 31$

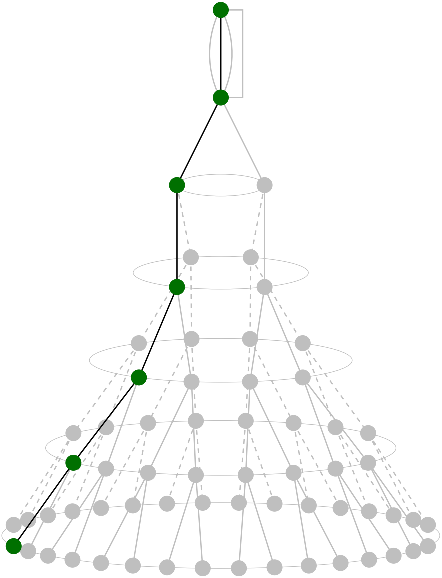
$\ell_3 = 43$



OSIDH PROTOCOL - AN EXAMPLE

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

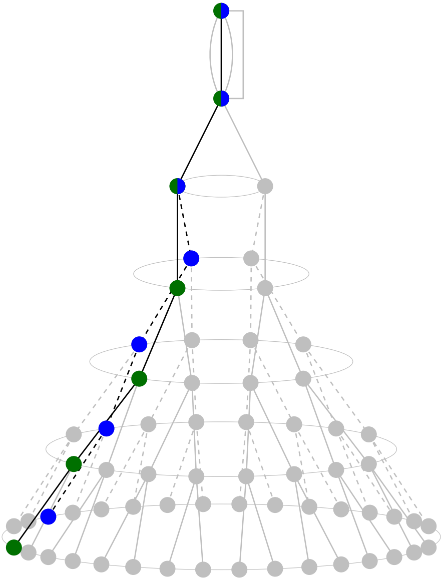




OSIDH PROTOCOL - AN EXAMPLE

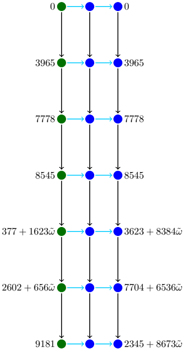
Alice secret key: $\mathfrak{l}_1^5\mathfrak{l}_2^3\mathfrak{l}_3^2$

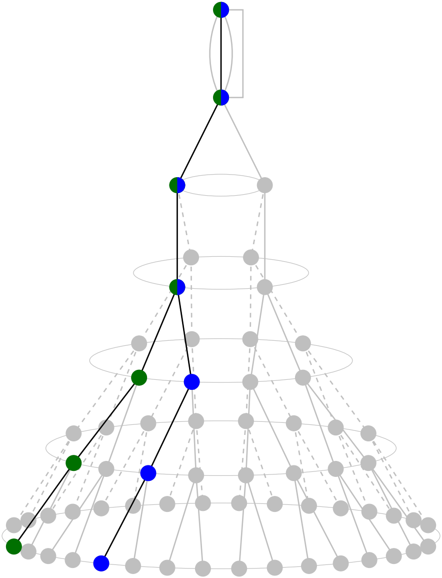
$$\begin{tikzcd}
0 \arrow[r] \arrow[d] & 0 \arrow[d] \\
3965 \arrow[r] \arrow[d] & 3965 \arrow[d] \\
7778 \arrow[r] \arrow[d] & 7778 \arrow[d] \\
8545 \arrow[r] \arrow[d] & 8789 \arrow[d] \\
377+1623\tilde{\omega} \arrow[r] \arrow[d] & 8379 \arrow[d] \\
2602+656\tilde{\omega} \arrow[r] \arrow[d] & 9174+7039\tilde{\omega} \arrow[d] \\
9181 \arrow[r] & 413+3287\tilde{\omega}
\end{tikzcd}$$



OSIDH PROTOCOL - AN EXAMPLE

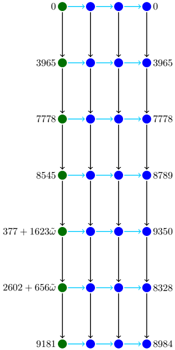
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$

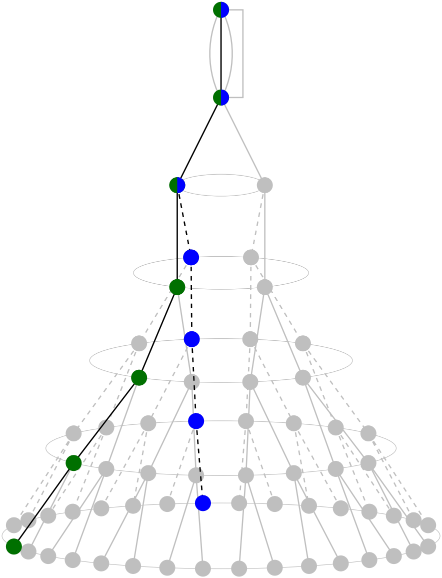

0
0
3965
3965
7778
7778
8545
8545
$377 + 1623\tilde{\omega}$
$3623 + 8384\tilde{\omega}$
$2602 + 656\tilde{\omega}$
$7704 + 6536\tilde{\omega}$
9181
$2345 + 8673\tilde{\omega}$



OSIDH protocol - an example

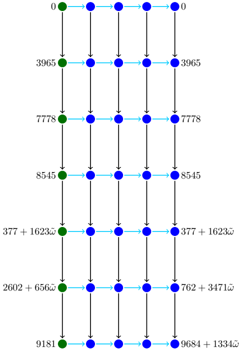
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$



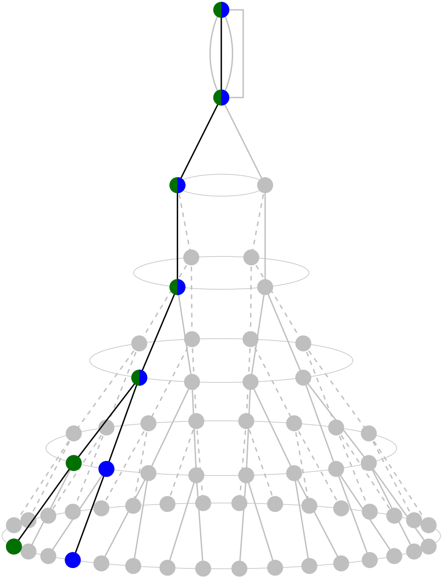


OSIDH PROTOCOL - AN EXAMPLE

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

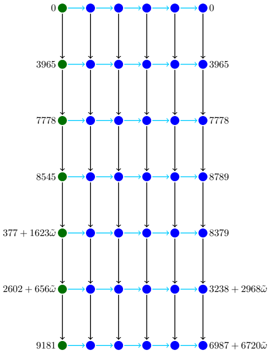


0
0
3965
3965
7778
7778
8545
8545
$377 + 1623\tilde{\omega}$
$377 + 1623\tilde{\omega}$
$2602 + 656\tilde{\omega}$
$762 + 3471\tilde{\omega}$
9181
$9684 + 1334\tilde{\omega}$

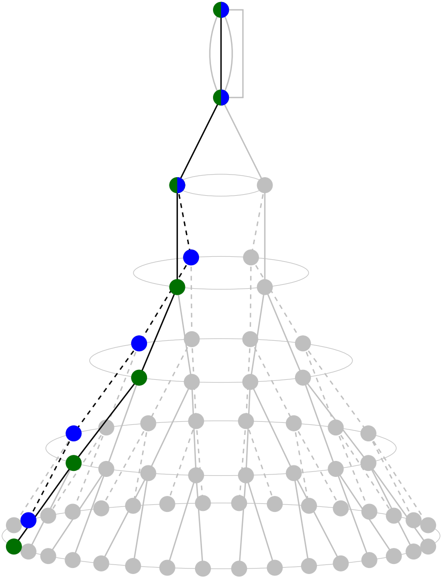


OSIDH PROTOCOL - AN EXAMPLE

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

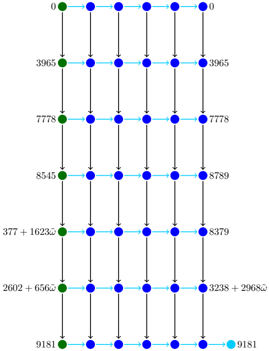


0
0
3965
3965
7778
7778
8545
8789
$377 + 1623\tilde{\omega}$
8379
$2602 + 656\tilde{\omega}$
$3238 + 2968\tilde{\omega}$
9181
$6987 + 6720\tilde{\omega}$

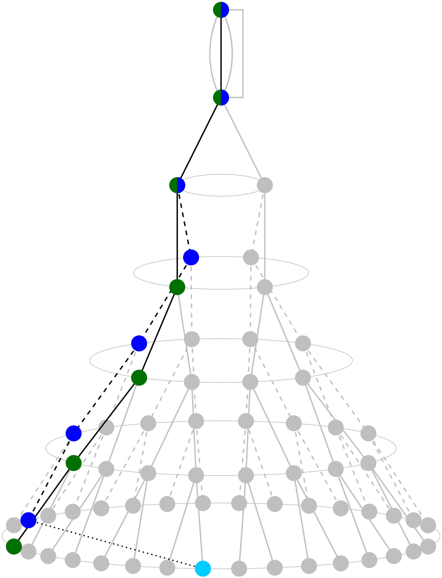


OSIDH PROTOCOL - AN EXAMPLE

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

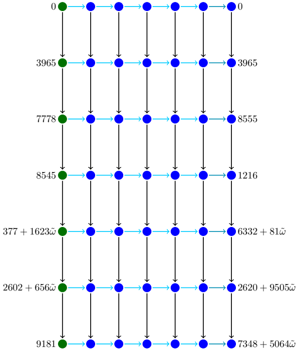


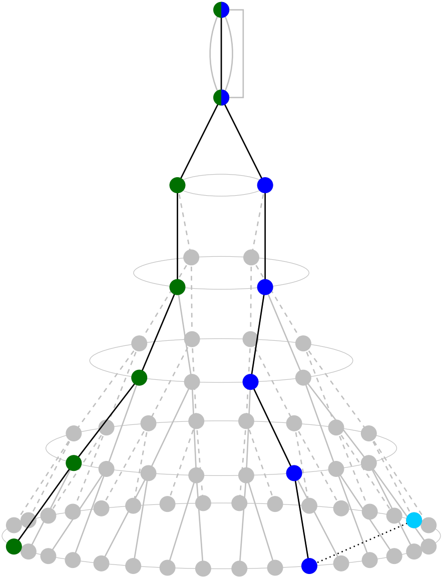
0
0
3965
3965
7778
7778
8545
8789
377 + 1623$\tilde{\omega}$
8379
2602 + 656$\tilde{\omega}$
3238 + 2968$\tilde{\omega}$
9181
9181



OSIDH PROTOCOL - AN EXAMPLE

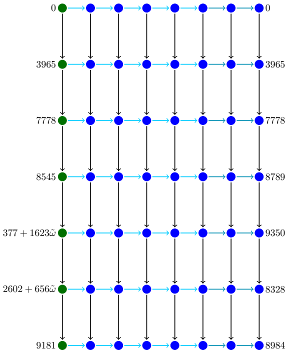
Alice secret key: $\mathfrak{l}_1^5\mathfrak{l}_2^3\mathfrak{l}_3^2$

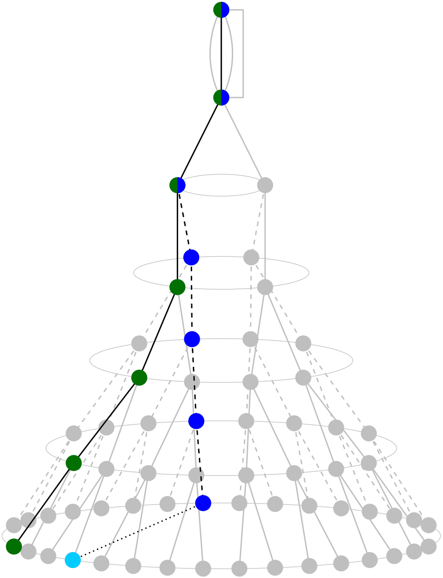

0
0
3965
3965
7778
8555
8545
1216
$377 + 1623\tilde{\omega}$
$6332 + 81\tilde{\omega}$
$2602 + 656\tilde{\omega}$
$2620 + 9505\tilde{\omega}$
9181
$7348 + 5064\tilde{\omega}$



OSIDH PROTOCOL - AN EXAMPLE

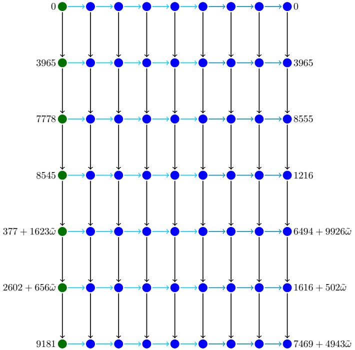
Alice secret key: $\mathfrak{l}_1^5\mathfrak{l}_2^3\mathfrak{l}_3^2$

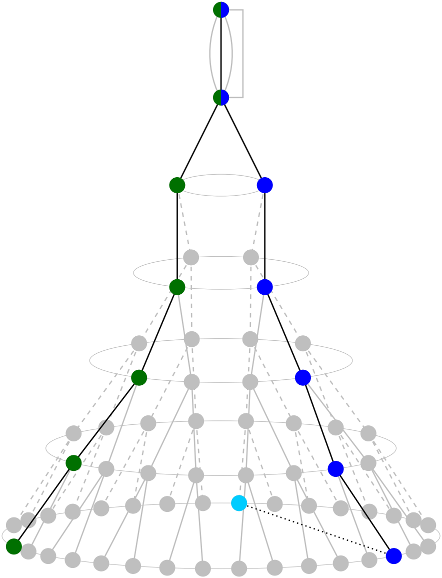




OSIDH PROTOCOL - AN EXAMPLE

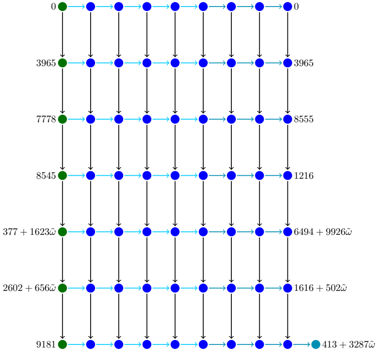
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$

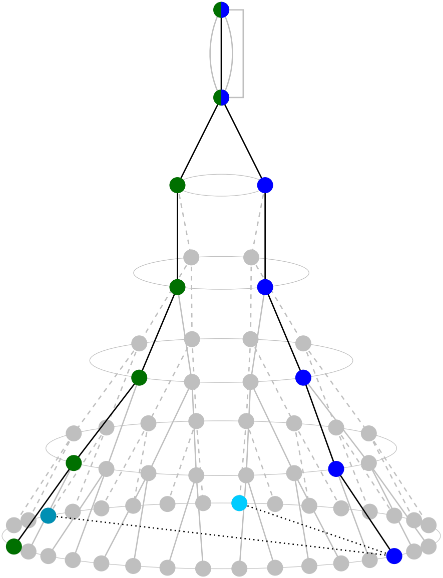

0
0
3965
3965
7778
8555
8545
1216
$377 + 1623\tilde{\omega}$
$6494 + 9926\tilde{\omega}$
$2602 + 656\tilde{\omega}$
$1616 + 502\tilde{\omega}$
9181
$7469 + 4943\tilde{\omega}$



OSIDH PROTOCOL - AN EXAMPLE

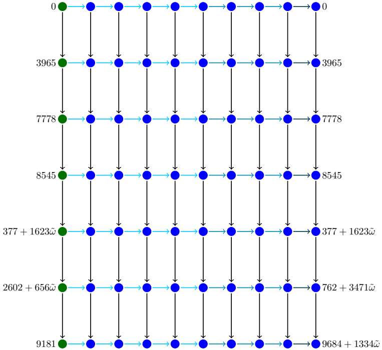
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$

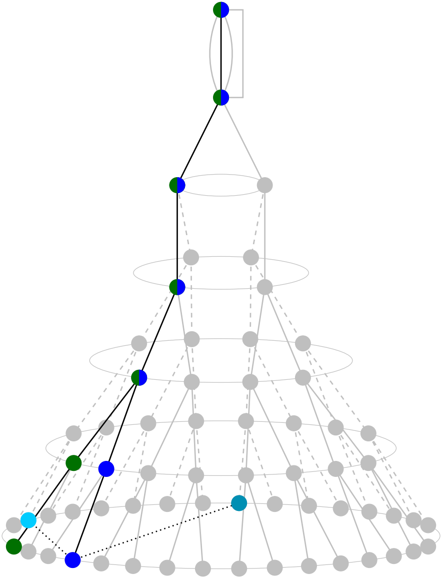

0
0
3965
3965
7778
8555
8545
1216
$377 + 1623\tilde{\omega}$
$6494 + 9926\tilde{\omega}$
$2602 + 656\tilde{\omega}$
$1616 + 502\tilde{\omega}$
9181
$413 + 3287\tilde{\omega}$



OSIDH PROTOCOL - AN EXAMPLE

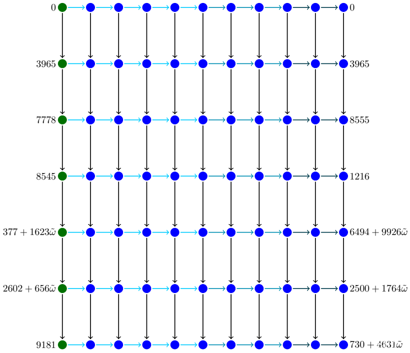
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$


0
0
3965
3965
7778
7778
8545
8545
$377 + 1623\tilde{\omega}$
$377 + 1623\tilde{\omega}$
$2602 + 656\tilde{\omega}$
$762 + 3471\tilde{\omega}$
9181
$9684 + 1334\tilde{\omega}$

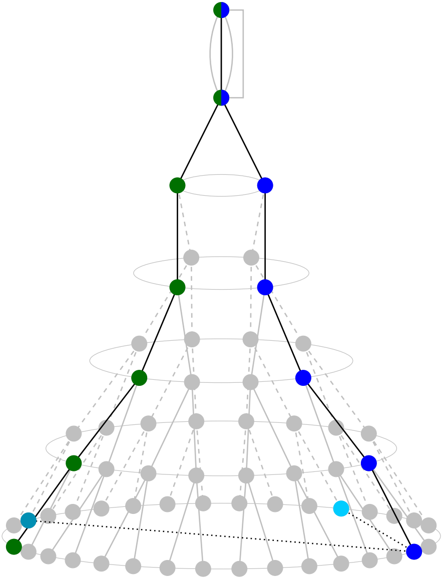


OSIDH PROTOCOL - AN EXAMPLE

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

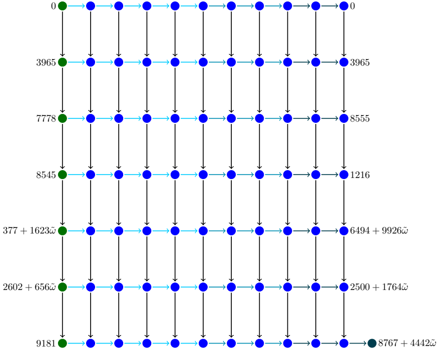


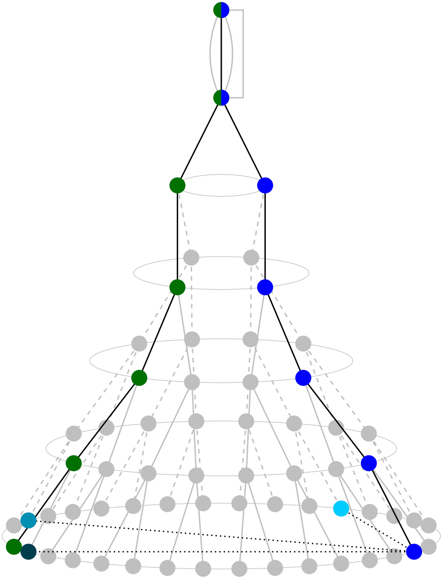
0
0
3965
3965
7778
8555
8545
1216
$377 + 1623\tilde{\omega}$
$6494 + 9926\tilde{\omega}$
$2602 + 656\tilde{\omega}$
$2500 + 1764\tilde{\omega}$
9181
$730 + 4631\tilde{\omega}$



OSIDH PROTOCOL - AN EXAMPLE

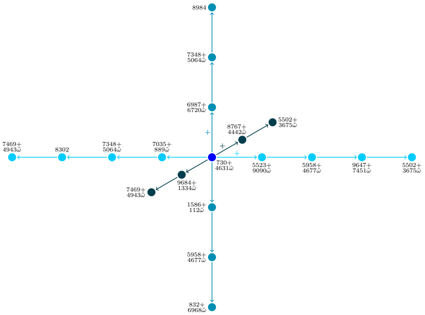
Alice secret key: $\mathfrak{l}_1^5\mathfrak{l}_2^3\mathfrak{l}_3^2$

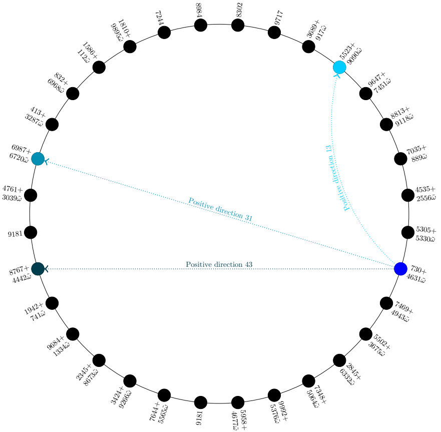




OSIDH PROTOCOL - AN EXAMPLE

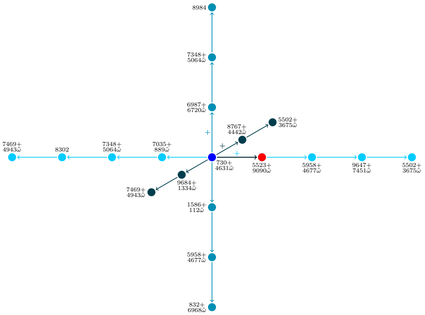
Bob secret key: $\mathfrak{l}_1^3\mathfrak{l}_2\mathfrak{l}_3^2$

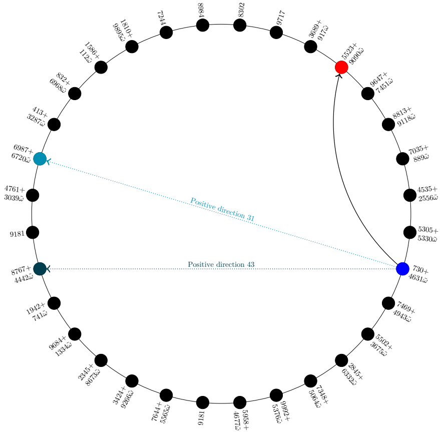

8984
7348+5064$\tilde{\omega}$
6987+6720$\tilde{\omega}$
+
8767+4442$\tilde{\omega}$
5502+3675$\tilde{\omega}$
+
7469+4943$\tilde{\omega}$
8302
7348+5064$\tilde{\omega}$
7035+889$\tilde{\omega}$
+
730+4631$\tilde{\omega}$
5523+9090$\tilde{\omega}$
5958+4677$\tilde{\omega}$
9647+7451$\tilde{\omega}$
5502+3675$\tilde{\omega}$
9684+1334$\tilde{\omega}$
7469+4943$\tilde{\omega}$
1586+112$\tilde{\omega}$
5958+4677$\tilde{\omega}$
832+6968$\tilde{\omega}$


8984
8302
9717
3689+917$\tilde{\omega}$
5523+9090$\tilde{\omega}$
9647+7451$\tilde{\omega}$
8813+9118$\tilde{\omega}$
7035+889$\tilde{\omega}$
4535+2556$\tilde{\omega}$
5305+5330$\tilde{\omega}$
730+4631$\tilde{\omega}$
7469+4943$\tilde{\omega}$
5502+3675$\tilde{\omega}$
2845+6332$\tilde{\omega}$
7348+5064$\tilde{\omega}$
9992+5376$\tilde{\omega}$
5958+4677$\tilde{\omega}$
1816
7644+5565$\tilde{\omega}$
3424+9266$\tilde{\omega}$
2345+8673$\tilde{\omega}$
9684+1334$\tilde{\omega}$
1942+741$\tilde{\omega}$
8767+4442$\tilde{\omega}$
9181
4761+3039$\tilde{\omega}$
6987+6720$\tilde{\omega}$
413+3287$\tilde{\omega}$
832+6968$\tilde{\omega}$
1586+112$\tilde{\omega}$
1810+9895$\tilde{\omega}$
7244
Positive direction 13
Positive direction 31
Positive direction 43

OSIDH PROTOCOL - AN EXAMPLE

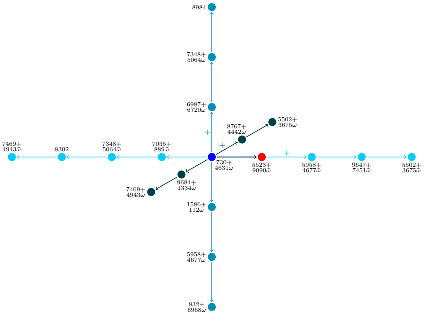
Bob secret key: $\mathfrak{l}_1^3\mathfrak{l}_2\mathfrak{l}_3^2$

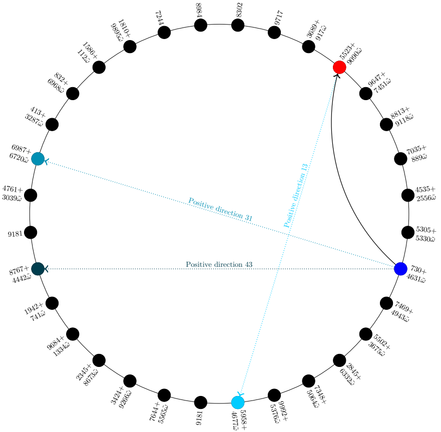

8984
7348+ 5064$\tilde{\omega}$
6987+ 6720$\tilde{\omega}$
+
8767+ 4442$\tilde{\omega}$
5502+ 3675$\tilde{\omega}$
+
+
7469+ 4943$\tilde{\omega}$
8302
7348+ 5064$\tilde{\omega}$
7035+ 889$\tilde{\omega}$
730+ 4631$\tilde{\omega}$
5523+ 9090$\tilde{\omega}$
5958+ 4677$\tilde{\omega}$
9647+ 7451$\tilde{\omega}$
5502+ 3675$\tilde{\omega}$
9684+ 1334$\tilde{\omega}$
7469+ 4943$\tilde{\omega}$
1586+ 112$\tilde{\omega}$
5958+ 4677$\tilde{\omega}$
832+ 6968$\tilde{\omega}$


8984
8302
9717
3689+ 917$\tilde{\omega}$
5523+ 9090$\tilde{\omega}$
9647+ 7451$\tilde{\omega}$
8813+ 9118$\tilde{\omega}$
7035+ 889$\tilde{\omega}$
4535+ 2556$\tilde{\omega}$
5305+ 5330$\tilde{\omega}$
730+ 4631$\tilde{\omega}$
7469+ 4943$\tilde{\omega}$
5502+ 3675$\tilde{\omega}$
2845+ 6332$\tilde{\omega}$
7348+ 5064$\tilde{\omega}$
9992+ 5376$\tilde{\omega}$
5958+ 4677$\tilde{\omega}$
9181
7644+ 5565$\tilde{\omega}$
3424+ 9266$\tilde{\omega}$
2345+ 8673$\tilde{\omega}$
9684+ 1334$\tilde{\omega}$
1942+ 741$\tilde{\omega}$
8767+ 4442$\tilde{\omega}$
9181
4761+ 3039$\tilde{\omega}$
6987+ 6720$\tilde{\omega}$
413+ 3287$\tilde{\omega}$
832+ 6968$\tilde{\omega}$
1586+ 112$\tilde{\omega}$
1810+ 9895$\tilde{\omega}$
7244
Positive direction 31
Positive direction 43

OSIDH PROTOCOL - AN EXAMPLE

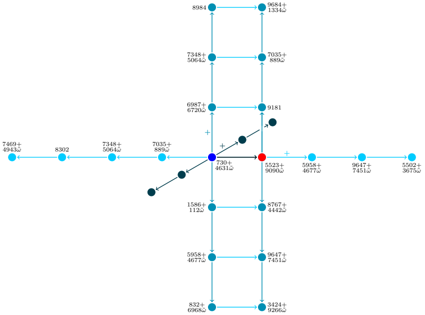
Bob secret key: $\mathfrak{l}_1^3 \mathfrak{l}_2 \mathfrak{l}_3^2$

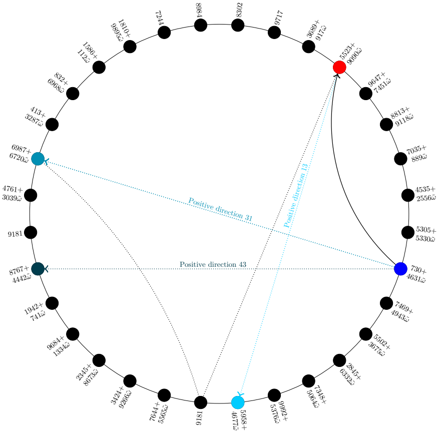




OSIDH PROTOCOL - AN EXAMPLE

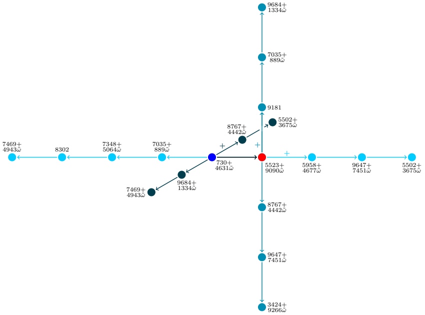
Bob secret key: $\mathfrak{l}_1^3\mathfrak{l}_2\mathfrak{l}_3^2$


8984
9684+ 1334$\tilde{\omega}$
7348+ 5064$\tilde{\omega}$
7035+ 889$\tilde{\omega}$
6987+ 6720$\tilde{\omega}$
9181
+
7469+ 4943$\tilde{\omega}$
8302
7348+ 5064$\tilde{\omega}$
7035+ 889$\tilde{\omega}$
+
730+ 4631$\tilde{\omega}$
5523+ 9090$\tilde{\omega}$
+
5958+ 4677$\tilde{\omega}$
9647+ 7451$\tilde{\omega}$
5502+ 3675$\tilde{\omega}$
1586+ 112$\tilde{\omega}$
8767+ 4442$\tilde{\omega}$
5958+ 4677$\tilde{\omega}$
9647+ 7451$\tilde{\omega}$
832+ 6968$\tilde{\omega}$
3424+ 9266$\tilde{\omega}$

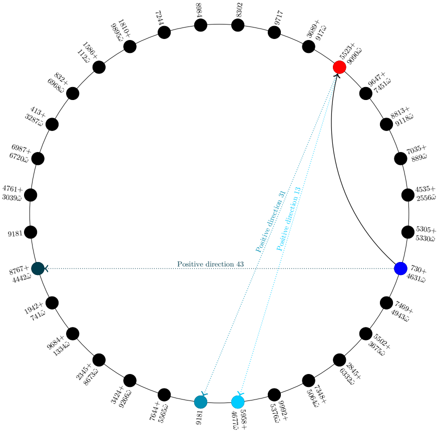

8984
8302
9717
7244
1810+ 9895$\tilde{\omega}$
3689+ 917$\tilde{\omega}$
1586+ 112$\tilde{\omega}$
5523+ 9090$\tilde{\omega}$
832+ 6968$\tilde{\omega}$
9647+ 7451$\tilde{\omega}$
413+ 3287$\tilde{\omega}$
8813+ 9118$\tilde{\omega}$
6987+ 6720$\tilde{\omega}$
7035+ 889$\tilde{\omega}$
4761+ 3039$\tilde{\omega}$
4535+ 2556$\tilde{\omega}$
Positive direction 31
Positive direction 13
9181
5305+ 5330$\tilde{\omega}$
8767+ 4442$\tilde{\omega}$
Positive direction 43
730+ 4631$\tilde{\omega}$
1942+ 741$\tilde{\omega}$
7469+ 4943$\tilde{\omega}$
9684+ 1334$\tilde{\omega}$
5502+ 3675$\tilde{\omega}$
2345+ 8673$\tilde{\omega}$
2845+ 6332$\tilde{\omega}$
3424+ 9266$\tilde{\omega}$
7348+ 5064$\tilde{\omega}$
7644+ 5565$\tilde{\omega}$
9181
5958+ 4677$\tilde{\omega}$
9992+ 5376$\tilde{\omega}$

OSIDH PROTOCOL - AN EXAMPLE

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



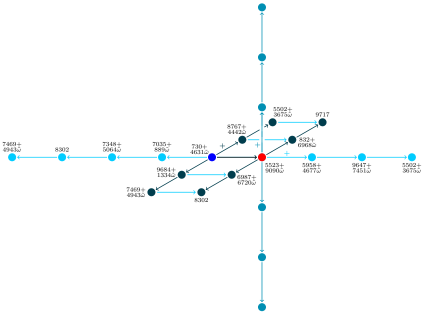
$9684+1334\tilde{\omega}$
$7035+889\tilde{\omega}$
9181
$5502+3675\tilde{\omega}$
$8767+4442\tilde{\omega}$
+
+
+
$7469+4943\tilde{\omega}$
8302
$7348+5064\tilde{\omega}$
$7035+889\tilde{\omega}$
$730+4631\tilde{\omega}$
$5523+9090\tilde{\omega}$
$5958+4677\tilde{\omega}$
$9647+7451\tilde{\omega}$
$5502+3675\tilde{\omega}$
$9684+1334\tilde{\omega}$
$7469+4943\tilde{\omega}$
$8767+4442\tilde{\omega}$
$9647+7451\tilde{\omega}$
$3424+9266\tilde{\omega}$

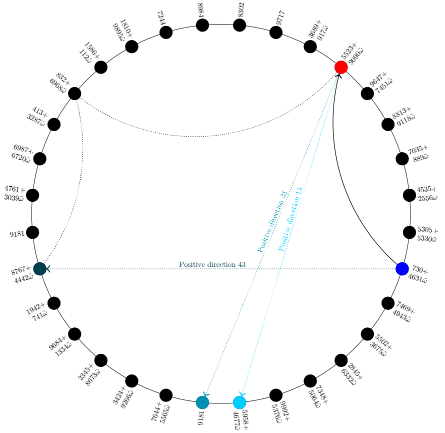


8984
8302
9717
$3689+917\tilde{\omega}$
$5523+9090\tilde{\omega}$
$9647+7451\tilde{\omega}$
$8813+9118\tilde{\omega}$
$7035+889\tilde{\omega}$
$4535+2556\tilde{\omega}$
$5305+5330\tilde{\omega}$
$730+4631\tilde{\omega}$
$7469+4943\tilde{\omega}$
$5502+3675\tilde{\omega}$
$2845+6332\tilde{\omega}$
$7348+5064\tilde{\omega}$
$9992+5376\tilde{\omega}$
$5958+4677\tilde{\omega}$
9181
$7644+5565\tilde{\omega}$
$3424+9266\tilde{\omega}$
$2345+8673\tilde{\omega}$
$9684+1334\tilde{\omega}$
$1942+741\tilde{\omega}$
$8767+4442\tilde{\omega}$
9181
$4761+3039\tilde{\omega}$
$6987+6720\tilde{\omega}$
$413+3287\tilde{\omega}$
$832+6968\tilde{\omega}$
$1586+112\tilde{\omega}$
$1810+9895\tilde{\omega}$
7244
Positive direction 31
Positive direction 13
Positive direction 43

OSIDH PROTOCOL - AN EXAMPLE

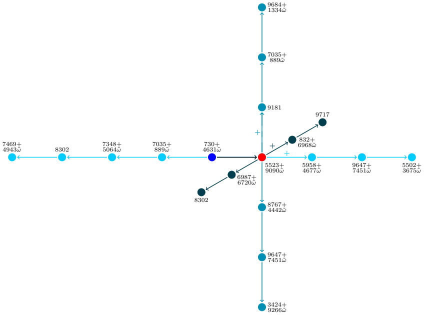
Bob secret key: $\mathfrak{l}_1^3\mathfrak{l}_2\mathfrak{l}_3^2$

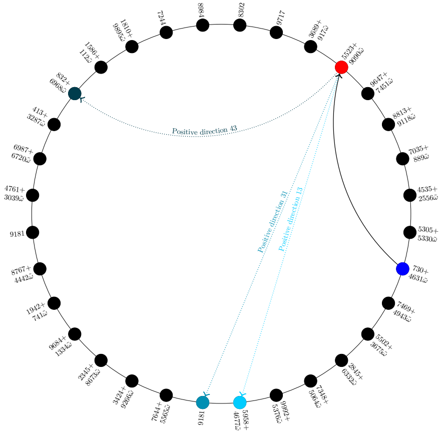




OSIDH PROTOCOL - AN EXAMPLE

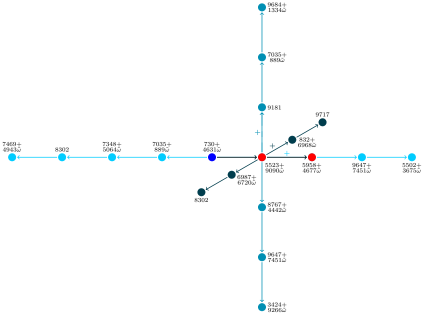
Bob secret key: $\mathfrak{l}_1^3\mathfrak{l}_2\mathfrak{l}_3^2$

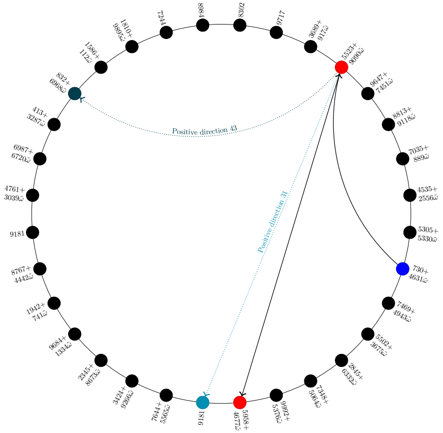




OSIDH PROTOCOL - AN EXAMPLE

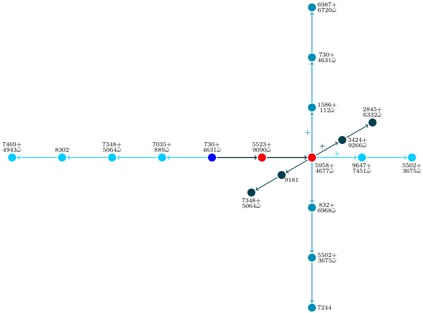
Bob secret key: $\mathfrak{l}_1^3 \mathfrak{l}_2 \mathfrak{l}_3^2$

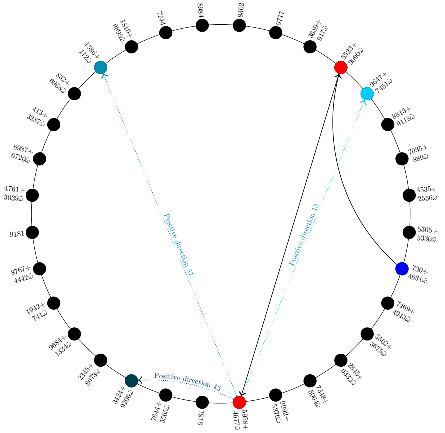




OSIDH PROTOCOL - AN EXAMPLE

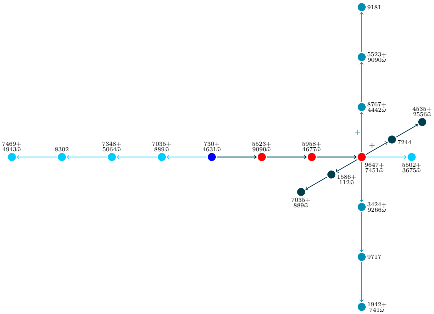
Bob secret key: $\mathfrak{l}_1^3\mathfrak{l}_2\mathfrak{l}_3^2$

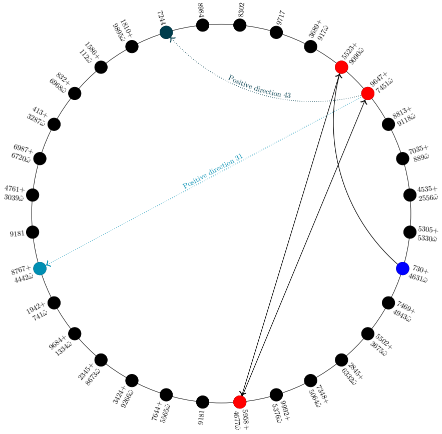




OSIDH PROTOCOL - AN EXAMPLE

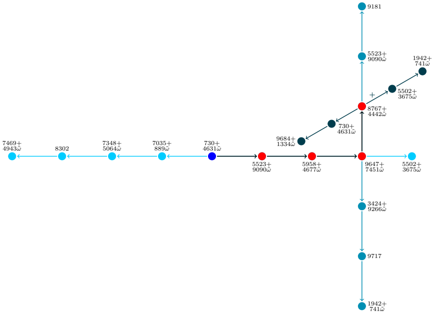
Bob secret key: $\mathfrak{l}_1^3\mathfrak{l}_2\mathfrak{l}_3^2$

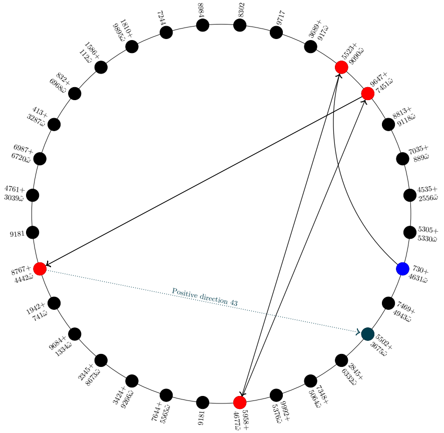




OSIDH PROTOCOL - AN EXAMPLE

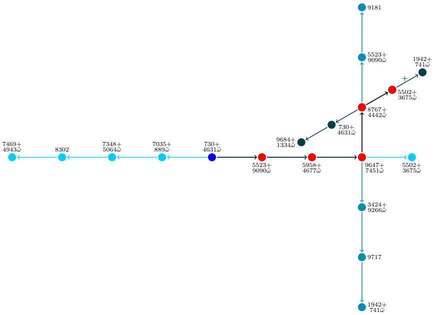
Bob secret key: $\mathfrak{l}_1^3\mathfrak{l}_2\mathfrak{l}_3^2$

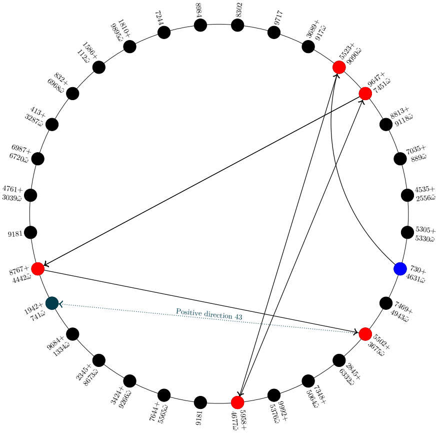




OSIDH PROTOCOL - AN EXAMPLE

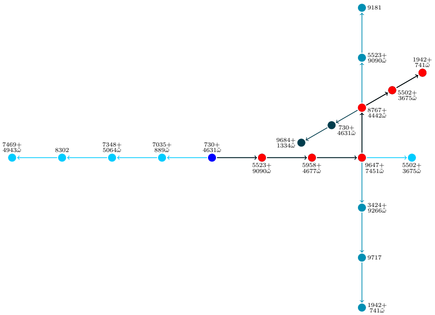
Bob secret key: $\mathfrak{l}_1^3\mathfrak{l}_2\mathfrak{l}_3^2$

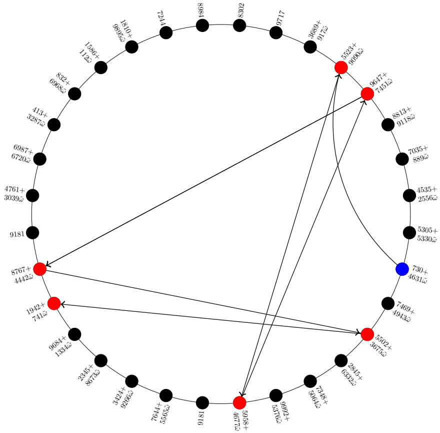




OSIDH PROTOCOL - AN EXAMPLE

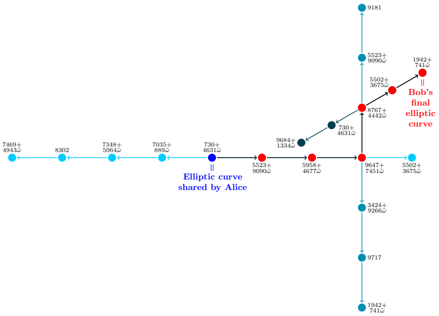
Bob secret key: $\mathfrak{l}_1^3\mathfrak{l}_2\mathfrak{l}_3^2$

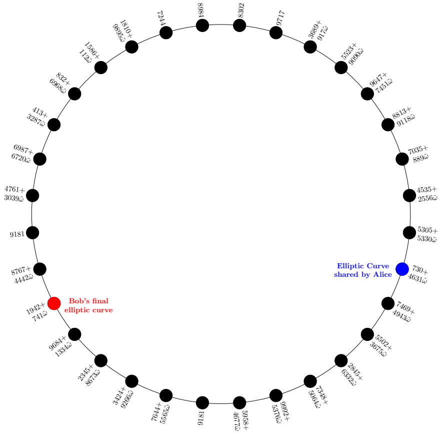




OSIDH PROTOCOL - AN EXAMPLE

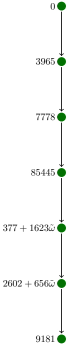
Bob secret key: $\mathfrak{l}_1^3\mathfrak{l}_2\mathfrak{l}_3^2$

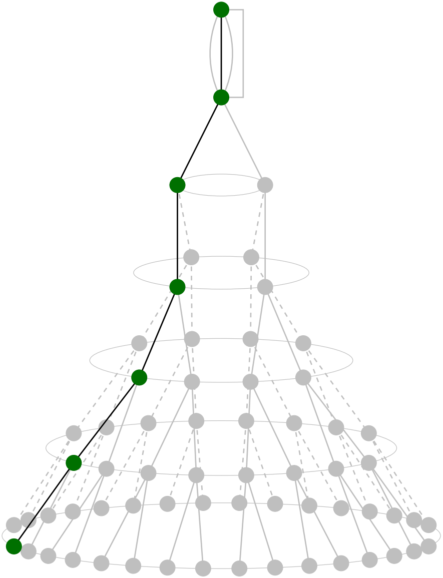

9181
5523+ $9090\tilde{\omega}$
1942+ $741\tilde{\omega}$
5502+ $3675\tilde{\omega}$
||
Bob's final elliptic curve
8767+ $4442\tilde{\omega}$
730+ $4631\tilde{\omega}$
9684+ $1334\tilde{\omega}$
7469+ $4943\tilde{\omega}$
8302
7348+ $5064\tilde{\omega}$
7035+ $889\tilde{\omega}$
730+ $4631\tilde{\omega}$
||
Elliptic curve shared by Alice
5523+ $9090\tilde{\omega}$
5958+ $4677\tilde{\omega}$
9647+ $7451\tilde{\omega}$
5502+ $3675\tilde{\omega}$
3424+ $9266\tilde{\omega}$
9717
1942+ $741\tilde{\omega}$


8984
8302
9717
3689+ $917\tilde{\omega}$
5523+ $9090\tilde{\omega}$
9647+ $7451\tilde{\omega}$
8813+ $9118\tilde{\omega}$
7035+ $889\tilde{\omega}$
4535+ $2556\tilde{\omega}$
5305+ $5330\tilde{\omega}$
Elliptic Curve shared by Alice
730+ $4631\tilde{\omega}$
7469+ $4943\tilde{\omega}$
5502+ $3675\tilde{\omega}$
2845+ $6332\tilde{\omega}$
7348+ $5064\tilde{\omega}$
9992+ $5376\tilde{\omega}$
5958+ $4677\tilde{\omega}$
9181
7644+ $5565\tilde{\omega}$
3424+ $9266\tilde{\omega}$
2345+ $8673\tilde{\omega}$
9684+ $1334\tilde{\omega}$
1942+ $741\tilde{\omega}$
Bob's final elliptic curve
8767+ $4442\tilde{\omega}$
9181
4761+ $3039\tilde{\omega}$
6987+ $6720\tilde{\omega}$
413+ $3287\tilde{\omega}$
832+ $6968\tilde{\omega}$
1586+ $112\tilde{\omega}$
1810+ $9895\tilde{\omega}$
7244

OSIDH PROTOCOL - AN EXAMPLE

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

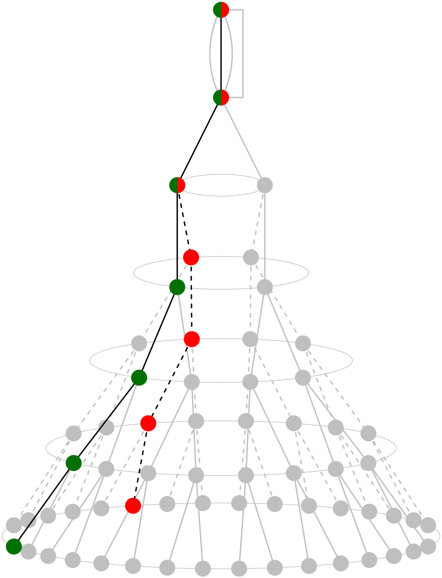




OSIDH PROTOCOL - AN EXAMPLE

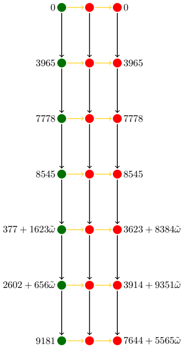
Bob secret key: $\mathfrak{l}_1^3\mathfrak{l}_2\mathfrak{l}_3^2$

$$\begin{tikzcd}
0 \arrow[r] \arrow[d] & 0 \arrow[d] \\
3965 \arrow[r] \arrow[d] & 3965 \arrow[d] \\
7778 \arrow[r] \arrow[d] & 7778 \arrow[d] \\
8545 \arrow[r] \arrow[d] & 8789 \arrow[d] \\
377+1623\tilde{\omega} \arrow[r] \arrow[d] & 9350 \arrow[d] \\
2602+656\tilde{\omega} \arrow[r] \arrow[d] & 3063 \arrow[d] \\
9181 \arrow[r] & 1810+9895\tilde{\omega}
\end{tikzcd}$$

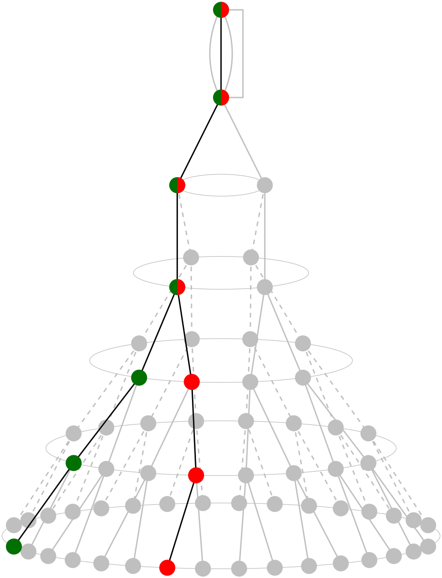


OSIDH PROTOCOL - AN EXAMPLE

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

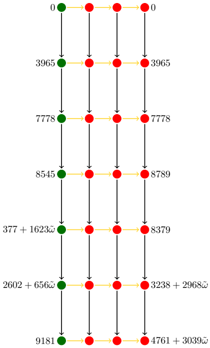


0
0
3965
3965
7778
7778
8545
8545
$377 + 1623\tilde{\omega}$
$3623 + 8384\tilde{\omega}$
$2602 + 656\tilde{\omega}$
$3914 + 9351\tilde{\omega}$
9181
$7644 + 5565\tilde{\omega}$

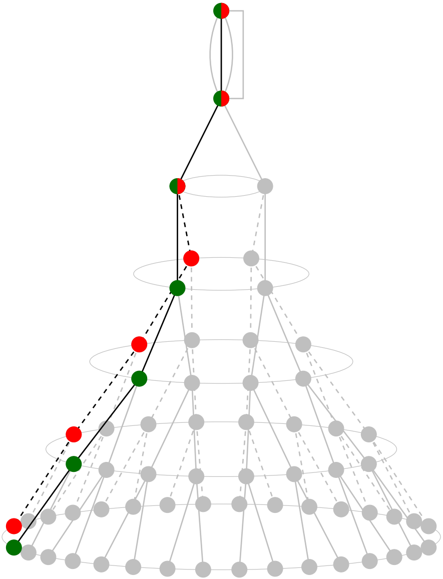


OSIDH PROTOCOL - AN EXAMPLE

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

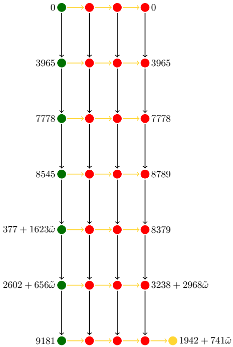


0
0
3965
3965
7778
7778
8545
8789
$377 + 1623\tilde{\omega}$
8379
$2602 + 656\tilde{\omega}$
$3238 + 2968\tilde{\omega}$
9181
$4761 + 3039\tilde{\omega}$

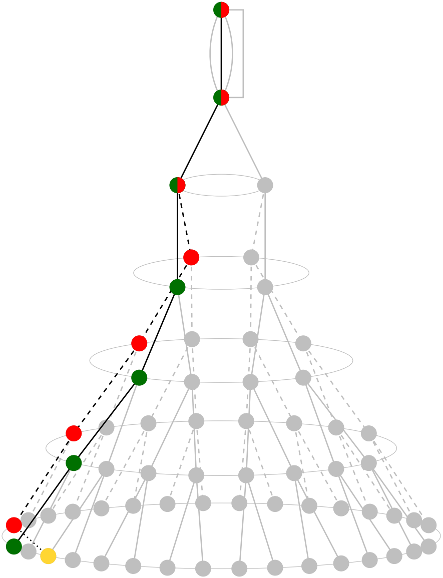


OSIDH PROTOCOL - AN EXAMPLE

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

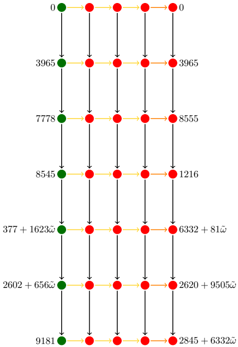


0
0
3965
3965
7778
7778
8545
8789
$377 + 1623\tilde{\omega}$
8379
$2602 + 656\tilde{\omega}$
$3238 + 2968\tilde{\omega}$
9181
$1942 + 741\tilde{\omega}$

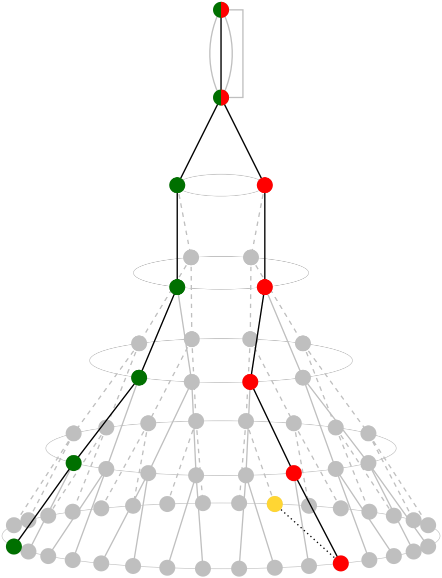


OSIDH PROTOCOL - AN EXAMPLE

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

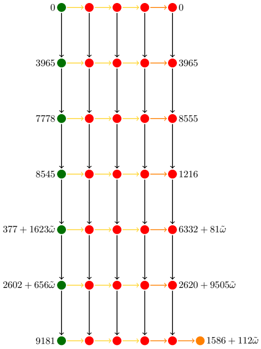


0
0
3965
3965
7778
8555
8545
1216
$377 + 1623\tilde{\omega}$
$6332 + 81\tilde{\omega}$
$2602 + 656\tilde{\omega}$
$2620 + 9505\tilde{\omega}$
9181
$2845 + 6332\tilde{\omega}$

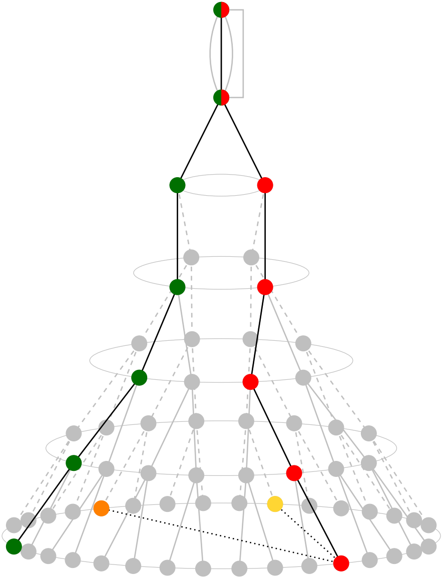


OSIDH PROTOCOL - AN EXAMPLE

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

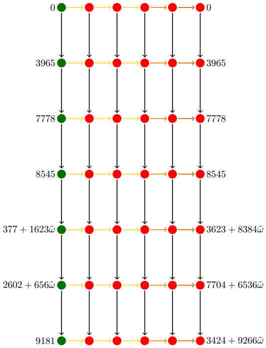


0
0
3965
3965
7778
8555
8545
1216
$377 + 1623\tilde{\omega}$
$6332 + 81\tilde{\omega}$
$2602 + 656\tilde{\omega}$
$2620 + 9505\tilde{\omega}$
9181
$1586 + 112\tilde{\omega}$

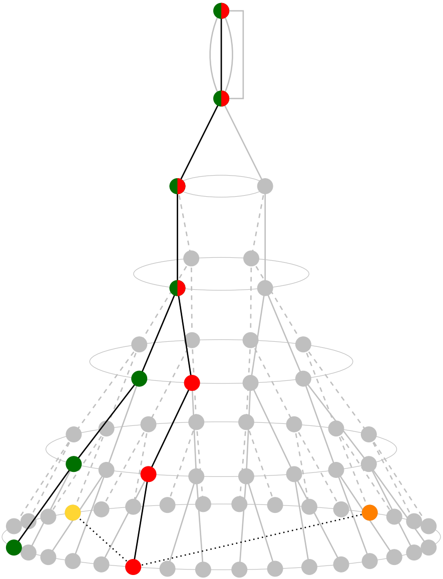


OSIDH PROTOCOL - AN EXAMPLE

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

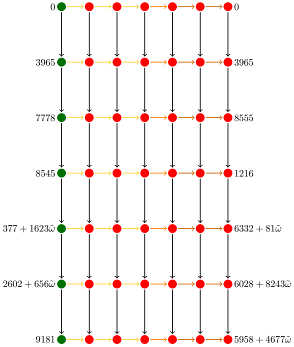


0
0
3965
3965
7778
7778
8545
8545
$377 + 1623\tilde{\omega}$
$3623 + 8384\tilde{\omega}$
$2602 + 656\tilde{\omega}$
$7704 + 6536\tilde{\omega}$
9181
$3424 + 9266\tilde{\omega}$

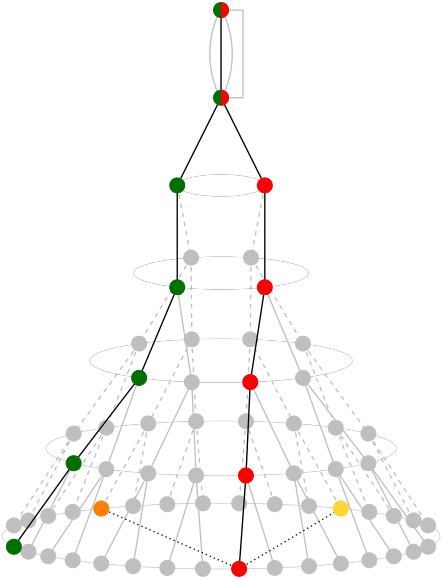


OSIDH PROTOCOL - AN EXAMPLE

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

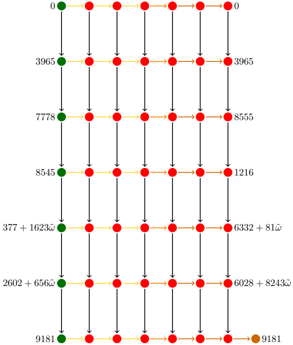


0
0
3965
3965
7778
8555
8545
1216
$377 + 1623\tilde{\omega}$
$6332 + 81\tilde{\omega}$
$2602 + 656\tilde{\omega}$
$6028 + 8243\tilde{\omega}$
9181
$5958 + 4677\tilde{\omega}$

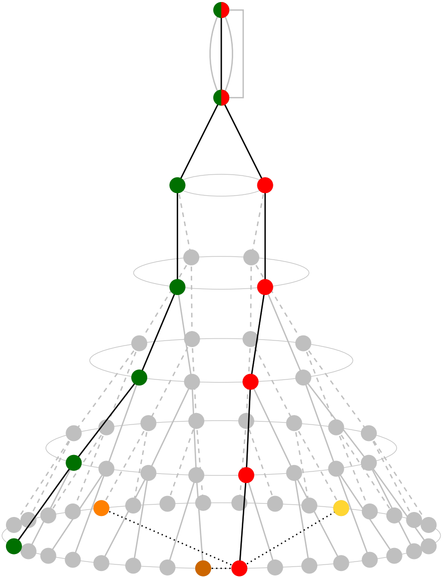


OSIDH PROTOCOL - AN EXAMPLE

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

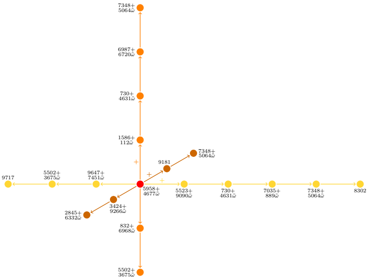


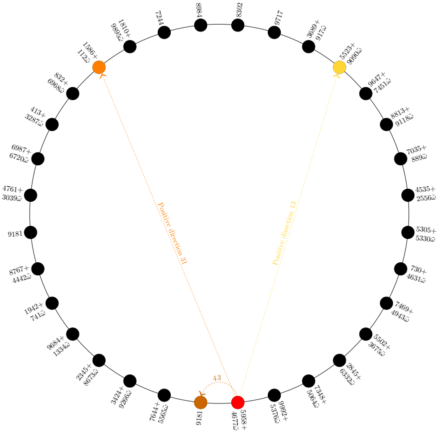
0
0
3965
3965
7778
8555
8545
1216
$377 + 1623\tilde{\omega}$
$6332 + 81\tilde{\omega}$
$2602 + 656\tilde{\omega}$
$6028 + 8243\tilde{\omega}$
9181
9181



OSIDH PROTOCOL - AN EXAMPLE

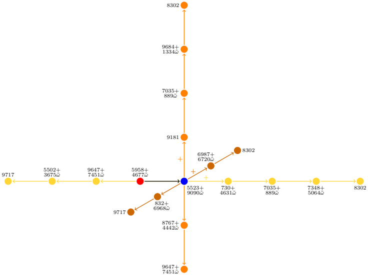
Alice secret key: $\mathfrak{l}_1^5\mathfrak{l}_2^3\mathfrak{l}_3^2$



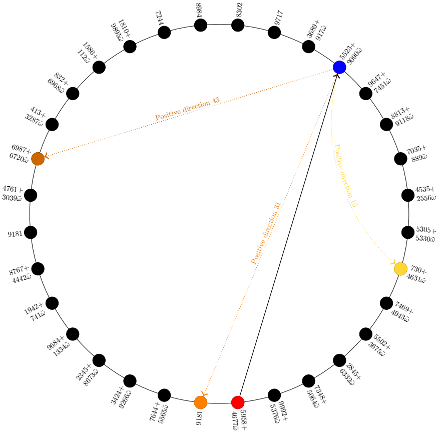


OSIDH PROTOCOL - AN EXAMPLE

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



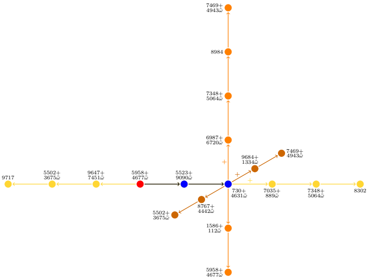
8302
9684+ 1334$\tilde{\omega}$
7035+ 889$\tilde{\omega}$
9181
6987+ 6720$\tilde{\omega}$
8302
+
+
+
9717
5502+ 3675$\tilde{\omega}$
9647+ 7451$\tilde{\omega}$
5958+ 4677$\tilde{\omega}$
5523+ 9090$\tilde{\omega}$
730+ 4631$\tilde{\omega}$
7035+ 889$\tilde{\omega}$
7348+ 5064$\tilde{\omega}$
8302
832+ 6968$\tilde{\omega}$
9717
8767+ 4442$\tilde{\omega}$
9647+ 7451$\tilde{\omega}$

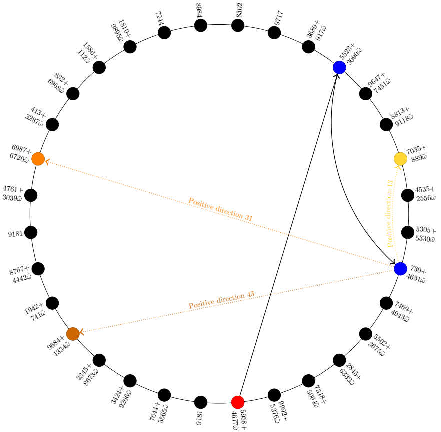


8984
8302
9717
3689+ 917$\tilde{\omega}$
5523+ 9090$\tilde{\omega}$
9647+ 7451$\tilde{\omega}$
8813+ 9118$\tilde{\omega}$
7035+ 889$\tilde{\omega}$
4535+ 2556$\tilde{\omega}$
5305+ 5330$\tilde{\omega}$
730+ 4631$\tilde{\omega}$
7469+ 4943$\tilde{\omega}$
5502+ 3675$\tilde{\omega}$
2845+ 6332$\tilde{\omega}$
7348+ 5064$\tilde{\omega}$
9992+ 5376$\tilde{\omega}$
5958+ 4677$\tilde{\omega}$
9181
7644+ 5565$\tilde{\omega}$
3424+ 9266$\tilde{\omega}$
2345+ 8673$\tilde{\omega}$
9684+ 1334$\tilde{\omega}$
1942+ 741$\tilde{\omega}$
8767+ 4442$\tilde{\omega}$
9181
4761+ 3039$\tilde{\omega}$
6987+ 6720$\tilde{\omega}$
413+ 3287$\tilde{\omega}$
832+ 6968$\tilde{\omega}$
1586+ 112$\tilde{\omega}$
1810+ 9895$\tilde{\omega}$
7244
Positive direction 43
Positive direction 31
Positive direction 13

OSIDH PROTOCOL - AN EXAMPLE

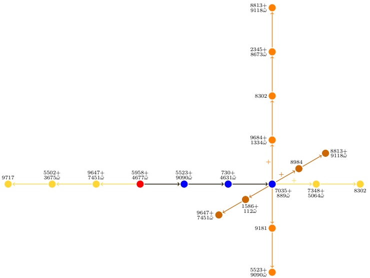
Alice secret key: $\mathfrak{l}_1^5\mathfrak{l}_2^3\mathfrak{l}_3^2$

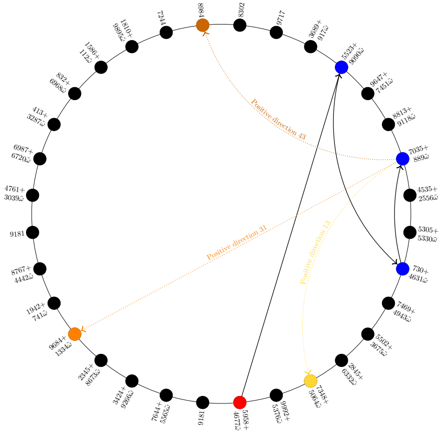




OSIDH PROTOCOL - AN EXAMPLE

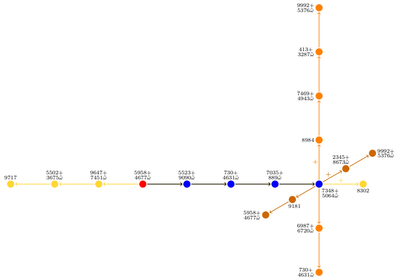
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$

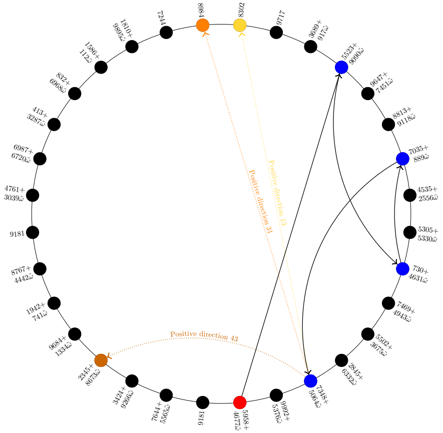




OSIDH PROTOCOL - AN EXAMPLE

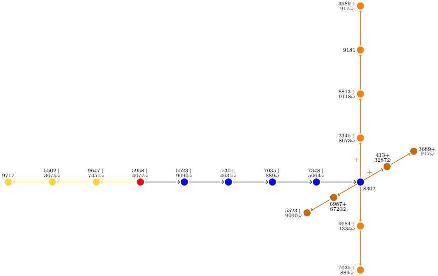
Alice secret key: $\mathfrak{l}_1^5\,\mathfrak{l}_2^3\,\mathfrak{l}_3^2$

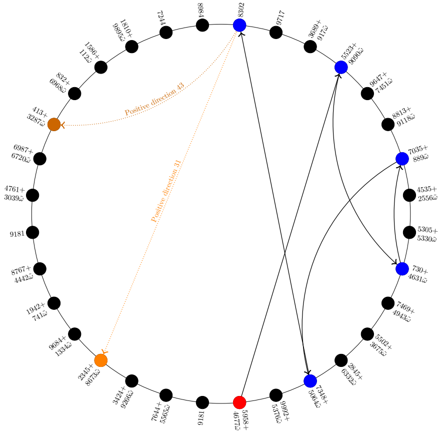




OSIDH PROTOCOL - AN EXAMPLE

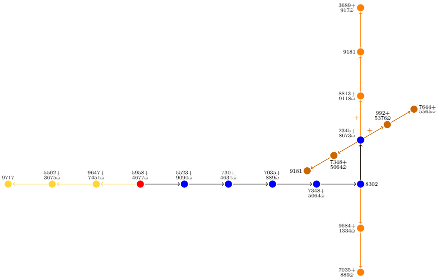
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$

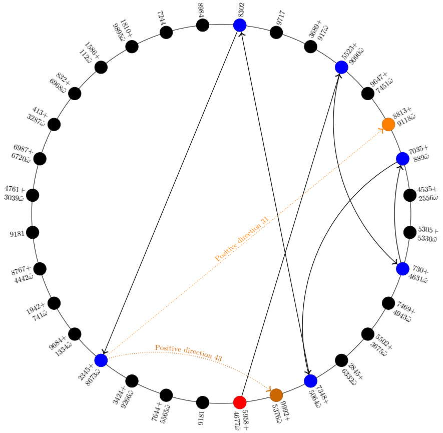




OSIDH PROTOCOL - AN EXAMPLE

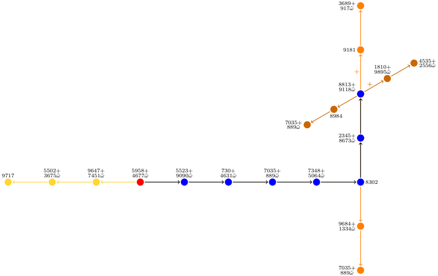
Alice secret key: $\mathfrak{l}_1^5\mathfrak{l}_2^3\mathfrak{l}_3^2$

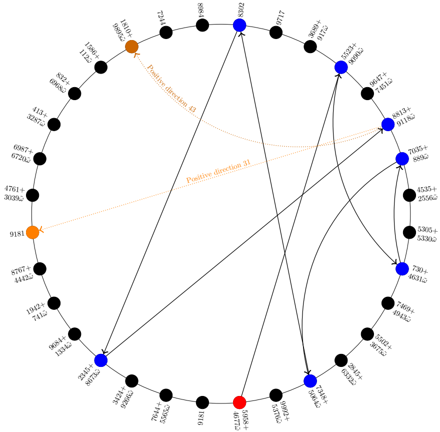




OSIDH PROTOCOL - AN EXAMPLE

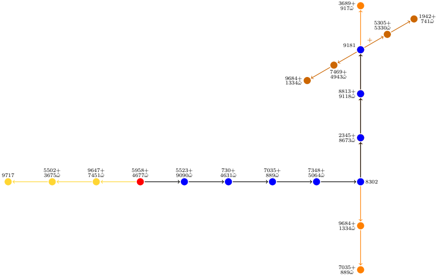
Alice secret key: $\mathfrak{l}_1^5 \mathfrak{l}_2^3 \mathfrak{l}_3^2$

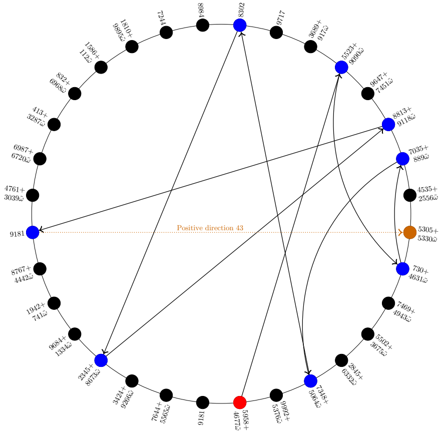




OSIDH PROTOCOL - AN EXAMPLE

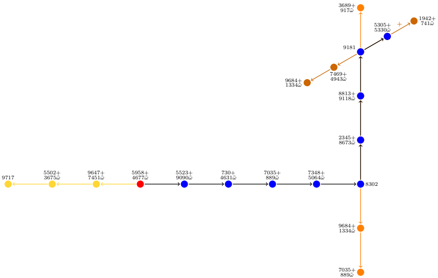
Alice secret key: $\mathfrak{l}_1^5\mathfrak{l}_2^3\mathfrak{l}_3^2$

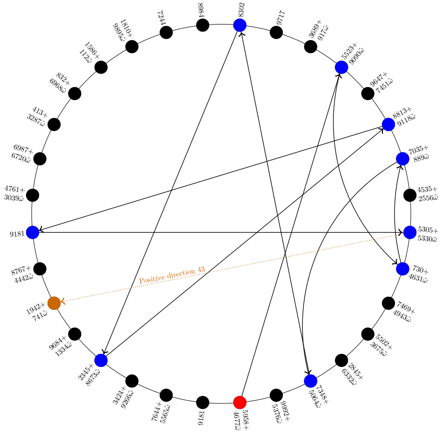




OSIDH PROTOCOL - AN EXAMPLE

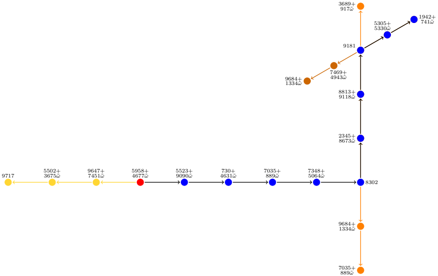
Alice secret key: $\mathfrak{l}_1^5\mathfrak{l}_2^3\mathfrak{l}_3^2$

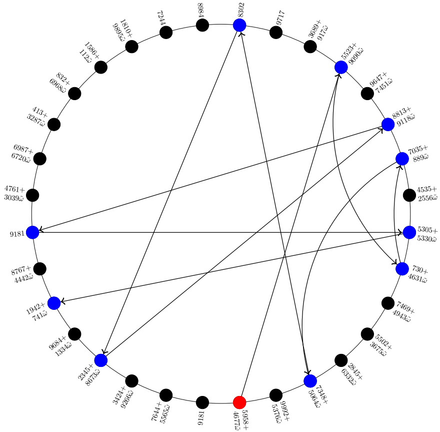




OSIDH PROTOCOL - AN EXAMPLE

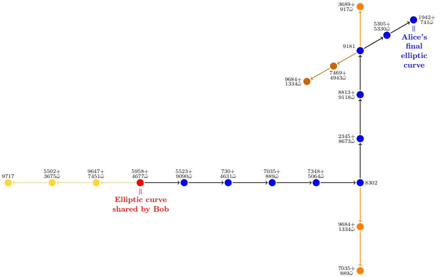
Alice secret key: $\mathfrak{l}_1^5\mathfrak{l}_2^3\mathfrak{l}_3^2$



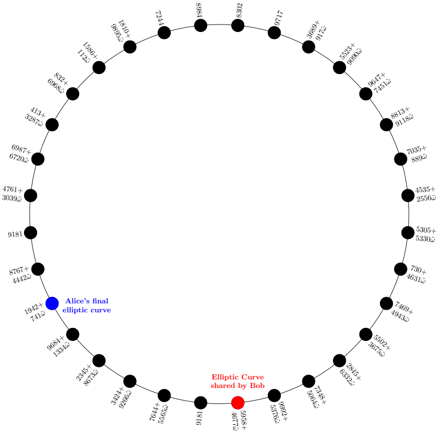


OSIDH PROTOCOL - AN EXAMPLE

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

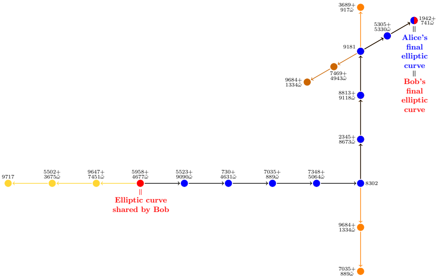


$3689+917\tilde{\omega}$
$5305+5330\tilde{\omega}$
$1942+741\tilde{\omega}$
||
Alice's final elliptic curve
9181
$7469+4943\tilde{\omega}$
$9684+1334\tilde{\omega}$
$8813+9118\tilde{\omega}$
$2345+8673\tilde{\omega}$
9717
$5502+3675\tilde{\omega}$
$9647+7451\tilde{\omega}$
$5958+4677\tilde{\omega}$
||
Elliptic curve shared by Bob
$5523+9090\tilde{\omega}$
$730+4631\tilde{\omega}$
$7035+889\tilde{\omega}$
$7348+5064\tilde{\omega}$
8302
$9684+1334\tilde{\omega}$
$7035+889\tilde{\omega}$



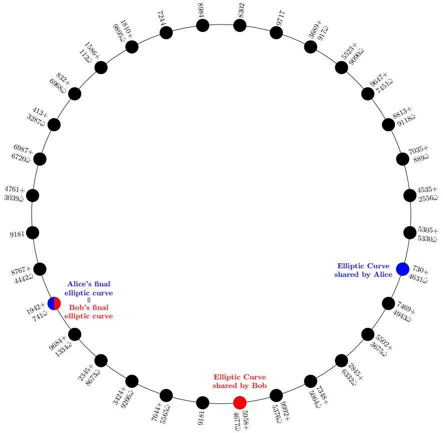
8984
8302
9717
$3689+917\tilde{\omega}$
$5523+9090\tilde{\omega}$
$9647+7451\tilde{\omega}$
$8813+9118\tilde{\omega}$
$7035+889\tilde{\omega}$
$4535+2556\tilde{\omega}$
$5305+5330\tilde{\omega}$
$730+4631\tilde{\omega}$
$7469+4943\tilde{\omega}$
$5502+3675\tilde{\omega}$
$2845+6332\tilde{\omega}$
$7348+5064\tilde{\omega}$
$9992+5376\tilde{\omega}$
Elliptic Curve shared by Bob
$5958+4677\tilde{\omega}$
9181
$7644+5565\tilde{\omega}$
$3424+9266\tilde{\omega}$
$2345+8673\tilde{\omega}$
$9684+1334\tilde{\omega}$
$1942+741\tilde{\omega}$
Alice's final elliptic curve
$8767+4442\tilde{\omega}$
9181
$4761+3039\tilde{\omega}$
$6987+6720\tilde{\omega}$
$413+3287\tilde{\omega}$
$832+6968\tilde{\omega}$
$1586+112\tilde{\omega}$
$1810+9895\tilde{\omega}$
7244

OSIDH PROTOCOL - AN EXAMPLE



|| Alice's final elliptic curve || Bob's final elliptic curve

|| Elliptic curve shared by Bob



Elliptic Curve shared by Alice

Elliptic Curve shared by Bob

Alice's final elliptic curve || Bob's final elliptic curve

CLASSICAL HARD PROBLEMS

Endomorphism ring problem

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

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

Endomorphism ring transfer problem

Given an isogeny chain

$$E_0 \longrightarrow E_1 \longrightarrow \dots \longrightarrow E_n$$

and $\text{End}(E_0)$, determine $\text{End}(E_n)$.

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 $\mathsf{End}(E)$ and a collection of compatible $(\mathcal{O}, \mathfrak{q}^n)$-orientations of E for $(\mathfrak{q}, n) \in S$, determine

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

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

$$\begin{tikzcd}
 & \mathsf{disc} : \mathcal{O}_{\mathfrak{B}}/\mathbb{Z} \arrow[r] \arrow[dl, phantom, "/\!/"] & \mathbb{Z} \\
\bigwedge^2 (\mathcal{O}_{\mathfrak{B}}) \supseteq \mathbb{Z} \wedge \mathcal{O}_{\mathfrak{B}} & \alpha \arrow[r, mapsto] & |\mathsf{disc}(\alpha)| = |\mathsf{disc}\,(\mathbb{Z}\,[\alpha])\,|
\end{tikzcd}$$

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

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

(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

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

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

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., $n \sim \mathtt{log}_\ell(p)$.

- $\#SS^{pr}_{\mathcal{O}}(p) = h(\mathcal{O}_n) =$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

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

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 - PRIVATE WALKS EXPONENTS

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 $I_j = \left[-m_j, m_j\right]$, defining ψ_A with kernel $E\left[\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}\right]$.
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 $(I_1 \times \ldots \times I_r) \cap \mathsf{ker}\left(\mathbb{Z}^r \to \mathcal{C}\ell(\mathcal{O})\right)$

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

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

for fixed $m = m_j$ this yields

$$n > r\mathsf{log}_\ell\left(2m+1\right) > \lambda\mathsf{log}_\ell(p)$$

Future directions:

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

Future directions:

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

MERCI POUR VOTRE ATTENTION