Orienting Supersingular Isogeny Graphs

Leonardo **Colò** & David **Kohel**

Institut de Mathématiques de Marseille

Journées Nationales de Calcul Formel 2019
CIRM, Luminy, 7 February 2019

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

$$E : Y^2Z = X^3 + aXZ^2 + bZ^3 \quad \text{where } a, b \in k \text{ such that } 4a^3 + 27b^2 \neq 0$$

- We have a special point defined on E (point at infinity): $O = (0 : 1 : 0)$.
- Affine equation of E: $y^2 = x^3 + ax + b$.
- The set of k-rational points on E is a group.
  - if E is defined over an algebraically closed field $\overline{k}$ of characteristic p, then

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

- 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 and E' are isomorphic over $\overline{k}$ if and only if $j(E) = j(E')$.

- An isogeny $\phi : E_1 \to E_2$ of elliptic curves is a map that is also a surjective group homomorphism.
- Among isogenies, we have the multiplication by n map ($[n] : E \to E$) and the Frobenius morphism (k finite field): $\pi : (X : Y : Z) \to (X^p : Y^p : Z^p)$
- Tate's Theorem: two elliptic curves E and F defined over a finite field k are isogenous over k if and only if $\#E(k) = \#F(k)$.
- The degree of an isogeny ϕ is $\deg \phi = [k(E) : \phi^* k(F)]$.
- Given an isogeny $\phi : E \to F$, there is a unique isogeny $\hat{\phi} : F \to E$ such that

$$\phi \circ \hat{\phi} = [\deg \phi]_F \qquad \hat{\phi} \circ \phi = [\deg \phi]_E$$

  $\hat{\phi}$ is called dual isogeny.
- If E is an elliptic curve defined over a finite field k of characteristic p, there are $\ell + 1$ distinct isogenies of degree $\ell \neq p$ with domain E defined over $\overline{k}$.

Definition

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

Theorem (Deuring)

Let E/k be an elliptic curve over a finite field k of characteristic $p > 0$. $\mathrm{End}(E)$ 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.

Theorem (Hasse)

Let E/k be 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.

Theorem (Serre-Tate)

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

Definition

An isogeny graph is a graph whose vertices are j-invariants of elliptic curves (elliptic curves up to isomorphism) and whose edges are isogenies between them.

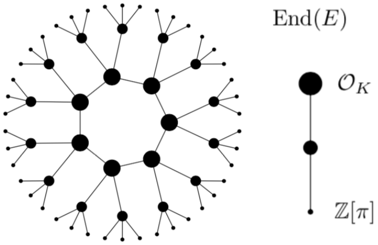
Theorem (Serre-Tate)

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

Definition

An isogeny graph is a graph whose vertices are j-invariants of elliptic curves (elliptic curves up to isomorphism) and whose edges are isogenies between them.

In the ordinary case, the isogeny graph has a precise structure (volcanoes):



Theorem (Serre-Tate)

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

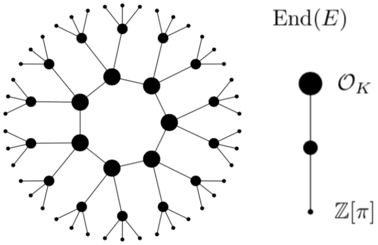
Definition

An isogeny graph is a graph whose vertices are j-invariants of elliptic curves (elliptic curves up to isomorphism) and whose edges are isogenies between them.

Let $\mathrm{End}(E) = \mathcal{O} \subseteq \mathbb{Q}(\sqrt{D})$. The class group of $\mathcal{O}$ is $\mathrm{Cl}(\mathcal{O})$ (finite abelian group) acts on the set of elliptic curves with endomorphism ring $\mathcal{O}$:

$$E \longrightarrow E/E[\mathfrak{a}]$$

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



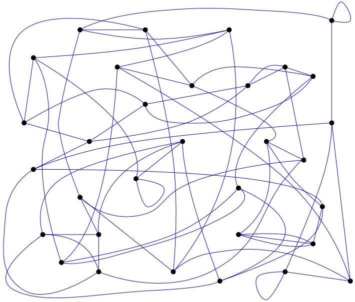
Theorem (Serre-Tate)

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

Definition

An isogeny graph is a graph whose vertices are j-invariants of elliptic curves (elliptic curves up to isomorphism) and whose edges are isogenies between them.

The supresingular case lack of the commutativity of $\mathrm{Cl}(\mathcal{O})$ and therefore is far more complicated.



Supersingular isogeny graphs have been used in the Charles-Goren-Lauter cryptographic hash function and the supersingular isogeny Diffie--Hellman (SIDH) protocole of De Feo and Jao.

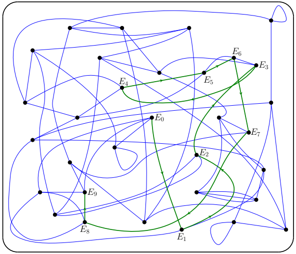
A recently proposed alternative to SIDH is the commutative supersingular isogeny Diffie-Hellman (CSIDH) protocole, in which the isogeny graph is first restricted to $\mathbb{F}_p$-rational curves E and $\mathbb{F}_p$-rational isogenies then oriented by the subring $\mathbb{Z}[\pi] \subset \mathrm{End}(E)$ generated by the Frobenius endomorphism $\pi : E \to E$.

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) protocole.

Supersingular isogeny graphs have been used in the Charles-Goren-Lauter cryptographic hash function and the supersingular isogeny Diffie--Hellman (SIDH) protocole of De Feo and Jao.

A recently proposed alternative to SIDH is the commutative supersingular isogeny Diffie-Hellman (CSIDH) protocole, in which the isogeny graph is first restricted to $\mathbb{F}_p$-rational curves E and $\mathbb{F}_p$-rational isogenies then oriented by the subring $\mathbb{Z}[\pi] \subset \mathrm{End}(E)$ generated by the Frobenius endomorphism $\pi : E \to E$.

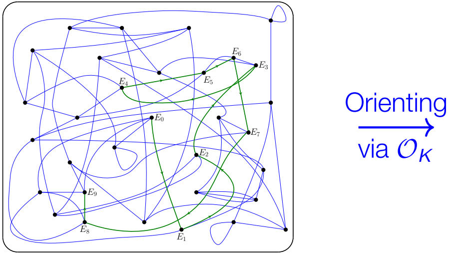
We introduce a general notion of orienting supersingular elliptic curves and their isogenies, and use this as the basis to construct a general oriented supersingular isogeny Diffie-Hellman (OSIDH) protocole.



Supersingular isogeny graphs have been used in the Charles-Goren-Lauter cryptographic hash function and the supersingular isogeny Diffie--Hellman (SIDH) protocole of De Feo and Jao.

A recently proposed alternative to SIDH is the commutative supersingular isogeny Diffie-Hellman (CSIDH) protocole, in which the isogeny graph is first restricted to $\mathbb{F}_p$-rational curves E and $\mathbb{F}_p$-rational isogenies then oriented by the subring $\mathbb{Z}[\pi] \subset \mathrm{End}(E)$ generated by the Frobenius endomorphism $\pi : E \to E$.

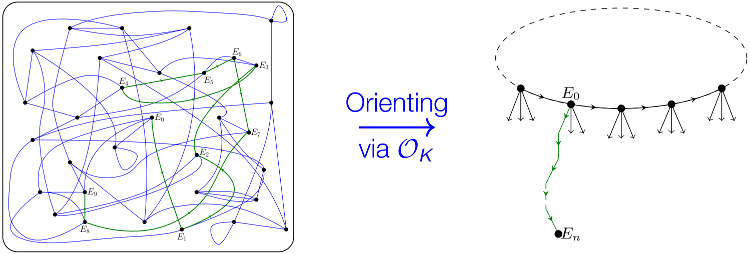
We introduce a general notion of orienting supersingular elliptic curves and their isogenies, and use this as the basis to construct a general oriented supersingular isogeny Diffie-Hellman (OSIDH) protocole.



Supersingular isogeny graphs have been used in the Charles-Goren-Lauter cryptographic hash function and the supersingular isogeny Diffie--Hellman (SIDH) protocole of De Feo and Jao.

A recently proposed alternative to SIDH is the commutative supersingular isogeny Diffie-Hellman (CSIDH) protocole, in which the isogeny graph is first restricted to $\mathbb{F}_p$-rational curves E and $\mathbb{F}_p$-rational isogenies then oriented by the subring $\mathbb{Z}[\pi] \subset \mathrm{End}(E)$ generated by the Frobenius endomorphism $\pi : E \to E$.

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) protocole.

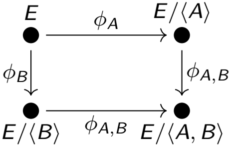


SIDH

We take two small primes ℓ_A and ℓ_B and a large prime $p = \ell_A^{n_A}\ell_B^{n_B} f \mp 1$ where f is a small correction term.
We also choose a random supersingular elliptic curve $E/\mathbb{F}_{p^2}$ with

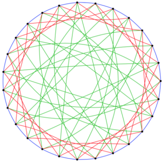
$$E(\mathbb{F}_{p^2}) \simeq (\mathbb{Z}/(p \pm 1)\mathbb{Z})^2$$

We use isogenies ϕ_A and ϕ_B with kernels of order $\ell_A^{e_a}$ and $\ell_B^{e_B}$ respectively.
The following commutative diagram establish the key exchange protocol:



CSIDH

We fix n small primes ℓ_i and a large prime $p = 4\ell_1 \cdot \ldots \cdot \ell_n - 1$.
We fix the supersingular elliptic curve $E_0 : y^2 = x^3 + x$ defined over $\mathbb{F}_p$. We consider endomorphism rings defined over $\mathbb{F}_p$ and therefore we get $\mathrm{End}(E_0) = \mathbb{Z}[\pi]$. Thus we orient supersingular isogeny graphs (over $\mathbb{F}_p$) using Frobenius.
The protocol then follows the Couveignes-Rostovtsev-Stolbunov idea in the union of ℓ_i-isogeny graphs (over $\mathbb{F}_p$):



Suppose we are given:

- A maximal order $\mathcal{O}_K$ in a quadratic imaginary field K of (small) discriminant Δ (eg. $\Delta = -3, -4$).
- A large prime number p ramified or inert in $\mathcal{O}_K$. Set $k = \mathbb{F}_{p^2}$.
- A supersingular elliptic curve E_0 defined over $\mathbb{F}_p$ equipped with an embedding $\mathcal{O}_K \hookrightarrow \mathrm{End}(E_0)$.
  - Observe that in the supersingular case $\mathrm{End}(E_0) := \mathrm{End}_{\overline{k}}(E_0) = \mathrm{End}_k(E_0)$
  - For $\Delta = -3$ we have $j = 0$ and we may take $E_0 : y^2 = x^3 + 1$.
- A small prime ℓ (eg $\ell = 2, 3$) and a chain of ℓ-isogenies

$$E_0 \xrightarrow[\phi_0]{\ell} E_1 \xrightarrow[\phi_1]{\ell} E_2 \xrightarrow[\phi_2]{\ell} \dots \xrightarrow[\phi_{n-1}]{\ell} E_n$$

Let us consider $K/\mathbb{Q}$ a quadratic imaginary extension and its ring of integers $\mathcal{O}_K$.

Definition

A K-orientation on E/k is a homomorphism

$$\iota : K \hookrightarrow \mathrm{End}_k(E) \otimes \mathbb{Q} = \mathrm{End}_k^0(E) = \mathfrak{B}$$

- E/k has complex multiplication: if k is a finite field then either
  - $K \simeq \mathbb{Q}(\pi)$ where $\pi = \mathrm{Frob}(\pi)$; E is ordinary or
  - $\mathfrak{B}$ is a quaternion algebra; E is supersingular.

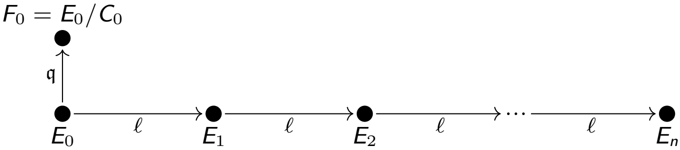
Definition

Given an order $\mathcal{O} \subseteq \mathcal{O}_K \subseteq K$, a primitive $\mathcal{O}$-orientation on $E_{/k}$ is:

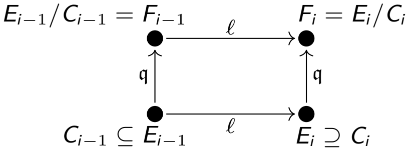
- A K-orientation on E/k such that
- $\iota : \mathcal{O} \xrightarrow{\sim} \iota(K) \cap \mathrm{End}_k(E)$ is an isomorphism.

- Let q be a prime such that $q\mathcal{O}_K = \mathfrak{q}\overline{\mathfrak{q}}$, i.e., $\left(\frac{\Delta}{q}\right) = 1$. Here we consider q another ``small'' (bounded by some constant) prime different from ℓ.

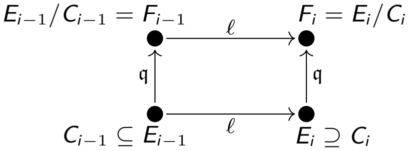
- Let q be a prime such that $q\mathcal{O}_K = \mathfrak{q}\bar{\mathfrak{q}}$, i.e., $\left(\frac{\Delta}{q}\right) = 1$. Here we consider q another "small" (bounded by some constant) prime different from ℓ.
- Solve for $C_0 = E_0[\mathfrak{q}]$. This can be determined by
  - Kernel polynomial or
  - Root of $\Phi_q(j_0, X)$.



- Let q be a prime such that $q\mathcal{O}_K = \mathfrak{q}\bar{\mathfrak{q}}$, i.e., $\left(\frac{\Delta}{q}\right) = 1$. Here we consider q another ``small'' (bounded by some constant) prime different from ℓ.
- Solve for $C_0 = E_0[\mathfrak{q}]$. This can be determined by
  - Kernel polynomial or
  - Root of $\Phi_q(j_0, X)$.
- Solve for $C_i = E_i[\mathfrak{q}_i]$ where now $\mathfrak{q}_i = \mathfrak{q} \cap \mathbb{Z} + \ell^i \mathcal{O}_K$
  - Pushing forward C_i, i.e., $C_i = \phi_{i-1}(C_{i-1})$*or*
  - Common root of $\Phi_\ell(j(F_{i-1}), X)$ and $\Phi_q(j(E_i), X)$.



- Let q be a prime such that $q\mathcal{O}_K = \mathfrak{q}\bar{\mathfrak{q}}$, i.e., $\left(\frac{\Delta}{q}\right) = 1$. Here we consider q another ``small'' (bounded by some constant) prime different from ℓ.
- Solve for $C_0 = E_0[\mathfrak{q}]$. This can be determined by
  - Kernel polynomial or
  - Root of $\Phi_q(j_0, X)$.
- Solve for $C_i = E_i[\mathfrak{q}_i]$ where now $\mathfrak{q}_i = \mathfrak{q} \cap \mathbb{Z} + \ell^i\mathcal{O}_K$
  - Pushing forward C_i, i.e., $C_i = \phi_{i-1}(C_{i-1})$*or*
  - Common root of $\Phi_\ell(j(F_{i-1}), X)$ and $\Phi_q(j(E_i), X)$.

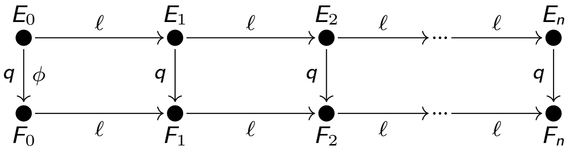


- The data of C_n (or $j(F_n)$) and $\mathfrak{q} \subseteq \mathcal{O}_K$ determine a $(K, \mathfrak{q})$-orientation on E_n.

Let $E_0 \to E_1 \to E_2 \to \ldots \to E_n$ be an ℓ-isogeny chain of length n and $\phi : E_0 \to F_0$ an isogeny of degree q with ℓ and q two distinct "small" primes.

Definition

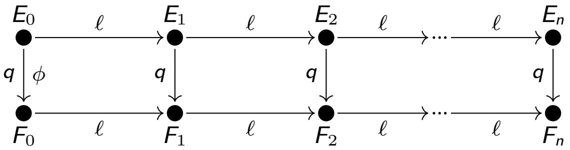
A ladder is a commutative diagram of isogenies



Let $E_0 \to E_1 \to E_2 \to \ldots \to E_n$ be an ℓ-isogeny chain of length n and $\phi : E_0 \to F_0$ an isogeny of degree q with ℓ and q two distinct "small" primes.

Definition

A ladder is a commutative diagram of isogenies



Modular Interpretation

A modular ladder of width q and depth n is a pair of $(n+1)$-tuples

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

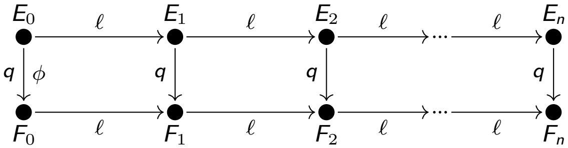
such that

$$\Phi_\ell(j_i, j_{i+1}) = \Phi_\ell(j'_i, j'_{i+1}) = \Phi_q(j_i, j'_i) = 0 \quad \text{for all } 0 \le i \le n$$

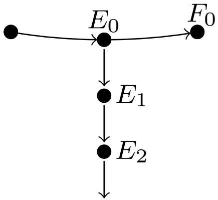
Let $E_0 \to E_1 \to E_2 \to \ldots \to E_n$ be an ℓ-isogeny chain of length n and $\phi : E_0 \to F_0$ an isogeny of degree q with ℓ and q two distinct "small" primes.

Definition

A ladder is a commutative diagram of isogenies



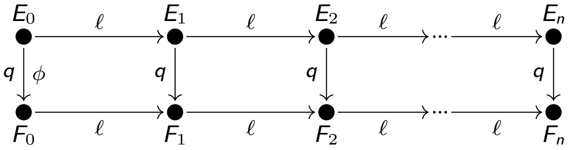
If $q = \ell$, the ladder collapses:



Let $E_0 \to E_1 \to E_2 \to \ldots \to E_n$ be an ℓ-isogeny chain of length n and $\phi : E_0 \to F_0$ an isogeny of degree q with ℓ and q two distinct ``small'' primes.

Definition

A ladder is a commutative diagram of isogenies

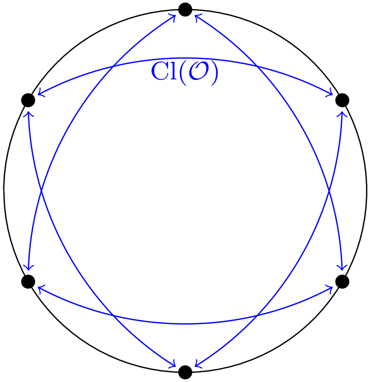


A ladder is rectangular if $\phi : E_0 \to F_0$ is horizontal.

Lemma

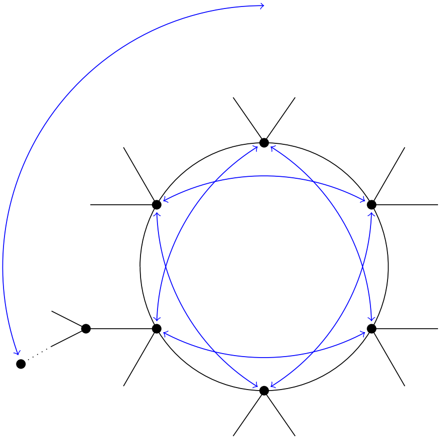
If a ladder is rectangular, then $\mathrm{End}(E_i) = \mathrm{End}(F_i)$ for all $0 \leq i \leq n$.

We define a *vortex* to be an isogeny cycle (crater) equipped with an action of a (subgroup of) $\mathrm{Cl}(\mathcal{O})$.



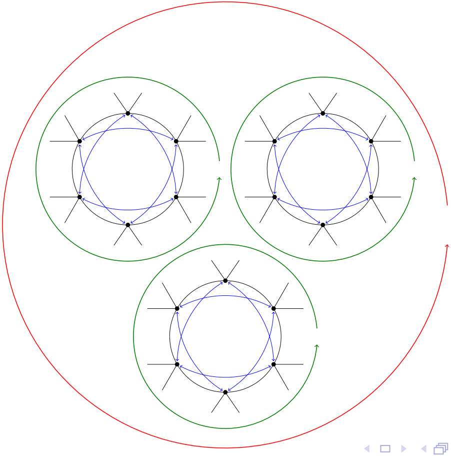
Instead of considering the union of different isogeny graphs, we focus on one single crater and we think of all the other primes as acting on it: the resulting object is a single isogeny circle rotating under the action of $\mathrm{Cl}(\mathcal{O})$.

In the same way, we define a *whirpool* to be a complete isogeny volcano acted on by the class group. We would like to think at isogeny graphs as moving objects.

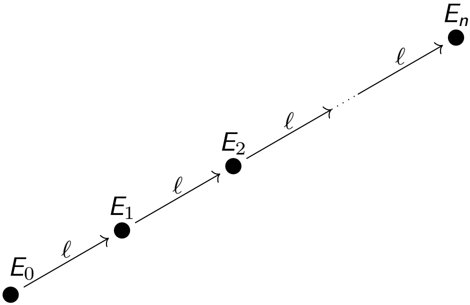


In the same way, we define a *whirpool* to be a complete isogeny volcano acted on by the class group. We would like to think at isogeny graphs as moving objects.

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

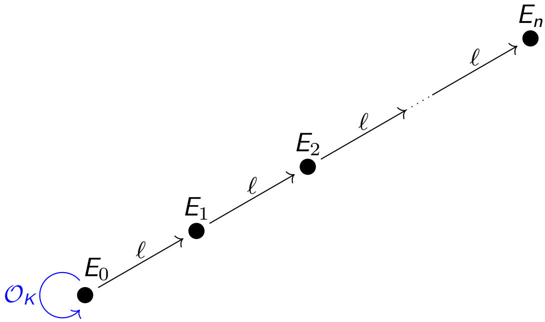


We consider an elliptic curve E_0 with an effective endomorphism ring (eg. $j_0 = 0, 1728$) and a chain of ℓ-isogenies.



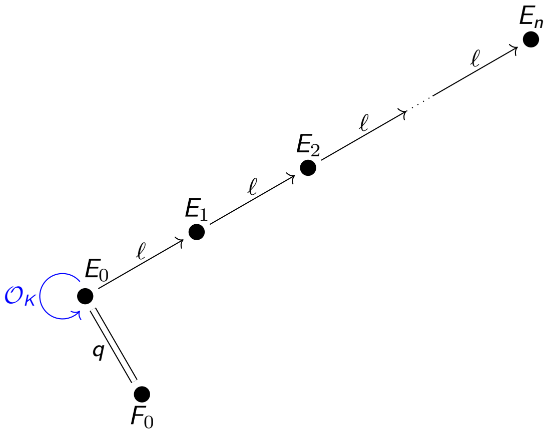
We consider an elliptic curve E_0 with an effective endomorphism ring (eg. $j_0 = 0, 1728$) and a chain of ℓ-isogenies.

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



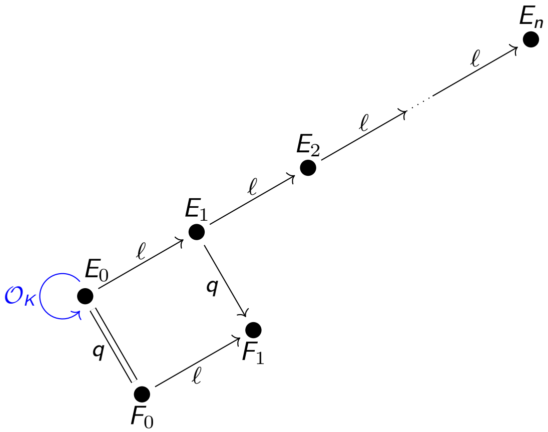
We consider an elliptic curve E_0 with an effective endomorphism ring (eg. $j_0 = 0, 1728$) and a chain of ℓ-isogenies.

- Horizontal isogenies must be endomorphisms



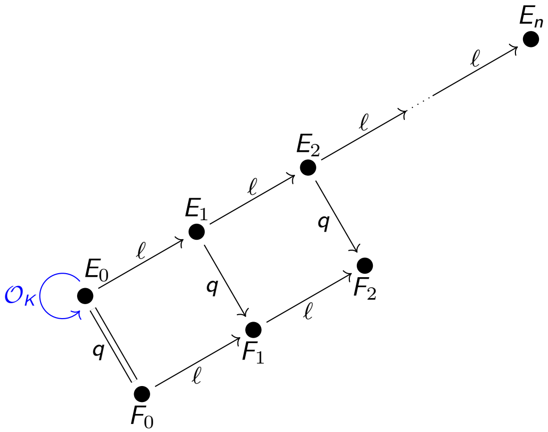
We consider an elliptic curve E_0 with an effective endomorphism ring (eg. $j_0 = 0, 1728$) and a chain of ℓ-isogenies.

- We push forward our q-orientation obtaining F_1.



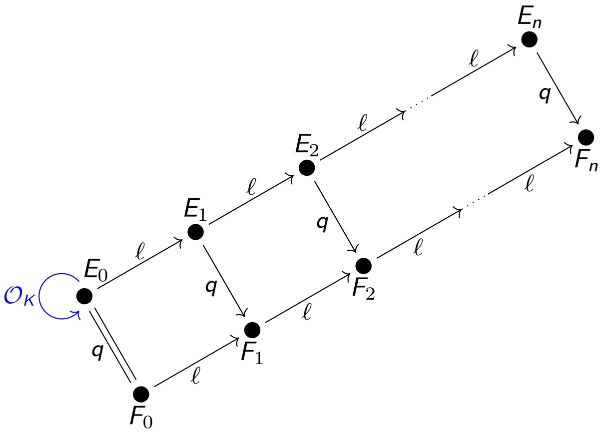
We consider an elliptic curve E_0 with an effective endomorphism ring (eg. $j_0 = 0, 1728$) and a chain of ℓ-isogenies.

- We repeat the process for F_2.

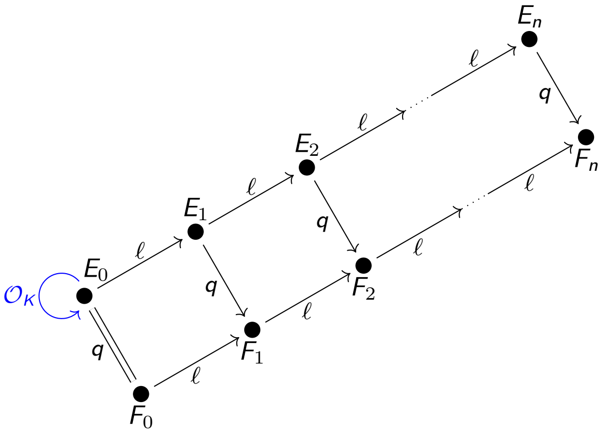


We consider an elliptic curve E_0 with an effective endomorphism ring (eg. $j_0 = 0, 1728$) and a chain of ℓ-isogenies.

- And again till F_n.

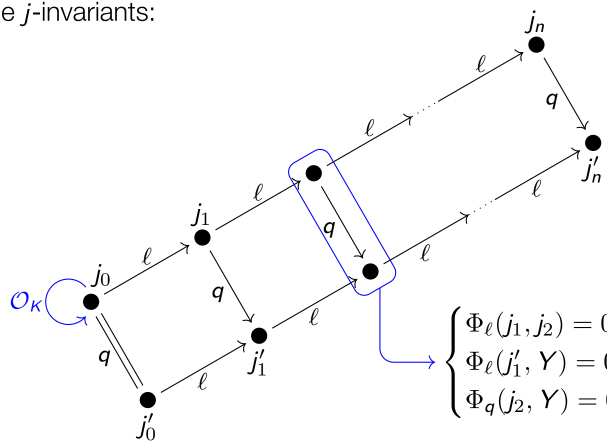


We consider an elliptic curve E_0 with an effective endomorphism ring (eg. $j_0 = 0, 1728$) and a chain of ℓ-isogenies.



How far should we go? We would like to move away from the center (E_0) untill $\#\mathrm{Cl}(\mathcal{O})$ is around the size of p in order to cover all supersingular curves (get all the possible choices). For instance, $p \sim 2^{1024}$ and $n \sim 1024$.

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:



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

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

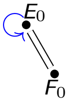
$$\begin{cases} \Phi_\ell(j'_1, Y) = 0 \\ \Phi_q(j_2, Y) = 0 \end{cases}$$

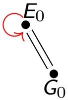
PUBLIC DATA: A chain of ℓ-isogenies $E_0 \to E_1 \to \ldots \to E_n$		
	ALICE	**BOB**

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

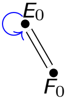
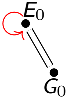
ALICE | **BOB**

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

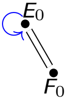
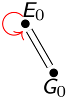




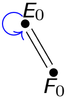
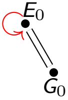
PUBLIC DATA: A chain of ℓ-isogenies $E_0 \to E_1 \to \ldots \to E_n$

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

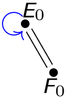
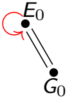
PUBLIC DATA: A chain of ℓ-isogenies $E_0 \to E_1 \to \ldots \to E_n$

	ALICE	**BOB**
Choose a smooth $\mathcal{O}_K$-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	$\{G_i\}_{i=1}^n$	$\{F_i\}_{i=1}^n$

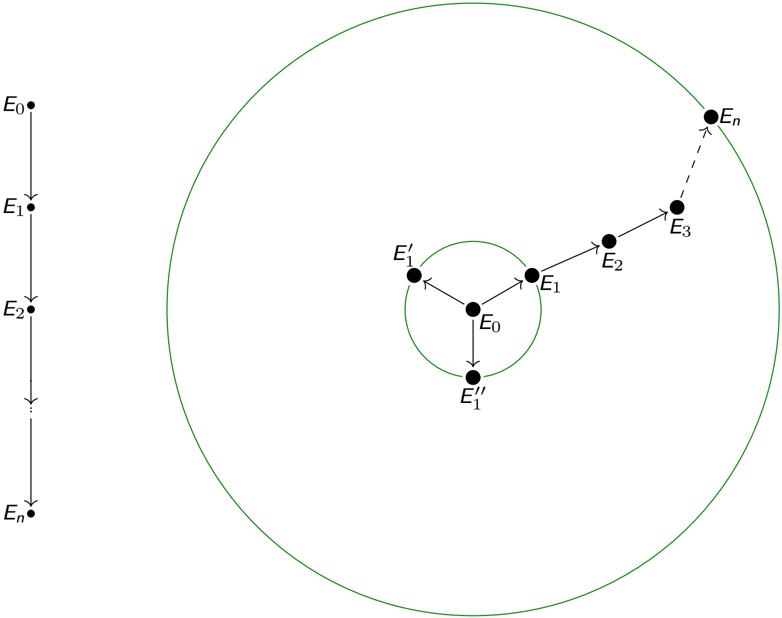
PUBLIC DATA: A chain of ℓ-isogenies $E_0 \to E_1 \to \ldots \to E_n$

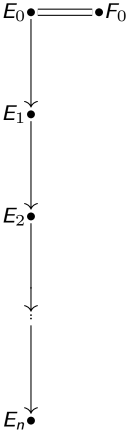
	ALICE	**BOB**
Choose a smooth $\mathcal{O}_K$-orientation of E_0		
Push it forward to depth n	$\underbrace{E_0 = F_0 \to F_1 \to \ldots \to F_n}_{\phi_A}$	$\underbrace{E_0 = G_0 \to G_1 \to \ldots \to G_n}_{\phi_B}$
Exchange data	$\{G_i\}_{i=1}^n$	$\{F_i\}_{i=1}^n$
Compute shared secret	Compute $\phi_A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

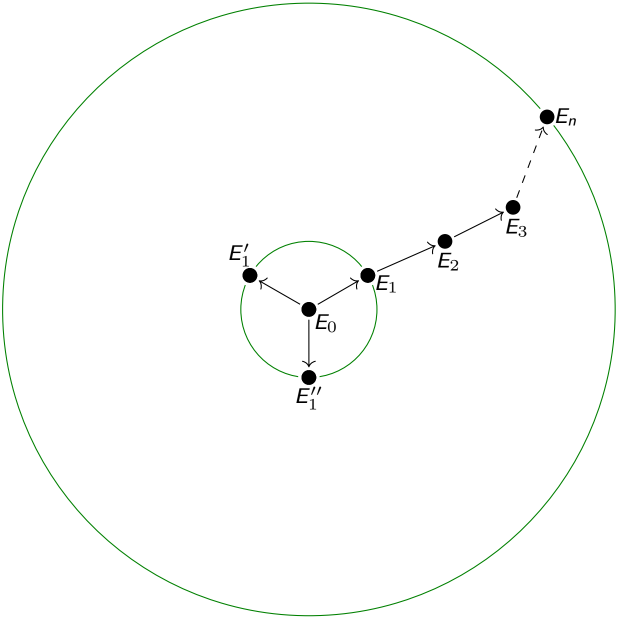
PUBLIC DATA: A chain of ℓ-isogenies $E_0 \to E_1 \to \ldots \to E_n$

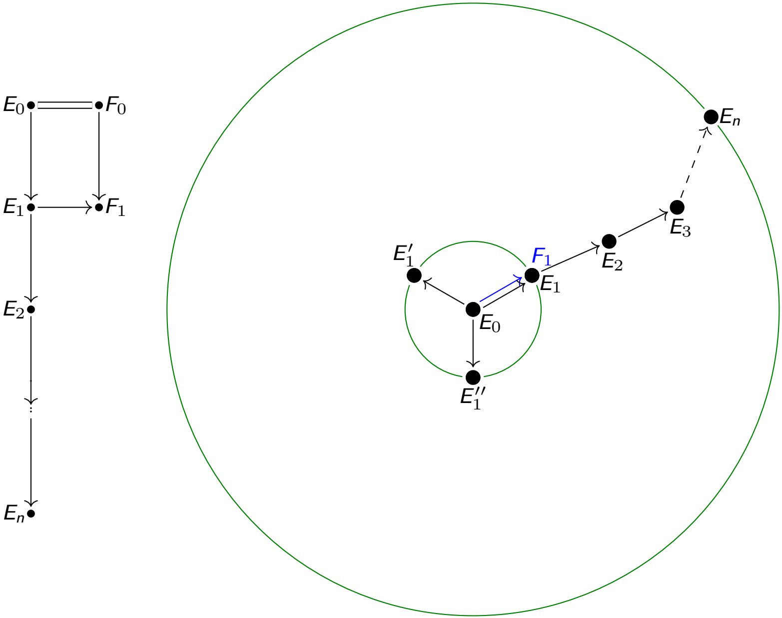
	ALICE	**BOB**
Choose a smooth $\mathcal{O}_K$-orientation of E_0		
Push it forward to depth n	$\underbrace{E_0 = F_0 \to F_1 \to \ldots \to F_n}_{\phi_A}$	$\underbrace{E_0 = G_0 \to G_1 \to \ldots \to G_n}_{\phi_B}$
Exchange data	$\{G_i\}_{i=1}^n$	$\{F_i\}_{i=1}^n$
Compute shared secret	Compute $\phi_A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

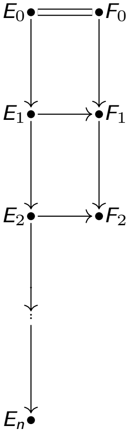
In the end, both Alice and Bob will share a new chain $E_0 \to H_1 \to \ldots \to H_n$

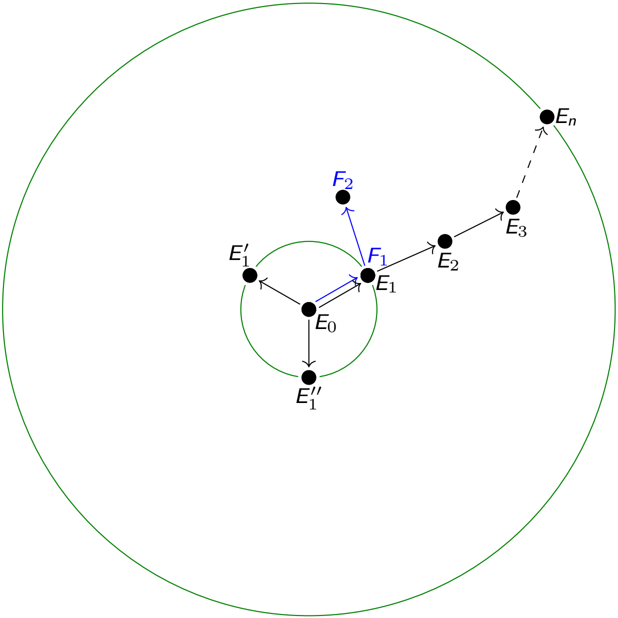

E_0
E_1
E_2
$\vdots$
E_n
E_1'
E_1
E_0
E_1''
E_2
E_3
E_n

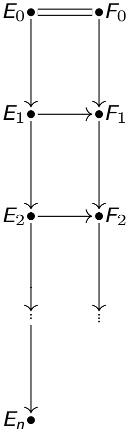

E_0
F_0
E_1
E_2
$\vdots$
E_n


E_n
E_3
E_2
E_1'
E_1
E_0
E_1''

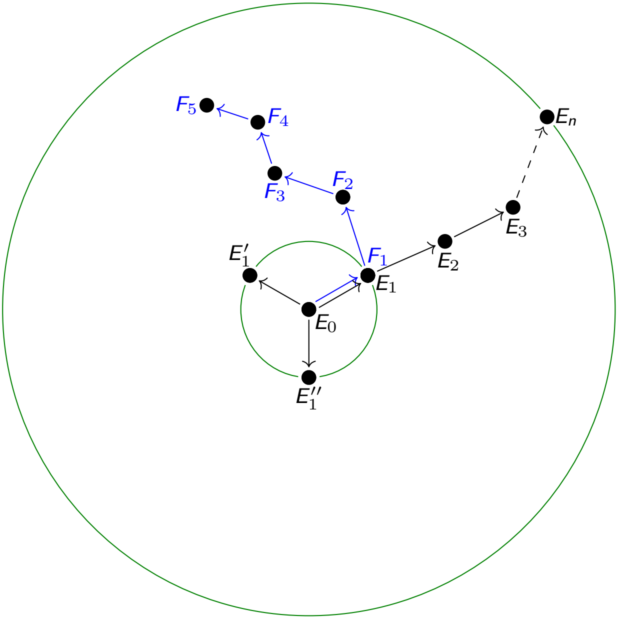

E_0
F_0
E_1
F_1
E_2
E_n
E_1'
F_1
E_1
E_2
E_3
E_n
E_0
E_1''


E_0
F_0
E_1
F_1
E_2
F_2
E_n

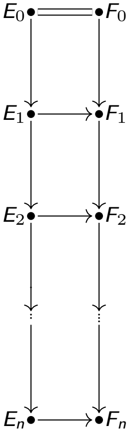

E_n
F_2
E_3
E_1'
F_1
E_2
E_1
E_0
E_1''

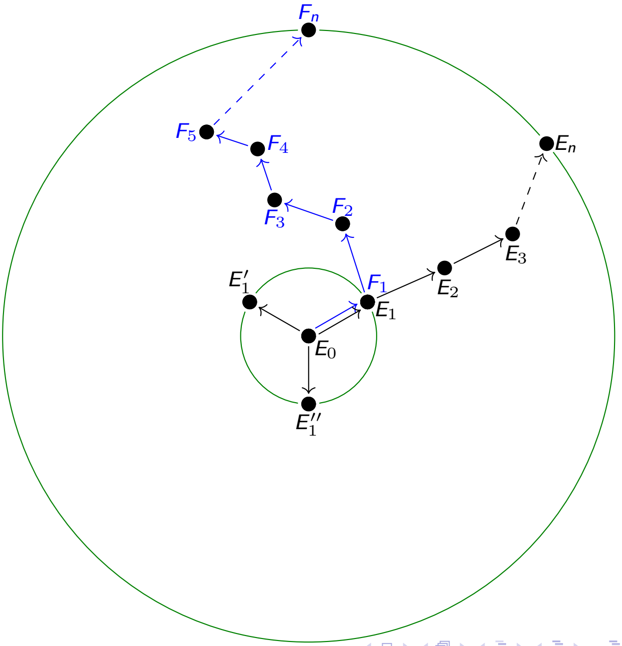


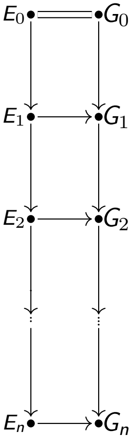
E_0
F_0
E_1
F_1
E_2
F_2
E_n

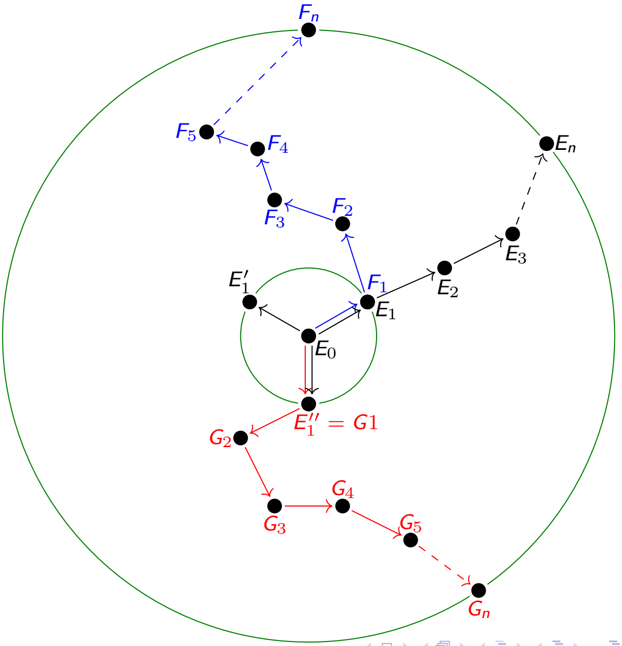


F_5
F_4
E_n
F_2
F_3
E_3
E'_1
F_1
E_2
E_1
E_0
E''_1


E_0
F_0
E_1
F_1
E_2
F_2
E_n
F_n


F_n
F_5
F_4
E_n
F_3
F_2
E_3
E_1'
F_1
E_2
E_1
E_0
E_1''


E_0
G_0
E_1
G_1
E_2
G_2
E_n
G_n


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

This first attempt presents a weak point: we know $\text{End}(E_0)$ and, at each step, we also deduce

$$\mathbb{Z} + \ell\text{End}(E_i) \subset \text{End}(E_{i+1}) = \text{End}(F_{i+1})$$

Thus, knowing $\mathbb{Z} + \ell^n\text{End}(E_0) \subset \text{End}(F_n)$, we can construct $\text{End}(F_n)$ and this will give us information on how to construct ϕ_A - Alice's private key.[1]

The problem is that we pass to the other party the knowledge of the entire chain $\{F_i\}$ (respectively G_i).

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

[1] Theorem 4.1 "On the security of supersingular isogeny cryptosystems", S.D. Galbraith, C. Petit, B. Shani, Y. Bo Ti, 2016

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

ALICE	**BOB**

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

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

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

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

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

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

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

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

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

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

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 some bound $[-r, r]$	$(e_1, \ldots, e_t)$	$(d_1, \ldots, d_t)$
Construct an isogenous curve	$F_n = E_n/E_n\left[\mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_t^{e_t}\right]$	$G_n = E_n/E_n\left[\mathfrak{p}_1^{d_1} \cdot \ldots \cdot \mathfrak{p}_t^{d_t}\right]$
Precompute all directions for each 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 $j > i$.

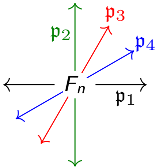
PUBLIC DATA: A chain of ℓ-isogenies $E_0 \to E_1 \to \ldots \to E_n$ and a set of splitting primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_t \subseteq \mathcal{O} \subseteq \mathrm{End}(E_n) \cap K \subseteq \mathcal{O}_K$

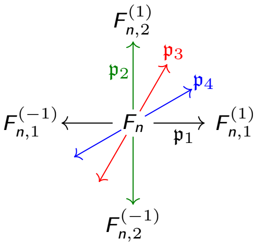
	ALICE	**BOB**
Choose integers in some bound $[-r, r]$	$(e_1, \ldots, e_t)$	$(d_1, \ldots, d_t)$
Construct an isogenous curve	$F_n = E_n / E_n \left[\mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_t^{e_t}\right]$	$G_n = E_n / E_n \left[\mathfrak{p}_1^{d_1} \cdot \ldots \cdot \mathfrak{p}_t^{d_t}\right]$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

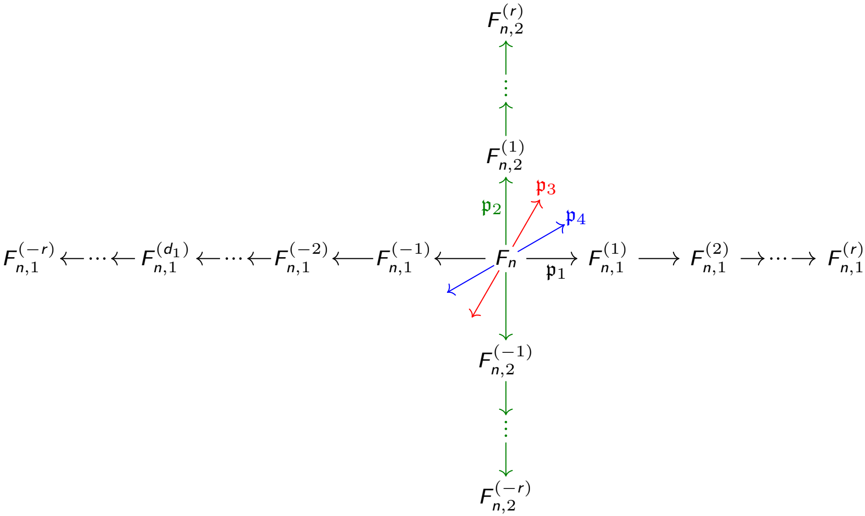
In the end, both Alice and Bob will share the elliptic curve

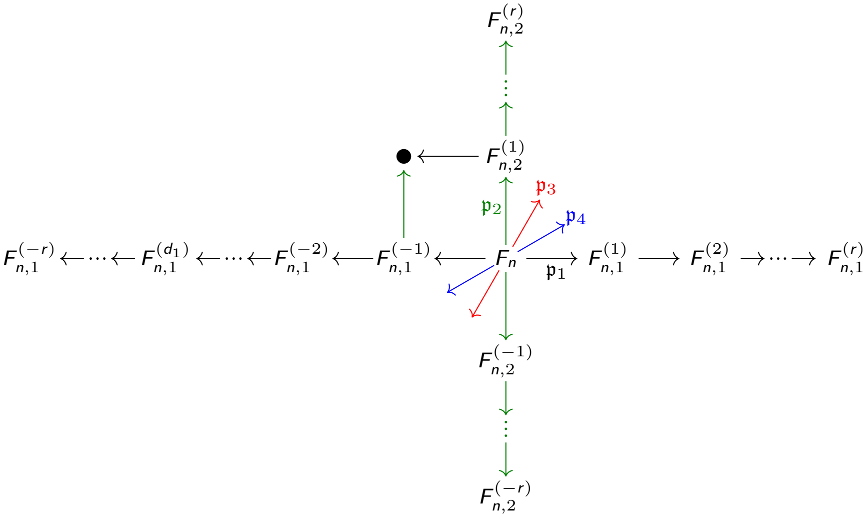
$$H_n = E_n / E_n \left[\mathfrak{p}_1^{e_1+d_1} \cdot \ldots \cdot \mathfrak{p}_t^{e_t+d_t}\right]$$

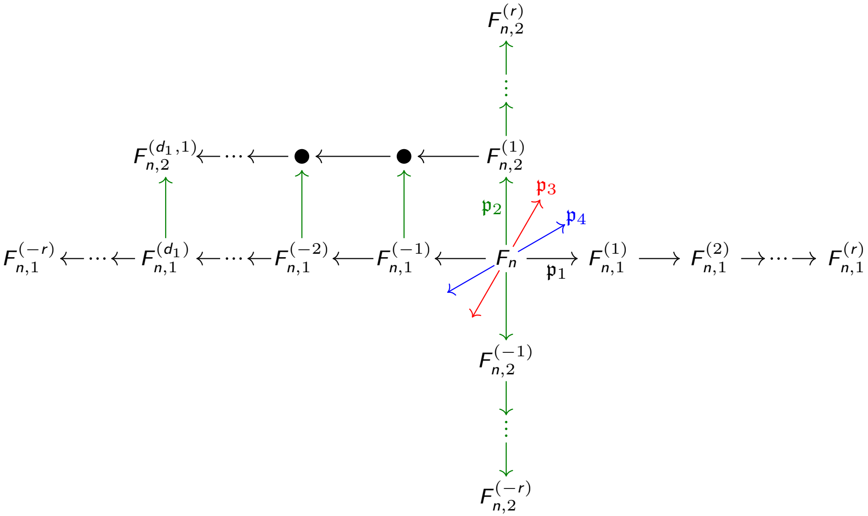
F_n

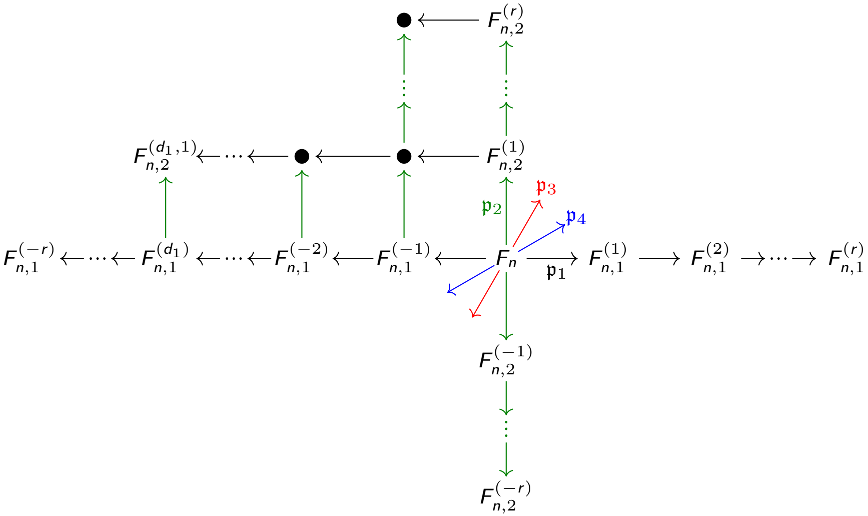

$\mathfrak{p}_3$
$\mathfrak{p}_2$
$\mathfrak{p}_4$
F_n
$\mathfrak{p}_1$

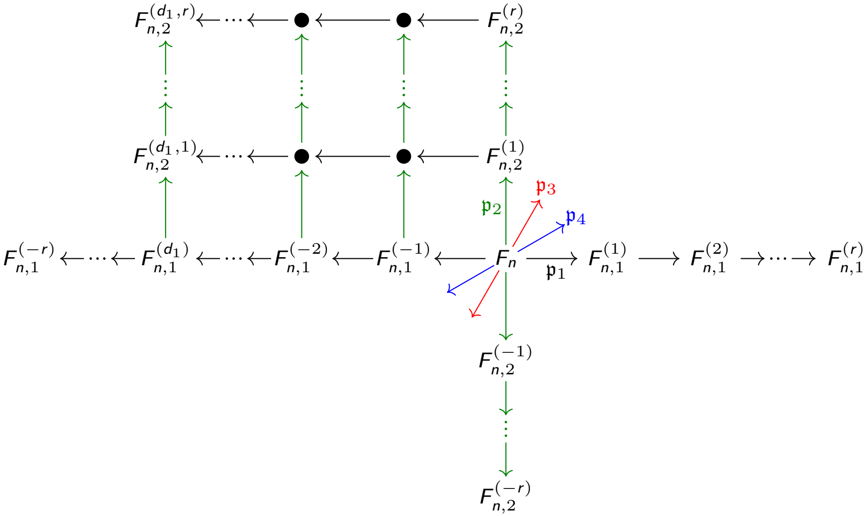

$F_{n,2}^{(1)}$
$\mathfrak{p}_2$
$\mathfrak{p}_3$
$\mathfrak{p}_4$
$F_{n,1}^{(-1)}$
F_n
$\mathfrak{p}_1$
$F_{n,1}^{(1)}$
$F_{n,2}^{(-1)}$

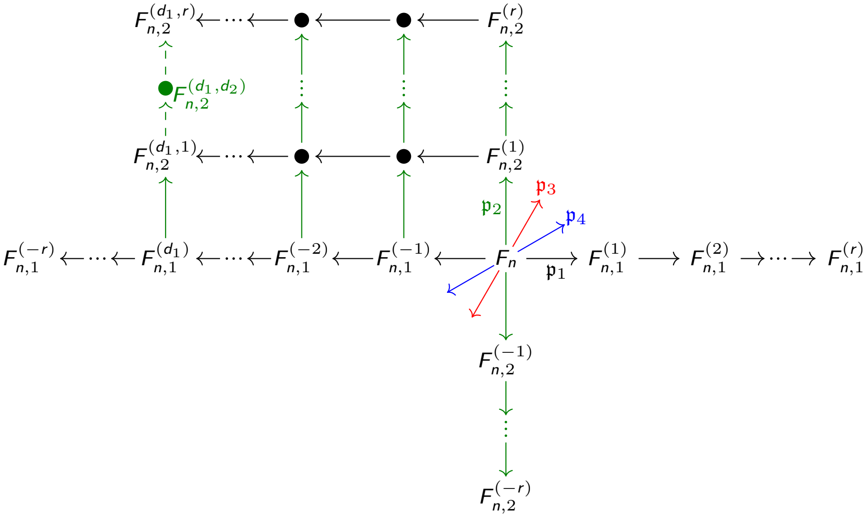

$F_{n,2}^{(r)}$
$F_{n,2}^{(1)}$
$\mathfrak{p}_2$
$\mathfrak{p}_3$
$\mathfrak{p}_4$
$F_{n,1}^{(-r)} \longleftarrow \cdots \longleftarrow F_{n,1}^{(d_1)} \longleftarrow \cdots \longleftarrow F_{n,1}^{(-2)} \longleftarrow F_{n,1}^{(-1)} \longleftarrow F_n \longrightarrow F_{n,1}^{(1)} \longrightarrow F_{n,1}^{(2)} \longrightarrow \cdots \longrightarrow F_{n,1}^{(r)}$
$\mathfrak{p}_1$
$F_{n,2}^{(-1)}$
$F_{n,2}^{(-r)}$


$F_{n,2}^{(r)}$
$F_{n,2}^{(1)}$
$\mathfrak{p}_3$
$\mathfrak{p}_2$
$\mathfrak{p}_4$
$F_{n,1}^{(-r)}$
$F_{n,1}^{(d_1)}$
$F_{n,1}^{(-2)}$
$F_{n,1}^{(-1)}$
F_n
$\mathfrak{p}_1$
$F_{n,1}^{(1)}$
$F_{n,1}^{(2)}$
$F_{n,1}^{(r)}$
$F_{n,2}^{(-1)}$
$F_{n,2}^{(-r)}$

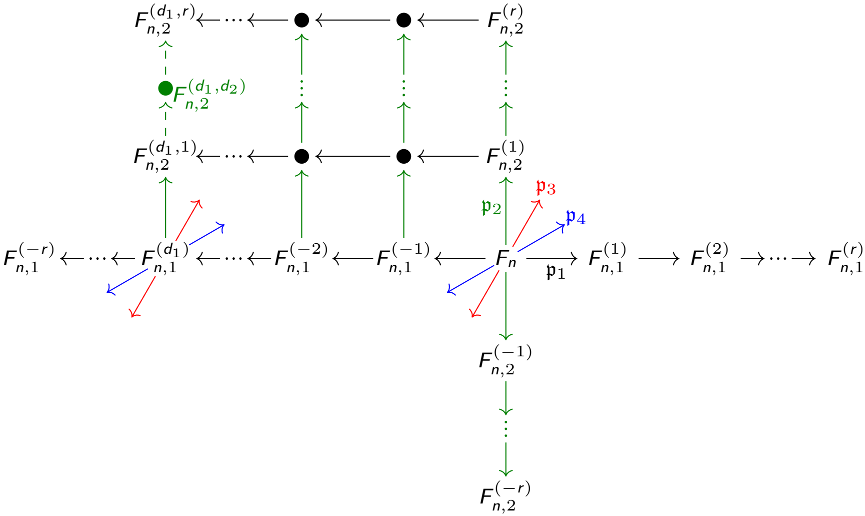

$F_{n,2}^{(r)}$
$F_{n,2}^{(d_1,1)}$
$F_{n,2}^{(1)}$
$\mathfrak{p}_2$
$\mathfrak{p}_3$
$\mathfrak{p}_4$
$F_{n,1}^{(-r)}$
$F_{n,1}^{(d_1)}$
$F_{n,1}^{(-2)}$
$F_{n,1}^{(-1)}$
F_n
$\mathfrak{p}_1$
$F_{n,1}^{(1)}$
$F_{n,1}^{(2)}$
$F_{n,1}^{(r)}$
$F_{n,2}^{(-1)}$
$F_{n,2}^{(-r)}$

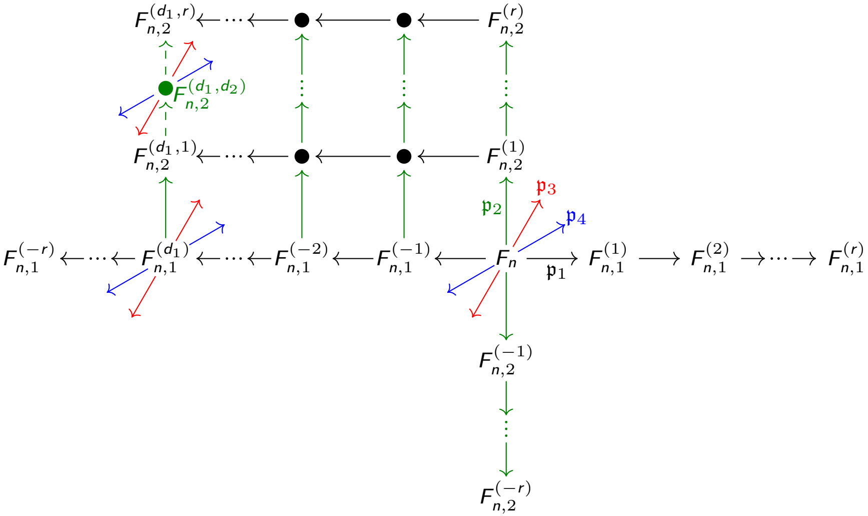

$F_{n,2}^{(r)}$
$F_{n,2}^{(d_1,1)}$
$F_{n,2}^{(1)}$
$\mathfrak{p}_3$
$\mathfrak{p}_2$
$\mathfrak{p}_4$
$F_{n,1}^{(-r)}$
$F_{n,1}^{(d_1)}$
$F_{n,1}^{(-2)}$
$F_{n,1}^{(-1)}$
F_n
$F_{n,1}^{(1)}$
$F_{n,1}^{(2)}$
$F_{n,1}^{(r)}$
$\mathfrak{p}_1$
$F_{n,2}^{(-1)}$
$F_{n,2}^{(-r)}$


$F_{n,2}^{(d_1,r)}$
$F_{n,2}^{(r)}$
$F_{n,2}^{(d_1,1)}$
$F_{n,2}^{(1)}$
$\mathfrak{p}_3$
$\mathfrak{p}_2$
$\mathfrak{p}_4$
$F_{n,1}^{(-r)}$
$F_{n,1}^{(d_1)}$
$F_{n,1}^{(-2)}$
$F_{n,1}^{(-1)}$
F_n
$F_{n,1}^{(1)}$
$F_{n,1}^{(2)}$
$F_{n,1}^{(r)}$
$\mathfrak{p}_1$
$F_{n,2}^{(-1)}$
$F_{n,2}^{(-r)}$

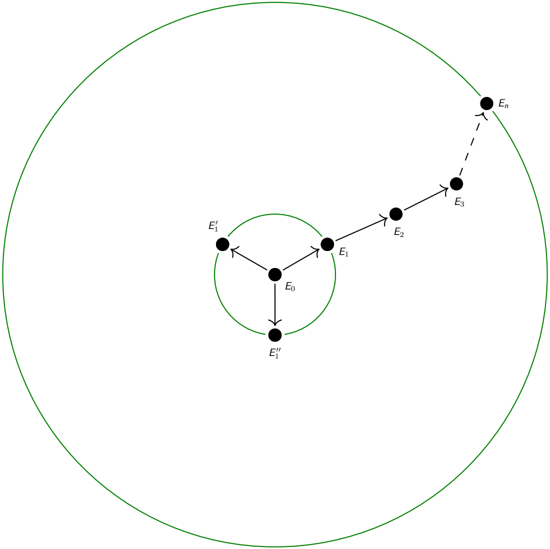


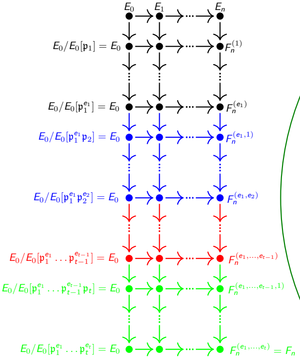
$F_{n,2}^{(d_1,r)}$
$F_{n,2}^{(r)}$
$F_{n,2}^{(d_1,d_2)}$
$F_{n,2}^{(d_1,1)}$
$F_{n,2}^{(1)}$
$\mathfrak{p}_3$
$\mathfrak{p}_2$
$\mathfrak{p}_4$
$F_{n,1}^{(-r)}$
$F_{n,1}^{(d_1)}$
$F_{n,1}^{(-2)}$
$F_{n,1}^{(-1)}$
F_n
$\mathfrak{p}_1$
$F_{n,1}^{(1)}$
$F_{n,1}^{(2)}$
$F_{n,1}^{(r)}$
$F_{n,2}^{(-1)}$
$F_{n,2}^{(-r)}$

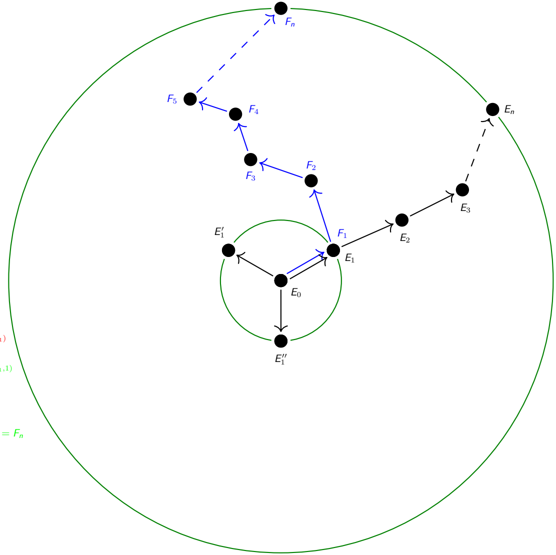

$F_{n,2}^{(d_1,r)}$
$F_{n,2}^{(r)}$
$F_{n,2}^{(d_1,d_2)}$
$F_{n,2}^{(d_1,1)}$
$F_{n,2}^{(1)}$
$\mathfrak{p}_3$
$\mathfrak{p}_2$
$\mathfrak{p}_4$
$F_{n,1}^{(-r)}$
$F_{n,1}^{(d_1)}$
$F_{n,1}^{(-2)}$
$F_{n,1}^{(-1)}$
F_n
$\mathfrak{p}_1$
$F_{n,1}^{(1)}$
$F_{n,1}^{(2)}$
$F_{n,1}^{(r)}$
$F_{n,2}^{(-1)}$
$F_{n,2}^{(-r)}$

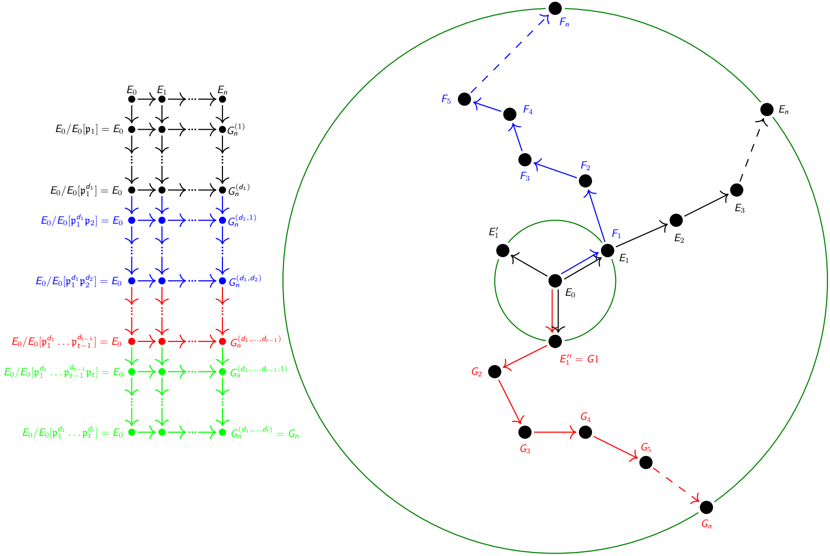


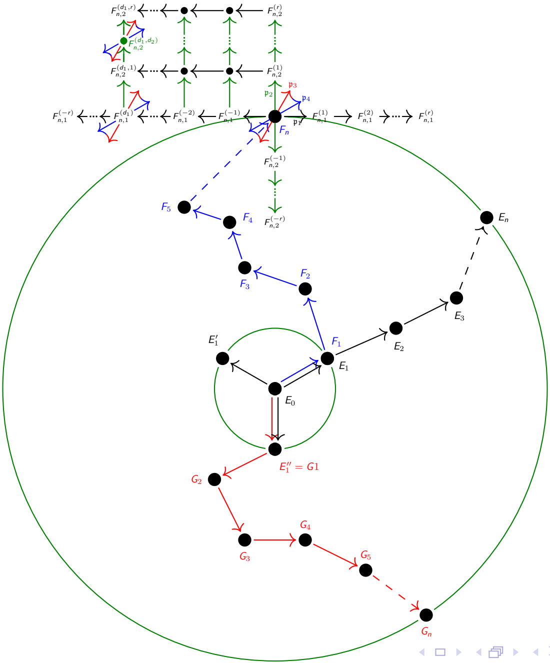
$F_{n,2}^{(d_1,r)}$
$F_{n,2}^{(r)}$
$F_{n,2}^{(d_1,d_2)}$
$F_{n,2}^{(d_1,1)}$
$F_{n,2}^{(1)}$
$\mathfrak{p}_2$
$\mathfrak{p}_3$
$\mathfrak{p}_4$
$F_{n,1}^{(-r)}$
$F_{n,1}^{(d_1)}$
$F_{n,1}^{(-2)}$
$F_{n,1}^{(-1)}$
F_n
$\mathfrak{p}_1$
$F_{n,1}^{(1)}$
$F_{n,1}^{(2)}$
$F_{n,1}^{(r)}$
$F_{n,2}^{(-1)}$
$F_{n,2}^{(-r)}$


E_n
E_3
E_2
E_1'
E_1
E_0
E_1''


E_0 E_1 E_n
$E_0/E_0[\mathfrak{p}_1] = E_0$ $F_n^{(1)}$
$E_0/E_0[\mathfrak{p}_1^{e_1}] = E_0$ $F_n^{(e_1)}$
$E_0/E_0[\mathfrak{p}_1^{e_1}\mathfrak{p}_2] = E_0$ $F_n^{(e_1,1)}$
$E_0/E_0[\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}] = E_0$ $F_n^{(e_1,e_2)}$
$E_0/E_0[\mathfrak{p}_1^{e_1}\dots\mathfrak{p}_{t-1}^{e_{t-1}}] = E_0$ $F_n^{(e_1,\dots,e_{t-1})}$
$E_0/E_0[\mathfrak{p}_1^{e_1}\dots\mathfrak{p}_{t-1}^{e_{t-1}}\mathfrak{p}_t] = E_0$ $F_n^{(e_1,\dots,e_{t-1},1)}$
$E_0/E_0[\mathfrak{p}_1^{e_1}\dots\mathfrak{p}_t^{e_t}] = E_0$ $F_n^{(e_1,\dots,e_t)} = F_n$


F_n
F_5
F_4
E_n
F_3
F_2
E_3
E_1'
F_1
E_2
E_1
E_0
E_1''


E_0 E_1 E_n
$E_0/E_0[\mathfrak{p}_1] = E_0$ $G_n^{(1)}$
$E_0/E_0[\mathfrak{p}_1^{d_1}] = E_0$ $G_n^{(d_1)}$
$E_0/E_0[\mathfrak{p}_1^{d_1}\mathfrak{p}_2] = E_0$ $G_n^{(d_1,1)}$
$E_0/E_0[\mathfrak{p}_1^{d_1}\mathfrak{p}_2^{d_2}] = E_0$ $G_n^{(d_1,d_2)}$
$E_0/E_0[\mathfrak{p}_1^{d_1}\dots\mathfrak{p}_{t-1}^{d_{t-1}}] = E_0$ $G_n^{(d_1,\dots,d_{t-1})}$
$E_0/E_0[\mathfrak{p}_1^{d_1}\dots\mathfrak{p}_{t-1}^{d_{t-1}}\mathfrak{p}_t] = E_0$ $G_n^{(d_1,\dots,d_{t-1},1)}$
$E_0/E_0[\mathfrak{p}_1^{d_1}\dots\mathfrak{p}_t^{d_t}] = E_0$ $G_n^{(d_1,\dots,d_t)} = G_n$
F_n 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


$F_{n,2}^{(d_1,r)}$
$F_{n,2}^{(r)}$
$F_{n,2}^{(d_1,d_2)}$
$F_{n,2}^{(d_1,1)}$
$F_{n,2}^{(1)}$
$\mathfrak{p}_2$
$\mathfrak{p}_3$
$\mathfrak{p}_4$
$\mathfrak{p}_1$
$F_{n,1}^{(-r)}$
$F_{n,1}^{(d_1)}$
$F_{n,1}^{(-2)}$
$F_{n,1}^{(-1)}$
$F_{n,1}^{(1)}$
$F_{n,1}^{(2)}$
$F_{n,1}^{(r)}$
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

This is a work in progress and we still want to develop the following aspects:

- Security analysis and setting security parameters.
- Implementation and algorithmic optimization.

This is a work in progress and we still want to develop the following aspects:

- Security analysis and setting security parameters.
- Implementation and algorithmic optimization.

MERCI POUR VOTRE ATTENTION