Isogeny representations for cryptography

Abel Laval
Université Libre de Bruxelles

December 2nd, 2025

Prelude

What do we know about isogeny-based cryptography ?

Prelude

What do we know about isogeny-based cryptography ?

Elliptic curves and their isogenies are very rich mathematical objects !

Prelude

What do we know about isogeny-based cryptography ?

Elliptic curves and their isogenies are very rich mathematical objects !

- Downsides :

- Upsides :

Prelude

What do we know about isogeny-based cryptography ?

Elliptic curves and their isogenies are very rich mathematical objects !

- Downsides :
  - Schemes are slow
- Upsides :

Prelude

What do we know about isogeny-based cryptography ?

Elliptic curves and their isogenies are very rich mathematical objects !

- Downsides :
  - Schemes are slow
  - Schemes die when a theorem from 1997 is discovered by cryptographers.
- Upsides :

Prelude

What do we know about isogeny-based cryptography ?

Elliptic curves and their isogenies are very rich mathematical objects !

- Downsides :
  - Schemes are slow
  - Schemes die when a theorem from 1997 is discovered by cryptographers.
- Upsides :
  - Keys are small

Prelude

What do we know about isogeny-based cryptography ?

Elliptic curves and their isogenies are very rich mathematical objects !

- Downsides :
  - Schemes are slow
  - Schemes die when a theorem from 1997 is discovered by cryptographers.
- Upsides :
  - Keys are small
  - There are many different approaches to tackle a specific problem.

Act I – Standard isogeny representations

Act I – The rational maps and kernel representations

Elliptic curves, isogenies, torsion groups and graphs

Elliptic curves and their isogenies

Definition (Elliptic curve)

An elliptic curve E over $\mathbb{F}_q$ is a smooth projective algebraic curve of genus 1. It is described by a cubic equation :

$$E = \left\{(x, y) \in \overline{\mathbb{F}}_q \times \overline{\mathbb{F}}_q,\ \ y^2 = x^3 + ax + b\right\} \cup \{\infty\}$$

with $a, b \in \mathbb{F}_q$ such that $4a^3 + 27b^2 \neq 0 \mod q$.

Elliptic curves and their isogenies

Definition (Elliptic curve)

An elliptic curve E over $\mathbb{F}_q$ is a smooth projective algebraic curve of genus 1.
It is described by a cubic equation :

$$E = \left\{(x, y) \in \overline{\mathbb{F}}_q \times \overline{\mathbb{F}}_q, \;\; y^2 = x^3 + ax + b\right\} \cup \{\infty\}$$

with $a, b \in \mathbb{F}_q$ such that $4a^3 + 27b^2 \neq 0 \mod q$.

E is the elliptic curve; $E(\mathbb{F}_q)$ is the set of rational points over $\mathbb{F}_q$.
$E(\mathbb{F}_q)$ is an abelian group. Its neutral element is ∞.

Elliptic curves and their isogenies

Definition (Elliptic curve)

An elliptic curve E over $\mathbb{F}_q$ is a smooth projective algebraic curve of genus 1. It is described by a cubic equation :

$$E = \left\{(x, y) \in \overline{\mathbb{F}}_q \times \overline{\mathbb{F}}_q, \;\; y^2 = x^3 + ax + b\right\} \cup \{\infty\}$$

with $a, b \in \mathbb{F}_q$ such that $4a^3 + 27b^2 \neq 0 \mod q$.

E is the elliptic curve; $E(\mathbb{F}_q)$ is the set of rational points over $\mathbb{F}_q$.
$E(\mathbb{F}_q)$ is an abelian group. Its neutral element is ∞.

Example

Let's take $E : y^2 = x^3 + 1$ over $\mathbb{F}_5$. It has 6 rational points :

$$E(\mathbb{F}_5) = \{(0, 1), (0, 4), (2, 2), (2, 3), (4, 0), \infty\}$$

Elliptic curves and their isogenies

Definition (Isogeny)

Let E_1, E_2 be two elliptic curves over $\mathbb{F}_q$.

Elliptic curves and their isogenies

Definition (Isogeny)

Let E_1, E_2 be two elliptic curves over $\mathbb{F}_q$.
An isogeny $\varphi : E_1 \to E_2$ is a group homomorphism with finite kernel.

Elliptic curves and their isogenies

Definition (Isogeny)

Let E_1, E_2 be two elliptic curves over $\mathbb{F}_q$.
An isogeny $\varphi : E_1 \to E_2$ is a group homomorphism with finite kernel.
It can be represented with rational maps.

Elliptic curves and their isogenies

Definition (Isogeny)

Let E_1, E_2 be two elliptic curves over $\mathbb{F}_q$.
An isogeny $\varphi : E_1 \to E_2$ is a group homomorphism with finite kernel.
It can be represented with rational maps.
The *degree* of a (separable) isogeny is the size of it kernel.

Elliptic curves and their isogenies

Definition (Isogeny)

Let E_1, E_2 be two elliptic curves over $\mathbb{F}_q$.
An isogeny $\varphi : E_1 \to E_2$ is a group homomorphism with finite kernel.
It can be represented with rational maps.
The *degree* of a (separable) isogeny is the size of it kernel.

Example

Over $\mathbb{F}_5$, we take :

$$\begin{cases} E_1 & : \quad y^2 = x^3 + 1 \\ E_2 & : \quad y^2 = x^3 + 2 \end{cases}$$

Elliptic curves and their isogenies

Definition (Isogeny)

Let E_1, E_2 be two elliptic curves over $\mathbb{F}_q$.
An isogeny $\varphi : E_1 \to E_2$ is a group homomorphism with finite kernel.
It can be represented with rational maps.
The *degree* of a (separable) isogeny is the size of it kernel.

Example

Over $\mathbb{F}_5$, we take :

$$\begin{cases} E_1 & : \quad y^2 = x^3 + 1 \\ E_2 & : \quad y^2 = x^3 + 2 \end{cases}$$

We can consider the isogeny $\varphi : E_1 \to E_2$ given by the map

$$\varphi : (x, y) \mapsto \left(\frac{x^2 + x - 2}{x + 1}, \frac{x^2 + 2x - 2}{x^2 + 2x + 1} y \right)$$

Elliptic curves and their isogenies

Definition (Isogeny)

Let E_1, E_2 be two elliptic curves over $\mathbb{F}_q$.
An isogeny $\varphi : E_1 \to E_2$ is a group homomorphism with finite kernel.
It can be represented with rational maps.
The *degree* of a (separable) isogeny is the size of it kernel.

Example

Over $\mathbb{F}_5$, we take :

$$\begin{cases} E_1 & : \quad y^2 = x^3 + 1 \\ E_2 & : \quad y^2 = x^3 + 2 \end{cases}$$

We can consider the isogeny $\varphi : E_1 \to E_2$ given by the map

$$\varphi : (x, y) \mapsto \left(\frac{x^2 + x - 2}{x + 1}, \frac{x^2 + 2x - 2}{x^2 + 2x + 1} y \right)$$

The kernel of φ is $\{(4, 0), \infty\} \leftrightsquigarrow \deg(\varphi) = 2$.

Isogeny representations

Definition (Isogeny representation)

A *representation* for $\varphi : E_1 \to E_2$ is any data associated to an algorithm $\mathcal{A}$ that, given P, computes $\varphi(P)$.

Isogeny representations

Definition (Isogeny representation)

A *representation* for $\varphi : E_1 \to E_2$ is any data associated to an algorithm $\mathcal{A}$ that, given P, computes $\varphi(P)$.
A representation is said *efficient* if $\mathcal{A}$ runs in polynomial time with polynomial memory access.

Isogeny representations

Definition (Isogeny representation)

A *representation* for $\varphi : E_1 \to E_2$ is any data associated to an algorithm $\mathcal{A}$ that, given P, computes $\varphi(P)$.
A representation is said *efficient* if $\mathcal{A}$ runs in polynomial time with polynomial memory access.

Being efficient is not an intrinsic property !
Efficiency can depend on :

- The degree of φ,
- The height of the field extension involved,
- What data is available to us
- The co/domain curves having special properties.

Isogeny representations

Definition (Isogeny representation)

A *representation* for $\varphi : E_1 \to E_2$ is any data associated to an algorithm $\mathcal{A}$ that, given P, computes $\varphi(P)$.
A representation is said *efficient* if $\mathcal{A}$ runs in polynomial time with polynomial memory access.

Being efficient is not an intrinsic property !
Efficiency can depend on :

- The degree of φ,
- The height of the field extension involved,
- What data is available to us
- The co/domain curves having special properties.

[Robert24] : **Damien Robert**, *On the efficient representation of isogenies*, eprint : 2024/1071

1.1 : The Rational maps representation

Rational maps representation (example)

Over $\mathbb{F}_5$, we take :

$$\begin{cases} E_1 & : \quad y^2 = x^3 + 1 \\ E_2 & : \quad y^2 = x^3 + 2 \end{cases}$$

We can consider the isogeny $\varphi : E_1 \to E_2$ given by the map

$$\varphi : (x, y) \mapsto \left(\frac{x^2 + x - 2}{x + 1}, y \frac{x^2 + 2x - 2}{x^2 + 2x + 1} \right)$$

1.1 : The Rational maps representation

Rational maps representation (example)

Over $\mathbb{F}_5$, we take :

$$\begin{cases} E_1 & : \quad y^2 = x^3 + 1 \\ E_2 & : \quad y^2 = x^3 + 2 \end{cases}$$

We can consider the isogeny $\varphi : E_1 \to E_2$ given by the map

$$\varphi : (x, y) \mapsto \left(\frac{x^2 + x - 2}{x + 1}, y \frac{x^2 + 2x - 2}{x^2 + 2x + 1} \right)$$

Properties of the representation

- Evaluation is completely explicit
- The degree of the polynomials grows like $O(\deg(\varphi))$.
  $\rightsquigarrow$ Impracticable (*a priori*) for isogenies of cryptographic size ($\geq 2^{128}$).

1.1 : The Rational maps representation

Rational maps representation (example)

Over $\mathbb{F}_5$, we take :

$$\begin{cases} E_1 & : \quad y^2 = x^3 + 1 \\ E_2 & : \quad y^2 = x^3 + 2 \end{cases}$$

We can consider the isogeny $\varphi : E_1 \to E_2$ given by the map

$$\varphi : (x, y) \mapsto \left(\frac{x^2 + x - 2}{x + 1}, y \frac{x^2 + 2x - 2}{x^2 + 2x + 1} \right)$$

Properties of the representation

- Evaluation is completely explicit
- The degree of the polynomials grows like $O(\deg(\varphi))$.
  $\rightsquigarrow$ Impracticable (*a priori*) for isogenies of cryptographic size ($\geq 2^{128}$).

But factoring φ into smaller pieces $\rightsquigarrow$ efficient for smooth-degree isogenies !

1.2 : The kernel representation

Definition (n-torsion group)

Let n be a positive integer. The n-torsion group of E is defined as

$$E[n] = \left\{ P \in \overline{\mathbb{F}}_p, \quad nP = \infty \right\}$$

1.2 : The kernel representation

Definition (n-torsion group)

Let n be a positive integer. The n-torsion group of E is defined as

$$E[n] = \left\{ P \in \overline{\mathbb{F}}_p, \quad nP = \infty \right\}$$

If $\gcd(n, p) = 1$, then $E[n] \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

1.2 : The kernel representation

Definition (n-torsion group)

Let n be a positive integer. The n-torsion group of E is defined as

$$E[n] = \left\{ P \in \overline{\mathbb{F}}_p, \quad nP = \infty \right\}$$

If $\gcd(n, p) = 1$, then $E[n] \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.
Furthermore, for a prime ℓ, $E[\ell]$ contains $\ell + 1$ distinct cyclic subgroups.

1.2 : The kernel representation

Definition (n-torsion group)

Let n be a positive integer. The n-torsion group of E is defined as

$$E[n] = \left\{ P \in \overline{\mathbb{F}}_p, \quad nP = \infty \right\}$$

If $\gcd(n, p) = 1$, then $E[n] \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.
Furthermore, for a prime ℓ, $E[\ell]$ contains $\ell + 1$ distinct cyclic subgroups.

Theorem

Let E be an elliptic curve and ℓ a prime. There is a 1-to-1 correspondence

$$\left\{ \begin{array}{c} \text{Cyclic subgroups} \\ \text{of } E[\ell] \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{Isogenies of degree } \ell \\ \text{emanating from } E \end{array} \right\}$$

1.2 : The kernel representation

Definition (n-torsion group)

Let n be a positive integer. The n-torsion group of E is defined as

$$E[n] = \left\{ P \in \overline{\mathbb{F}}_p, \quad nP = \infty \right\}$$

If $\gcd(n, p) = 1$, then $E[n] \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.
Furthermore, for a prime ℓ, $E[\ell]$ contains $\ell + 1$ distinct cyclic subgroups.

Theorem

Let E be an elliptic curve and ℓ a prime. There is a 1-to-1 correspondence

$$\left\{ \begin{array}{c} \text{Cyclic subgroups} \\ \text{of } E[\ell] \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{Isogenies of degree } \ell \\ \text{emanating from } E \end{array} \right\}$$

$$\{\infty\} \longrightarrow \langle P \rangle \longrightarrow E \xrightarrow{\varphi} E/\langle P \rangle \longrightarrow \{\infty\}$$

1.2 : The kernel representation

Kernel representation

We can represent $\varphi : E_1 \to E_2$ with degree n just with $P \in E_1[n]$.
The evaluation algorithm involves the Vélu's formulas.

1.2 : The kernel representation

Kernel representation

We can represent $\varphi : E_1 \to E_2$ with degree n just with $P \in E_1[n]$.
The evaluation algorithm involves the Vélu's formulas.

Properties of the representation

- $\mathrm{ord}(P)$ doesn't have to be smooth (*a priori*...)
- Allows for easy isogeny sampling
- Very compact

1.2 : The kernel representation

Kernel representation

We can represent $\varphi : E_1 \to E_2$ with degree n just with $P \in E_1[n]$.
The evaluation algorithm involves the Vélu's formulas.

Properties of the representation

- $\mathrm{ord}(P)$ doesn't have to be smooth (*a priori*...)
- Allows for easy isogeny sampling
- Very compact

Efficient only if $E[n]$ is defined over a small field extension
$\rightsquigarrow$ Imposes $n \mid (p+1)^2$.
Evaluation requires translating back to rational maps
$\rightsquigarrow$ n needs to be smooth, in the end

ℓ-isogeny graphs

$$\text{Vertices : } \left\{ \begin{array}{c} \text{Isomorphism classes} \\ \text{of supersingular} \\ \text{elliptic curves} \end{array} \right\}, \quad \text{Edges : } \left\{ \begin{array}{c} \ell\text{-isogenies} \\ \text{between the} \\ \text{curves} \end{array} \right\}$$

ℓ-isogeny graphs

Vertices : $\left\{ \begin{array}{c} \text{Isomorphism classes} \\ \text{of supersingular} \\ \text{elliptic curves} \end{array} \right\}$, Edges : $\left\{ \begin{array}{c} \ell\text{-isogenies} \\ \text{between the} \\ \text{curves} \end{array} \right\}$

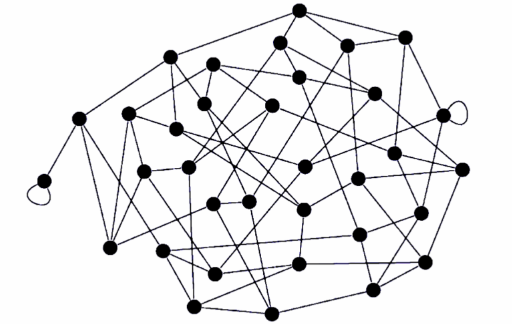


Figure: A representation of a supersingular 3-isogenies graph

ℓ-isogeny graphs

Vertices : $\left\{ \begin{array}{c} \text{Isomorphism classes} \\ \text{of supersingular} \\ \text{elliptic curves} \end{array} \right\}$, Edges : $\left\{ \begin{array}{c} \ell\text{-isogenies} \\ \text{between the} \\ \text{curves} \end{array} \right\}$

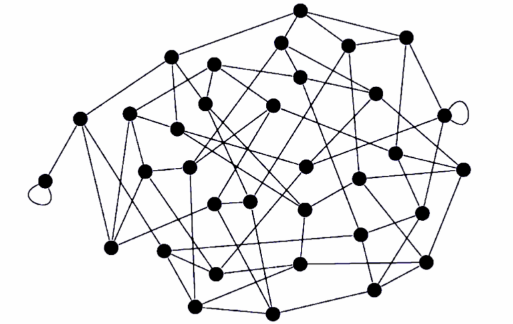


Figure: A representation of a supersingular 3-isogenies graph

- Isogeny graphs are connex and contain $\approx p/12$ vertices,
- The ℓ-isogeny graph is $(\ell + 1)$-regular,
- Those graphs are Ramanujan.

Isogenies hard problems

Isogeny Problem

Given two isogenous curves E_1 and E_2,
find an efficient representation of an isogeny $\varphi : E_1 \to E_2$.

ℓ-Isogeny Path Problem

Given two isogenous curves E_1 and E_2,
find an efficient representation of an isogeny $\varphi : E_1 \to E_2$ with degree ℓ^e.

Isogenies hard problems

Isogeny Problem

Given two isogenous curves E_1 and E_2,
find an efficient representation of an isogeny $\varphi : E_1 \to E_2$.

ℓ-Isogeny Path Problem

Given two isogenous curves E_1 and E_2,
find an efficient representation of an isogeny $\varphi : E_1 \to E_2$ with degree ℓ^e.

No sub-expomential time algorithm for those problems, even with access to a quantum computer.

Act II – Modern representations

Act II – The Quaternion and HD representations

Deuring, KLPT and Kani diagrams

New results

Using the quaternion representation, we can prove :

Theorem

The ℓ-isogeny path problem between E_1 and E_2 can be solved in polynomial time, assuming we know $\mathrm{End}(E_1)$, $\mathrm{End}(E_2)$.

New results

Using the quaternion representation, we can prove :

Theorem

The ℓ-isogeny path problem between E_1 and E_2 can be solved in polynomial time, assuming we know $\mathrm{End}(E_1)$, $\mathrm{End}(E_2)$.

Using the HD representation, we can prove :

Theorem

An isogeny $\varphi : E_1 \to E_2$ with non-smooth degree can be efficiently represented, assuming we know $\varphi(E_1[m])$ for m big enough.

Quaternion algebras and orders

Definition (The quaternion algebra ramified at p and ∞)

We will make use of the quaternion algebra $B_{p,\infty}$ defined as :

$$B_{p,\infty} = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + k\mathbb{Q}$$

with $i^2 = -1$, $j^2 = -p$, $k := ij = -ji$.

Quaternion algebras and orders

Definition (The quaternion algebra ramified at p and ∞)

We will make use of the quaternion algebra $B_{p,\infty}$ defined as :

$$B_{p,\infty} = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + k\mathbb{Q}$$

with $i^2 = -1$, $j^2 = -p$, $k := ij = -ji$.

We can define "rings of integers" for this algebra :

Quaternion algebras and orders

Definition (The quaternion algebra ramified at p and ∞)

We will make use of the quaternion algebra $B_{p,\infty}$ defined as :

$$B_{p,\infty} = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + k\mathbb{Q}$$

with $i^2 = -1$, $j^2 = -p$, $k := ij = -ji$.

We can define “rings of integers” for this algebra :

Definition (Order of an algebra)

Quaternion algebras and orders

Definition (The quaternion algebra ramified at p and ∞)

We will make use of the quaternion algebra $B_{p,\infty}$ defined as :

$$B_{p,\infty} = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + k\mathbb{Q}$$

with $i^2 = -1$, $j^2 = -p$, $k := ij = -ji$.

We can define “rings of integers” for this algebra :

Definition (Order of an algebra)

An order $\mathcal{O}$ of $B_{p,\infty}$ is a full-rank lattice in B that is also a ring.

Quaternion algebras and orders

Definition (The quaternion algebra ramified at p and ∞)

We will make use of the quaternion algebra $B_{p,\infty}$ defined as :

$$B_{p,\infty} = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + k\mathbb{Q}$$

with $i^2 = -1$, $j^2 = -p$, $k := ij = -ji$.

We can define "rings of integers" for this algebra :

Definition (Order of an algebra)

An order $\mathcal{O}$ of $B_{p,\infty}$ is a full-rank lattice in B that is also a ring.
An order is called *maximal* if not contained in any other order.

Quaternion algebras and orders

Definition (The quaternion algebra ramified at p and ∞)

We will make use of the quaternion algebra $B_{p,\infty}$ defined as :

$$B_{p,\infty} = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + k\mathbb{Q}$$

with $i^2 = -1$, $j^2 = -p$, $k := ij = -ji$.

We can define "rings of integers" for this algebra :

Definition (Order of an algebra)

An order $\mathcal{O}$ of $B_{p,\infty}$ is a full-rank lattice in B that is also a ring.
An order is called *maximal* if not contained in any other order.

Example

$\mathcal{O} = \mathbb{Z} + i\mathbb{Z} + j\mathbb{Z} + k\mathbb{Z}$ is an order.

Quaternion algebras and orders

Definition (The quaternion algebra ramified at p and ∞)

We will make use of the quaternion algebra $B_{p,\infty}$ defined as :

$$B_{p,\infty} = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + k\mathbb{Q}$$

with $i^2 = -1$, $j^2 = -p$, $k := ij = -ji$.

We can define “rings of integers” for this algebra :

Definition (Order of an algebra)

An order $\mathcal{O}$ of $B_{p,\infty}$ is a full-rank lattice in B that is also a ring.
An order is called *maximal* if not contained in any other order.

Example

$\mathcal{O} = \mathbb{Z} + i\mathbb{Z} + j\mathbb{Z} + k\mathbb{Z}$ is an order.
$\mathcal{O}_0 = \mathbb{Z} + i\mathbb{Z} + \frac{i+j}{2}\mathbb{Z} + \frac{1+k}{2}\mathbb{Z}$ is a maximal order.

The Deuring Correspondence in one slide

Theorem (Deuring)

$$\left\{ \begin{array}{c} \text{Isomorphism classes of} \\ \text{(supersingular) elliptic curves} \\ \text{over } \mathbb{F}_{p^2} \text{ and their isogenies} \end{array} \right\} \overset{\text{2-to-1}}{\longleftrightarrow} \left\{ \begin{array}{c} \text{Maximal orders of } B_{p,\infty} \\ \text{and their connecting ideals} \end{array} \right\}$$

The Deuring Correspondence in one slide

Theorem (Deuring)

$$\left\{ \begin{array}{c} \text{Isomorphism classes of} \\ \text{(supersingular) elliptic curves} \\ \text{over } \mathbb{F}_{p^2} \text{ and their isogenies} \end{array} \right\} \overset{\text{2-to-1}}{\longleftrightarrow} \left\{ \begin{array}{c} \text{Maximal orders of } B_{p,\infty} \\ \text{and their connecting ideals} \end{array} \right\}$$

The canonical example

Take $E_0 : y^2 = x^3 + x$ over $\mathbb{F}_{p^2}$, with $p = 3 \mod 4$.
Then, we have

$$\begin{array}{ccc} \mathrm{End}(E_0) & = & \mathbb{Z} + \iota\mathbb{Z} + \frac{\iota+\pi}{2}\mathbb{Z} + \frac{1+\pi\iota}{2}\mathbb{Z} \\ \wr\| & & \\ \mathcal{O}_0 & = & \mathbb{Z} + i\mathbb{Z} + \frac{i+j}{2}\mathbb{Z} + \frac{1+k}{2}\mathbb{Z} \end{array}$$

Translating the ℓ-isogeny path problem

The ℓ-isogeny path problem

Let E_1, E_2 be two elliptic curves over $\mathbb{F}_{p^2}$. Let ℓ be a small prime.

Compute an isogeny $\varphi : E_1 \to E_2$ of degree ℓ^e.

$$E_1 \xrightarrow{\varphi} E_2$$

The quaternion ℓ-isogeny path problem

Let $\mathcal{O}_1, \mathcal{O}_2$ be two maximal orders in the quaternion algebra $B_{p,\infty}$.

Compute an ideal $I : \mathcal{O}_1 \to \mathcal{O}_2$ of norm ℓ^e.

$$\mathcal{O}_1 \xrightarrow{I} \mathcal{O}_2$$

Translating the ℓ-isogeny path problem

The ℓ-isogeny path problem

Let E_1, E_2 be two elliptic curves over $\mathbb{F}_{p^2}$. Let ℓ be a small prime.

Compute an isogeny $\varphi : E_1 \to E_2$ of degree ℓ^e.

$$E_1 \xrightarrow{\varphi} E_2$$

$$\xleftrightarrow{\textbf{Deuring}}$$

The quaternion ℓ-isogeny path problem

Let $\mathcal{O}_1, \mathcal{O}_2$ be two maximal orders in the quaternion algebra $B_{p,\infty}$.

Compute an ideal $I : \mathcal{O}_1 \to \mathcal{O}_2$ of norm ℓ^e.

$$\mathcal{O}_1 \xrightarrow{I} \mathcal{O}_2$$

The translation requires the knowledge of $\mathrm{End}(E_1)$ and $\mathrm{End}(E_2)$.

Quaternions (hard ?) problems

Quaternion Isogeny Problem

Given two maximal orders $\mathcal{O}_1$ and $\mathcal{O}_2$,
find an ideal $I : \mathcal{O}_1 \to \mathcal{O}_2$.

Quaternion ℓ-Isogeny Path Problem

Given two maxima orders $\mathcal{O}_1$ and $\mathcal{O}_2$,
find an ideal $I : \mathcal{O}_1 \to \mathcal{O}_2$ with reduced norm ℓ^e.

Quaternions (hard ?) problems

Quaternion Isogeny Problem

Given two maximal orders $\mathcal{O}_1$ and $\mathcal{O}_2$,
find an ideal $I : \mathcal{O}_1 \to \mathcal{O}_2$.

Quaternion ℓ-Isogeny Path Problem

Given two maxima orders $\mathcal{O}_1$ and $\mathcal{O}_2$,
find an ideal $I : \mathcal{O}_1 \to \mathcal{O}_2$ with reduced norm ℓ^e.

Both problem can be solved in polynomial time :

- The Quaternion Isogeny Problem is straightforward,
- The Quaternion ℓ-Isogeny Path Problem requires the KLPT algorithm.

2.1 : Quaternion representation

The quaternion ideal representation

One can represent an isogeny $\varphi : E_1 \to E_2$ as a connecting quaternion ideal $I : \mathcal{O}_1 \to \mathcal{O}_2$.

Properties of the representation

- The evaluation algorithm is split into two main steps :

$$I \xrightarrow{\text{Ideal-to-Iso}} \ker(\varphi) \xrightarrow{\text{Vélu}} \varphi$$

The evaluation requires translating back to kernel and rational maps
$\rightsquigarrow$ I must have powersmooth norm.

Solving the ℓ-Isogeny Path Problem

Instance of
the problem

Solution of
the problem

Geometric
world

$\boxed{E_1 \quad E_2}$

Solving the ℓ-Isogeny Path Problem

Instance of the problem

Solution of the problem

Geometric world

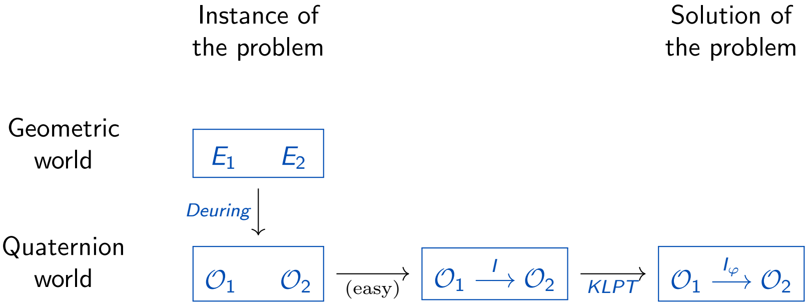
Quaternion world

$$\begin{tikzcd}
\boxed{E_1 \quad E_2} \arrow[d, "\textit{Deuring}"'] \\
\boxed{\mathcal{O}_1 \quad \mathcal{O}_2}
\end{tikzcd}$$

Solving the ℓ-Isogeny Path Problem

$$\begin{tikzcd}
 & \text{Instance of the problem} & & \text{Solution of the problem} \\
\text{Geometric world} & \boxed{E_1 \quad E_2} \arrow[d, "\textit{Deuring}"'] & & \\
\text{Quaternion world} & \boxed{\mathcal{O}_1 \quad \mathcal{O}_2} \arrow[r, "\text{(easy)}"'] & \boxed{\mathcal{O}_1 \xrightarrow{I} \mathcal{O}_2} &
\end{tikzcd}$$

Solving the ℓ-Isogeny Path Problem



Instance of the problem

Solution of the problem

Geometric world

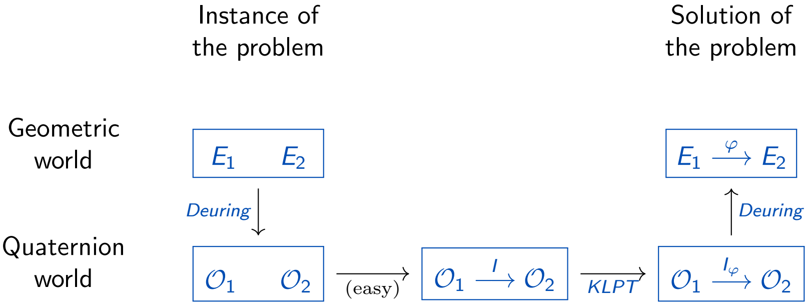
$\boxed{E_1 \quad E_2}$

Deuring

Quaternion world

$\boxed{\mathcal{O}_1 \quad \mathcal{O}_2} \xrightarrow[\text{(easy)}]{} \boxed{\mathcal{O}_1 \xrightarrow{I} \mathcal{O}_2} \xrightarrow[KLPT]{} \boxed{\mathcal{O}_1 \xrightarrow{I_\varphi} \mathcal{O}_2}$

Solving the ℓ-Isogeny Path Problem



Instance of the problem

Solution of the problem

Geometric world

Quaternion world

$E_1 \quad E_2$

$\mathcal{O}_1 \quad \mathcal{O}_2$

$\mathcal{O}_1 \xrightarrow{I} \mathcal{O}_2$

$\mathcal{O}_1 \xrightarrow{I_\varphi} \mathcal{O}_2$

$E_1 \xrightarrow{\varphi} E_2$

Solving the ℓ-Isogeny Path Problem

$$\begin{tikzcd}
 & \text{Instance of the problem} & & \text{Solution of the problem} \\
\text{Geometric world} & \boxed{E_1 \qquad E_2} \arrow[rr, dashed] \arrow[d, "\textit{Deuring}"'] & & \boxed{E_1 \xrightarrow{\varphi} E_2} \\
\text{Quaternion world} & \boxed{\mathcal{O}_1 \qquad \mathcal{O}_2} \arrow[r, "\text{(easy)}"'] & \boxed{\mathcal{O}_1 \xrightarrow{I} \mathcal{O}_2} \arrow[r, "\textit{KLPT}"'] & \boxed{\mathcal{O}_1 \xrightarrow{I_\varphi} \mathcal{O}_2} \arrow[u, "\textit{Deuring}"']
\end{tikzcd}$$

Higher-dimensional isogenies

Higher-dimensional isogenies

Isogeny embeddings

From an isogeny $\varphi : E_1 \to E_2$, we can build an isogeny square.

$$\begin{tikzcd} E_1 \arrow[r, "\varphi"] & E_2 \end{tikzcd}$$

with $\deg(\varphi) = n$,

Higher-dimensional isogenies

Isogeny embeddings

From an isogeny $\varphi : E_1 \to E_2$, we can build an isogeny square.

$$\begin{tikzcd} E_1 \arrow[r, "\varphi"] \arrow[d, "\alpha"'] & E_2 \\ E_3 & \end{tikzcd}$$

with $\deg(\varphi) = n$, $\deg(\alpha) = \ell^e - n$.

Higher-dimensional isogenies

Isogeny embeddings

From an isogeny $\varphi : E_1 \to E_2$, we can build an isogeny square.

$$\begin{tikzcd} E_1 \arrow[r, "\varphi"] \arrow[d, "\alpha"'] & E_2 \arrow[d, "\alpha'"] \\ E_3 \arrow[r, "\varphi'"'] & E_4 \end{tikzcd}$$

with $\deg(\varphi) = n$, $\deg(\alpha) = \ell^e - n$.

Higher-dimensional isogenies

Isogeny embeddings

From an isogeny $\varphi : E_1 \to E_2$, we can build an isogeny square.

$$\begin{tikzcd}
E_1 \arrow[r, "\varphi"] \arrow[d, "\alpha"'] & E_2 \arrow[d, "\alpha'"] \\
E_3 \arrow[r, "\varphi'"'] & E_4
\end{tikzcd}$$

with $\deg(\varphi) = n$, $\deg(\alpha) = \ell^e - n$.

This square defines a 2-dimensional isogeny $\Phi : E_2 \times E_3 \to E_1 \times E_4$:

$$\Phi = \begin{pmatrix} \hat{\varphi} & \hat{\alpha} \\ -\alpha' & \varphi' \end{pmatrix}$$

Higher-dimensional isogenies

Isogeny embeddings

From an isogeny $\varphi : E_1 \to E_2$, we can build an isogeny square.

$$\begin{tikzcd} E_1 \arrow[r, "\varphi"] \arrow[d, "\alpha"'] & E_2 \arrow[d, "\alpha'"] \\ E_3 \arrow[r, "\varphi'"'] & E_4 \end{tikzcd}$$

with $\deg(\varphi) = n$, $\deg(\alpha) = \ell^e - n$.

This square defines a 2-dimensional isogeny $\Phi : E_2 \times E_3 \to E_1 \times E_4$:

$$\Phi = \begin{pmatrix} \hat{\varphi} & \hat{\alpha} \\ -\alpha' & \varphi' \end{pmatrix}$$

It is a (ℓ^e, ℓ^e)-isogeny and its kernel is

$$\ker(\Phi) = \{(\varphi(P), \alpha(P)), \quad P \in E_1[\ell^e]\}$$

Higher-dimensional isogenies

Isogeny embeddings

From an isogeny $\varphi : E_1 \to E_2$, we can build an isogeny square.

$$\begin{tikzcd}
E_1 \arrow[r, "\varphi"] \arrow[d, "\alpha"'] & E_2 \arrow[d, "\alpha'"] \\
E_3 \arrow[r, "\varphi'"'] & E_4
\end{tikzcd}$$

with $\deg(\varphi) = n$, $\deg(\alpha) = \ell^e - n$.

This square defines a 2-dimensional isogeny $\Phi : E_2 \times E_3 \to E_1 \times E_4$:

$$\Phi = \begin{pmatrix} \hat{\varphi} & \hat{\alpha} \\ -\alpha' & \varphi' \end{pmatrix}$$

It is a (ℓ^e, ℓ^e)-isogeny and its kernel is

$$\ker(\Phi) = \{(\varphi(P), \alpha(P)), \quad P \in E_1[\ell^e]\}$$

$\rightsquigarrow$ From the kernel, we evaluate Φ as a chain of (ℓ, ℓ)-isogenies.

2.2 : The HD representation

The HD representation

One can efficiently represent an isogeny $\varphi : E_1 \to E_2$ of arbitrary degree n by embedding it into an isogeny of dimension at most 8, given $\varphi(E_1[m])$ is known, for $m > \sqrt{n}$.

2.2 : The HD representation

The HD representation

One can efficiently represent an isogeny $\varphi : E_1 \to E_2$ of arbitrary degree n by embedding it into an isogeny of dimension at most 8, given $\varphi(E_1[m])$ is known, for $m > \sqrt{n}$.

Properties of the representation

- Efficiency highly depends on the context,
- The evaluation algorithm computes $\hat{\varphi}(P)$ as the first component of

$$\Phi(P, 0) = \begin{pmatrix} \hat{\varphi} & \hat{\alpha} \\ -\alpha' & \varphi' \end{pmatrix} (P, 0)^t = (\hat{\varphi}(P), -\alpha'(P))^t$$

Then, we easily "reverse" $\hat{\varphi}$ to obtain φ. $\rightsquigarrow$ We never explicitely use the rational maps defining φ !

Act III – Recent representations

Act III – HD-quaternions and Hermitian modules representations

IKO, GSS, KLPT² and $\otimes$-MIKE

Abelian varieties

Elliptic curves are abelian varieties *of dimension 1*.
What about abelian varieties in dimensions 2 ?

Abelian varieties

Elliptic curves are abelian varieties *of dimension 1*.
What about abelian varieties in dimensions 2 ?

Funny Names

- $\dim = 1$: Supersingular elliptic curves
- $\dim = 2$: Superspecial Principally Polarised Abelian Surface

Abelian varieties

Elliptic curves are abelian varieties *of dimension 1*.
What about abelian varieties in dimensions 2 ?

Funny Names

- $\dim = 1$: Supersingular elliptic curves
- $\dim = 2$: Superspecial Principally Polarised Abelian Surface

The two flavors of PPAS

A PPAS is either :

- $A = E_1 \times E_2$, where both curves are supersingular,
- $A = \mathrm{Jac}(H)$, where H is an hyperelliptic curve of genus 2.

Abelian varieties

Elliptic curves are abelian varieties *of dimension 1*.
What about abelian varieties in dimensions 2 ?

Funny Names

- $\dim = 1$: Supersingular elliptic curves
- $\dim = 2$: Superspecial Principally Polarised Abelian Surface

The two flavors of PPAS

A PPAS is either :

- $A = E_1 \times E_2$, where both curves are supersingular,
- $A = \mathrm{Jac}(H)$, where H is an hyperelliptic curve of genus 2.

Polarisations

A polarisation on A is a special isogeny $\lambda : A \to A^\vee$.
When λ is an isomorphism, we say it is principal.

Overview of KLPT^2

	Instance of the problem	Solution of the problem
Geometric world	$\boxed{(A_1, \lambda_1) \qquad (A_2, \lambda_2)}$	$\boxed{(A_1, \lambda_1) \xrightarrow{\Phi} (A_2, \lambda_2)}$

- (A_1, λ_1) and (A_2, λ_2) are *principally polarized superspecial abelian surfaces*.

Overview of KLPT^2

$$\begin{tikzcd} & \text{Instance of the problem} & \text{Solution of the problem} \\ \text{Geometric world} & \boxed{(A_1, \lambda_1) \qquad (A_2, \lambda_2)} \arrow[d, "IKO{,}GSS"'] & \boxed{(A_1, \lambda_1) \xrightarrow{\Phi} (A_2, \lambda_2)} \\ \text{Quaternion world} & \boxed{g_1 \qquad g_2} & \end{tikzcd}$$

- (A_1, λ_1) and (A_2, λ_2) are *principally polarized superspecial abelian surfaces*.
- g_1, g_2 are matrices encoding the abelian surfaces.

[IKO] : **Ibukiyama-Katsura-Oort**, *Supersingular curves of genus two and class numbers*

[GSS] : **Gaudry-Soumier-Spaenlehauer**, *Computing Isomorphisms between products of supersingular elliptic curves*, eprint 2025/136

Overview of KLPT^2

$$\begin{tikzcd}
 & \text{Instance of the problem} & \text{Solution of the problem} \\
\text{Geometric world} & \boxed{(A_1, \lambda_1) \qquad (A_2, \lambda_2)} \arrow[d, "IKO, GSS"'] & \boxed{(A_1, \lambda_1) \xrightarrow{\Phi} (A_2, \lambda_2)} \\
\text{Quaternion world} & \boxed{g_1 \qquad g_2} \arrow[r, "\text{KLPT}^2"'] & \boxed{g_1 \xrightarrow{\gamma} g_2}
\end{tikzcd}$$

- (A_1, λ_1) and (A_2, λ_2) are *principally polarized superspecial abelian surfaces*.
- g_1, g_2 are matrices encoding the abelian surfaces.
- γ is a matrix encoding an isogeny.

[IKO] : **Ibukiyama-Katsura-Oort**, *Supersingular curves of genus two and class numbers*

[GSS] : **Gaudry-Soumier-Spaenlehauer**, *Computing Isomorphisms between products of supersingular elliptic curves*, eprint 2025/136

Overview of KLPT^2

$$\begin{tikzcd}
 & \text{Instance of the problem} & \text{Solution of the problem} \\
\text{Geometric world} & \boxed{(A_1, \lambda_1) \qquad (A_2, \lambda_2)} \arrow[d, "IKO, GSS"'] & \boxed{(A_1, \lambda_1) \xrightarrow{\Phi} (A_2, \lambda_2)} \\
\text{Quaternion world} & \boxed{g_1 \qquad g_2} \arrow[r, "\text{KLPT}^2"'] & \boxed{g_1 \xrightarrow{\gamma} g_2} \arrow[u, "IKO"']
\end{tikzcd}$$

- (A_1, λ_1) and (A_2, λ_2) are *principally polarized superspecial abelian surfaces*.
- g_1, g_2 are matrices encoding the abelian surfaces.
- γ is a matrix encoding an isogeny.

[IKO] : **Ibukiyama-Katsura-Oort**, *Supersingular curves of genus two and class numbers*

[GSS] : **Gaudry-Soumier-Spaenlehauer**, *Computing Isomorphisms between products of supersingular elliptic curves*, eprint 2025/136

Overview of KLPT^2

$$\begin{tikzcd}
 & \text{Instance of the problem} & \text{Solution of the problem} \\
\text{Geometric world} & \boxed{(A_1, \lambda_1) \qquad (A_2, \lambda_2)} \arrow[r, dashed] \arrow[d, "IKO{,}GSS"'] & \boxed{(A_1, \lambda_1) \xrightarrow{\Phi} (A_2, \lambda_2)} \\
\text{Quaternion world} & \boxed{g_1 \qquad g_2} \arrow[r, "\mathrm{KLPT}^2"'] & \boxed{g_1 \xrightarrow{\gamma} g_2} \arrow[u, "IKO"']
\end{tikzcd}$$

- (A_1, λ_1) and (A_2, λ_2) are *principally polarized superspecial abelian surfaces*.
- g_1, g_2 are matrices encoding the abelian surfaces.
- γ is a matrix encoding an isogeny.

[IKO] : **Ibukiyama-Katsura-Oort**, *Supersingular curves of genus two and class numbers*

[GSS] : **Gaudry-Soumier-Spaenlehauer**, *Computing Isomorphisms between products of supersingular elliptic curves*, eprint 2025/136

3.1 : The HD-quaternion representation

The HD-quaternion representation

One can represent a 2D isogeny $\Phi : (A_1, \lambda_1) \to (A_2, \lambda_2)$ as a connecting matrix $\gamma : g_1 \to g_2$, with :

$$\gamma \in \mathrm{M}_2(\mathcal{O}_0), \;\; \mathcal{O}_0 \simeq \mathrm{End}(E_0)$$

3.1 : The HD-quaternion representation

The HD-quaternion representation

One can represent a 2D isogeny $\Phi : (A_1, \lambda_1) \to (A_2, \lambda_2)$ as a connecting matrix $\gamma : g_1 \to g_2$, with :

$$\gamma \in \mathrm{M}_2(\mathcal{O}_0), \quad \mathcal{O}_0 \simeq \mathrm{End}(E_0)$$

Properties of the representation

- The evaluation algorithm requires algorithms developped in the KLPT² paper.
- Allows the generalisation of classic results in dimension 1
- Cannot be extended to dim 4 or 8 so readily.

[KLPT2] : **Castryck, Decru, Kutas, Laval, Petit, Ti**, *KLPT²: Algebraic pathfinding in dimension two and applications*, eprint : 2025/372

3.1 : The HD-quaternion representation

The HD-quaternion representation

One can represent a 2D isogeny $\Phi : (A_1, \lambda_1) \rightarrow (A_2, \lambda_2)$ as a connecting matrix $\gamma : g_1 \rightarrow g_2$, with :

$$\gamma \in \mathrm{M}_2(\mathcal{O}_0), \quad \mathcal{O}_0 \simeq \mathrm{End}(E_0)$$

Properties of the representation

- The evaluation algorithm requires algorithms developped in the KLPT² paper.
- Allows the generalisation of classic results in dimension 1
- Cannot be extended to dim 4 or 8 so readily.

Research for efficient PPAS/quaternion translations is a rather new subfield.
A lot of improvements to expect $\leftrightsquigarrow$ Robert's Hermitian modules ?

[KLPT2] : **Castryck, Decru, Kutas, Laval, Petit, Ti**, *KLPT²: Algebraic pathfinding in dimension two and applications*, eprint : 2025/372

Act IV – Abel Jugendtraum representation

Act IV – A Drinfeld module representation ?

Drinfeld modules, Wesolowski's algorithm, Hope & Dreams

Motivation and history

Drinfeld modules in one sentence

Drinfeld modules are to function fields what elliptic curves are to number fields.

E is a $\mathbb{Z}$-module $\longrightarrow$ φ is a $\mathbb{F}_p[T]$-module

Motivation and history

Drinfeld modules in one sentence

Drinfeld modules are to function fields what elliptic curves are to number fields.

E is a $\mathbb{Z}$-module $\longrightarrow$ φ is a $\mathbb{F}_p[T]$-module

- Motivations :

Motivation and history

Drinfeld modules in one sentence

Drinfeld modules are to function fields what elliptic curves are to number fields.

E is a $\mathbb{Z}$-module $\longrightarrow$ φ is a $\mathbb{F}_p[T]$-module

- Motivations :
  - Already extensively studied in mathematics

Motivation and history

Drinfeld modules in one sentence

Drinfeld modules are to function fields what elliptic curves are to number fields.

$$E \text{ is a } \mathbb{Z}\text{-module} \longrightarrow \varphi \text{ is a } \mathbb{F}_p[T]\text{-module}$$

- Motivations :
  - Already extensively studied in mathematics
  - Most hard problem for elliptic curves are easy for Drinfeld modules

Motivation and history

Drinfeld modules in one sentence

Drinfeld modules are to function fields what elliptic curves are to number fields.

$$E \text{ is a } \mathbb{Z}\text{-module} \longrightarrow \varphi \text{ is a } \mathbb{F}_p[T]\text{-module}$$

- Motivations :
  - Already extensively studied in mathematics
  - Most hard problem for elliptic curves are easy for Drinfeld modules
  - A lot a functions are now implemented in Sage

Motivation and history

Drinfeld modules in one sentence

Drinfeld modules are to function fields what elliptic curves are to number fields.

E is a $\mathbb{Z}$-module $\longrightarrow$ φ is a $\mathbb{F}_p[T]$-module

- Motivations :
  - Already extensively studied in mathematics
  - Most hard problem for elliptic curves are easy for Drinfeld modules
  - A lot a functions are now implemented in Sage
- Goals :

Motivation and history

Drinfeld modules in one sentence

Drinfeld modules are to function fields what elliptic curves are to number fields.

$$E \text{ is a } \mathbb{Z}\text{-module} \longrightarrow \varphi \text{ is a } \mathbb{F}_p[T]\text{-module}$$

- Motivations :
  - Already extensively studied in mathematics
  - Most hard problem for elliptic curves are easy for Drinfeld modules
  - A lot a functions are now implemented in Sage
- Goals :
  - Identify (potentially ad-hoc) hard problems in the Drinfeld world (pSIDH)

Motivation and history

Drinfeld modules in one sentence

Drinfeld modules are to function fields what elliptic curves are to number fields.

$$E \text{ is a } \mathbb{Z}\text{-module} \longrightarrow \varphi \text{ is a } \mathbb{F}_p[T]\text{-module}$$

- Motivations :
  - Already extensively studied in mathematics
  - Most hard problem for elliptic curves are easy for Drinfeld modules
  - A lot a functions are now implemented in Sage

- Goals :
  - Identify (potentially ad-hoc) hard problems in the Drinfeld world (pSIDH)
  - Build an ad-hoc correspondance EC world $\longleftrightarrow$ Drinfeld world (SQIsign)

Motivation and history

Drinfeld modules in one sentence

Drinfeld modules are to function fields what elliptic curves are to number fields.

$$E \text{ is a } \mathbb{Z}\text{-module} \longrightarrow \varphi \text{ is a } \mathbb{F}_p[T]\text{-module}$$

- Motivations :
  - Already extensively studied in mathematics
  - Most hard problem for elliptic curves are easy for Drinfeld modules
  - A lot a functions are now implemented in Sage

- Goals :
  - Identify (potentially ad-hoc) hard problems in the Drinfeld world (pSIDH)
  - Build an ad-hoc correspondance EC world $\longleftrightarrow$ Drinfeld world (SQIsign)

- What we **don't** try to do :

Motivation and history

Drinfeld modules in one sentence

Drinfeld modules are to function fields what elliptic curves are to number fields.

$$E \text{ is a } \mathbb{Z}\text{-module} \longrightarrow \varphi \text{ is a } \mathbb{F}_p[T]\text{-module}$$

- Motivations :
  - Already extensively studied in mathematics
  - Most hard problem for elliptic curves are easy for Drinfeld modules
  - A lot a functions are now implemented in Sage

- Goals :
  - Identify (potentially ad-hoc) hard problems in the Drinfeld world (pSIDH)
  - Build an ad-hoc correspondance EC world $\longleftrightarrow$ Drinfeld world (SQIsign)

- What we **don't** try to do :
  - Develop the general theory of Drinfeld modules $\leftrightsquigarrow$ way too hard

Motivation and history

- Drinfeld modules in cryptography

Motivation and history

- Drinfeld modules in cryptography
  - 2001 : Scanlon shows that Drinfeld-DLOG schemes are insecure.

Motivation and history

- Drinfeld modules in cryptography
  - 2001 : Scanlon shows that Drinfeld-DLOG schemes are insecure.
  - 2019 : Joux & Narayanan show that the Drinfeld variants of SIDH and CSIDH are insecure.

Motivation and history

- Drinfeld modules in cryptography
  - 2001 : Scanlon shows that Drinfeld-DLOG schemes are insecure.
  - 2019 : Joux & Narayanan show that the Drinfeld variants of SIDH and CSIDH are insecure.
  - 2022 : Leudière & Spaenlehauer propose a KEM based on Drinfeld modules.

Motivation and history

- Drinfeld modules in cryptography
  - 2001 : Scanlon shows that Drinfeld-DLOG schemes are insecure.
  - 2019 : Joux & Narayanan show that the Drinfeld variants of SIDH and CSIDH are insecure.
  - 2022 : Leudière & Spaenlehauer propose a KEM based on Drinfeld modules.
  - 2022 : Wesolowski breaks [LS22] and shows that the Drinfeld Isogeny Path Problem is easy.

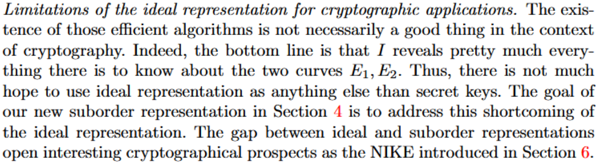
Motivation and history

- Drinfeld modules in cryptography
  - 2001 : Scanlon shows that Drinfeld-DLOG schemes are insecure.
  - 2019 : Joux & Narayanan show that the Drinfeld variants of SIDH and CSIDH are insecure.
  - 2022 : Leudière & Spaenlehauer propose a KEM based on Drinfeld modules.
  - 2022 : Wesolowski breaks [LS22] and shows that the Drinfeld Isogeny Path Problem is easy.

It doesn't sound good... but

First idea : Learning from pSIDH

First idea : Learning from pSIDH

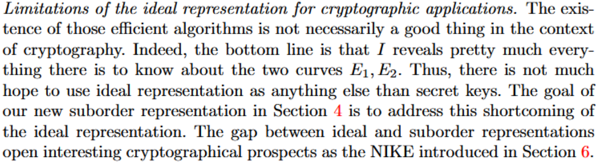


Limitations of the ideal representation for cryptographic applications. The existence of those efficient algorithms is not necessarily a good thing in the context of cryptography. Indeed, the bottom line is that I reveals pretty much everything there is to know about the two curves E_1, E_2. Thus, there is not much hope to use ideal representation as anything else than secret keys. The goal of our new suborder representation in Section 4 is to address this shortcoming of the ideal representation. The gap between ideal and suborder representations open interesting cryptographical prospects as the NIKE introduced in Section 6.

Figure: Section 3.3 of Leroux' pSIDH paper.

- Usual hard problems are easy in the quaternion world

First idea : Learning from pSIDH



Limitations of the ideal representation for cryptographic applications. The existence of those efficient algorithms is not necessarily a good thing in the context of cryptography. Indeed, the bottom line is that I reveals pretty much everything there is to know about the two curves E_1, E_2. Thus, there is not much hope to use ideal representation as anything else than secret keys. The goal of our new suborder representation in Section 4 is to address this shortcoming of the ideal representation. The gap between ideal and suborder representations open interesting cryptographical prospects as the NIKE introduced in Section 6.

Figure: Section 3.3 of Leroux' pSIDH paper.

- Usual hard problems are easy in the quaternion world
- pSIDH $\rightsquigarrow$ Ad-hoc isogeny representation with limited information

Second idea : A Drinfeld variant of SQIsign

Second idea : A Drinfeld variant of SQIsign

Rough idea

- There is an **analogy** between elliptic curves and Drinfeld modules,
  There is **no** equivalence of categories between the two.

Second idea : A Drinfeld variant of SQIsign

Rough idea

- There is an **analogy** between elliptic curves and Drinfeld modules,
  There is **no** equivalence of categories between the two.
- Describe a ”good-enough” correspondance EC world $\longleftrightarrow$ Drinfeld world.

Second idea : A Drinfeld variant of SQIsign

Rough idea

- There is an **analogy** between elliptic curves and Drinfeld modules, There is **no** equivalence of categories between the two.
- Describe a "good-enough" correspondance EC world $\longleftrightarrow$ Drinfeld world.
- Computing the correspondence requires some secret data (*e.g.* an endomorphism ring)

Second idea : A Drinfeld variant of SQIsign

Rough idea

- There is an **analogy** between elliptic curves and Drinfeld modules, There is **no** equivalence of categories between the two.
- Describe a "good-enough" correspondance EC world $\longleftrightarrow$ Drinfeld world.
- Computing the correspondence requires some secret data (*e.g.* an endomorphism ring)
- KLPT is replaced by (an adaptation of) Wesolowski's algorithm.

The mathematics of Drinfeld modules

Choosing an underlying setting

	Generic Drinfeld Modules	Special Drinfeld Modules	Elliptic Curves
Base field			
Base ring			
Prime ideal			
Residue field			
Finite extension			

Choosing an underlying setting

	Generic Drinfeld Modules	Special Drinfeld Modules	Elliptic Curves
Base field			
Base ring	A		
Prime ideal			
Residue field			
Finite extension			

Choosing an underlying setting

	Generic Drinfeld Modules	Special Drinfeld Modules	Elliptic Curves
Base field			
Base ring	A		
Prime ideal	$\mathfrak{p}$		
Residue field			
Finite extension			

Choosing an underlying setting

	Generic Drinfeld Modules	Special Drinfeld Modules	Elliptic Curves
Base field			
Base ring	A		
Prime ideal	$\mathfrak{p}$		
Residue field	$A/\mathfrak{p}$		
Finite extension			

Choosing an underlying setting

	Generic Drinfeld Modules	Special Drinfeld Modules	Elliptic Curves
Base field			
Base ring	A		
Prime ideal	$\mathfrak{p}$		
Residue field	$A/\mathfrak{p}$		
Finite extension	$A/\mathfrak{p} \hookrightarrow K$		

Choosing an underlying setting

	Generic Drinfeld Modules	Special Drinfeld Modules	Elliptic Curves
Base field	$\mathrm{Frac}(A)$		
Base ring	A		
Prime ideal	$\mathfrak{p}$		
Residue field	$A/\mathfrak{p}$		
Finite extension	$A/\mathfrak{p} \hookrightarrow K$		

- $\mathrm{Frac}(A)$ is the function field of some curve over $\mathbb{F}_p$.

Choosing an underlying setting

	Generic Drinfeld Modules	Special Drinfeld Modules	Elliptic Curves
Base field	$\mathrm{Frac}(A)$	$\mathbb{F}_p(T)$	$\mathbb{Q}$
Base ring	A		
Prime ideal	$\mathfrak{p}$		
Residue field	$A/\mathfrak{p}$		
Finite extension	$A/\mathfrak{p} \hookrightarrow K$		

- $\mathrm{Frac}(A)$ is the function field of some curve over $\mathbb{F}_p$.
- $\mathbb{F}_p(T)$ is the function field of $\mathbb{P}^1(\mathbb{F}_p)$.

Choosing an underlying setting

	Generic Drinfeld Modules	Special Drinfeld Modules	Elliptic Curves
Base field	$\mathrm{Frac}(A)$	$\mathbb{F}_p(T)$	$\mathbb{Q}$
Base ring	A	$\mathbb{F}_p[T]$	
Prime ideal	$\mathfrak{p}$		
Residue field	$A/\mathfrak{p}$		
Finite extension	$A/\mathfrak{p} \hookrightarrow K$		

- $\mathrm{Frac}(A)$ is the function field of some curve over $\mathbb{F}_p$.
- $\mathbb{F}_p(T)$ is the function field of $\mathbb{P}^1(\mathbb{F}_p)$.

Choosing an underlying setting

	Generic Drinfeld Modules	Special Drinfeld Modules	Elliptic Curves
Base field	$\mathrm{Frac}(A)$	$\mathbb{F}_p(T)$	$\mathbb{Q}$
Base ring	A	$\mathbb{F}_p[T]$	
Prime ideal	$\mathfrak{p}$	$\langle T - t \rangle$	
Residue field	$A/\mathfrak{p}$		
Finite extension	$A/\mathfrak{p} \hookrightarrow K$		

- $\mathrm{Frac}(A)$ is the function field of some curve over $\mathbb{F}_p$.
- $\mathbb{F}_p(T)$ is the function field of $\mathbb{P}^1(\mathbb{F}_p)$.

Choosing an underlying setting

	Generic Drinfeld Modules	Special Drinfeld Modules	Elliptic Curves
Base field	$\mathrm{Frac}(A)$	$\mathbb{F}_p(T)$	$\mathbb{Q}$
Base ring	A	$\mathbb{F}_p[T]$	
Prime ideal	$\mathfrak{p}$	$\langle T - t\rangle$	
Residue field	$A/\mathfrak{p}$	$\mathbb{F}_p[T]/\langle T - t\rangle \simeq \mathbb{F}_p$	
Finite extension	$A/\mathfrak{p} \hookrightarrow K$		

- $\mathrm{Frac}(A)$ is the function field of some curve over $\mathbb{F}_p$.
- $\mathbb{F}_p(T)$ is the function field of $\mathbb{P}^1(\mathbb{F}_p)$.

Choosing an underlying setting

	Generic Drinfeld Modules	Special Drinfeld Modules	Elliptic Curves
Base field	$\mathrm{Frac}(A)$	$\mathbb{F}_p(T)$	$\mathbb{Q}$
Base ring	A	$\mathbb{F}_p[T]$	
Prime ideal	$\mathfrak{p}$	$\langle T - t \rangle$	
Residue field	$A/\mathfrak{p}$	$\mathbb{F}_p[T]/\langle T - t \rangle \simeq \mathbb{F}_p$	
Finite extension	$A/\mathfrak{p} \hookrightarrow K$	$K \simeq \mathbb{F}_{p^d}$	

- $\mathrm{Frac}(A)$ is the function field of some curve over $\mathbb{F}_p$.
- $\mathbb{F}_p(T)$ is the function field of $\mathbb{P}^1(\mathbb{F}_p)$.

Choosing an underlying setting

	Generic Drinfeld Modules	Special Drinfeld Modules	Elliptic Curves
Base field	$\mathrm{Frac}(A)$	$\mathbb{F}_p(T)$	$\mathbb{Q}$
Base ring	A	$\mathbb{F}_p[T]$	$\mathbb{Z}$
Prime ideal	$\mathfrak{p}$	$\langle T - t\rangle$	
Residue field	$A/\mathfrak{p}$	$\mathbb{F}_p[T]/\langle T - t\rangle \simeq \mathbb{F}_p$	
Finite extension	$A/\mathfrak{p} \hookrightarrow K$	$K \simeq \mathbb{F}_{p^d}$	

- $\mathrm{Frac}(A)$ is the function field of some curve over $\mathbb{F}_p$.
- $\mathbb{F}_p(T)$ is the function field of $\mathbb{P}^1(\mathbb{F}_p)$.

Choosing an underlying setting

	Generic Drinfeld Modules	Special Drinfeld Modules	Elliptic Curves
Base field	$\mathrm{Frac}(A)$	$\mathbb{F}_p(T)$	$\mathbb{Q}$
Base ring	A	$\mathbb{F}_p[T]$	$\mathbb{Z}$
Prime ideal	$\mathfrak{p}$	$\langle T - t \rangle$	$p\mathbb{Z}$
Residue field	$A/\mathfrak{p}$	$\mathbb{F}_p[T]/\langle T - t \rangle \simeq \mathbb{F}_p$	
Finite extension	$A/\mathfrak{p} \hookrightarrow K$	$K \simeq \mathbb{F}_{p^d}$	

- $\mathrm{Frac}(A)$ is the function field of some curve over $\mathbb{F}_p$.
- $\mathbb{F}_p(T)$ is the function field of $\mathbb{P}^1(\mathbb{F}_p)$.

Choosing an underlying setting

	Generic Drinfeld Modules	Special Drinfeld Modules	Elliptic Curves
Base field	$\mathrm{Frac}(A)$	$\mathbb{F}_p(T)$	$\mathbb{Q}$
Base ring	A	$\mathbb{F}_p[T]$	$\mathbb{Z}$
Prime ideal	$\mathfrak{p}$	$\langle T - t \rangle$	$p\mathbb{Z}$
Residue field	$A/\mathfrak{p}$	$\mathbb{F}_p[T]/\langle T - t \rangle \simeq \mathbb{F}_p$	$\mathbb{Z}/p\mathbb{Z} \simeq \mathbb{F}_p$
Finite extension	$A/\mathfrak{p} \hookrightarrow K$	$K \simeq \mathbb{F}_{p^d}$	

- $\mathrm{Frac}(A)$ is the function field of some curve over $\mathbb{F}_p$.
- $\mathbb{F}_p(T)$ is the function field of $\mathbb{P}^1(\mathbb{F}_p)$.

Choosing an underlying setting

	Generic Drinfeld Modules	Special Drinfeld Modules	Elliptic Curves
Base field	$\mathrm{Frac}(A)$	$\mathbb{F}_p(T)$	$\mathbb{Q}$
Base ring	A	$\mathbb{F}_p[T]$	$\mathbb{Z}$
Prime ideal	$\mathfrak{p}$	$\langle T - t \rangle$	$p\mathbb{Z}$
Residue field	$A/\mathfrak{p}$	$\mathbb{F}_p[T]/\langle T - t \rangle \simeq \mathbb{F}_p$	$\mathbb{Z}/p\mathbb{Z} \simeq \mathbb{F}_p$
Finite extension	$A/\mathfrak{p} \hookrightarrow K$	$K \simeq \mathbb{F}_{p^d}$	$K = \mathbb{F}_{p^2}$

- $\mathrm{Frac}(A)$ is the function field of some curve over $\mathbb{F}_p$.
- $\mathbb{F}_p(T)$ is the function field of $\mathbb{P}^1(\mathbb{F}_p)$.

Choosing an underlying setting

	Generic Drinfeld Modules	Special Drinfeld Modules	Elliptic Curves
Base field	$\mathrm{Frac}(A)$	$\mathbb{F}_p(T)$	$\mathbb{Q}$
Base ring	A	$\mathbb{F}_p[T]$	$\mathbb{Z}$
Prime ideal	$\mathfrak{p}$	$\langle T - t \rangle$	$p\mathbb{Z}$
Residue field	$A/\mathfrak{p}$	$\mathbb{F}_p[T]/\langle T - t \rangle \simeq \mathbb{F}_p$	$\mathbb{Z}/p\mathbb{Z} \simeq \mathbb{F}_p$
Finite extension	$A/\mathfrak{p} \hookrightarrow K$	$K \simeq \mathbb{F}_{p^d}$	$K = \mathbb{F}_{p^2}$

- $\mathrm{Frac}(A)$ is the function field of some curve over $\mathbb{F}_p$.
- $\mathbb{F}_p(T)$ is the function field of $\mathbb{P}^1(\mathbb{F}_p)$.

- The prime ideal $\mathfrak{p}$ defines the field of coefficients.
- The degree d defines the extension we are working with.

4.1 : The Drinfeld representation

4.1 : The Drinfeld representation

The Drinfeld representation

TBD

4.1 : The Drinfeld representation

The Drinfeld representation

TBD

Properties of the representation

- Possibly cannot exist.
- Would leverage the analogy between elliptic curves and Drinfeld modules
- Could take advantage of Wesolowski's method for computing Drinfeld isogenies
  $\rightsquigarrow$ Some tools are possibly already there.

Conclusion ?

What do we know about isogeny-based cryptography ?

Elliptic curves and their isogenies are very rich mathematical objects !

- Downsides :
  - Schemes are slow
  - Schemes die when a theorem from 1997 is discovered by cryptographers.
- Upsides :
  - Keys are small
  - There are many different approaches to tackle a specific problem.

Conclusion ?

What do we know about isogeny-based cryptography ?

Elliptic curves and their isogenies are very rich mathematical objects !

- Downsides :
  - Schemes are slow
  - Schemes die when a theorem from 1997 is discovered by cryptographers.
- Upsides :
  - Keys are small
  - There are many different approaches to tackle a specific problem.

Discovering and understanding different isogeny representations :

- Bigger toolbox to build more efficient schemes

Conclusion ?

What do we know about isogeny-based cryptography ?

Elliptic curves and their isogenies are very rich mathematical objects !

- Downsides :
  - Schemes are slow
  - Schemes die when a theorem from 1997 is discovered by cryptographers.
- Upsides :
  - Keys are small
  - There are many different approaches to tackle a specific problem.

Discovering and understanding different isogeny representations :

- Bigger toolbox to build more efficient schemes
- Is required for thorough security assessment

Conclusion ?

What do we know about isogeny-based cryptography ?

Elliptic curves and their isogenies are very rich mathematical objects !

- Downsides :
  - Schemes are slow
  - Schemes die when a theorem from 1997 is discovered by cryptographers.
- Upsides :
  - Keys are small
  - There are many different approaches to tackle a specific problem.

Discovering and understanding different isogeny representations :

- Bigger toolbox to build more efficient schemes
- Is required for thorough security assessment
- Funny and interesting !

Conclusion ?

What do we know about isogeny-based cryptography ?

Elliptic curves and their isogenies are very rich mathematical objects !

- Downsides :
  - Schemes are slow
  - Schemes die when a theorem from 1997 is discovered by cryptographers.
- Upsides :
  - Keys are small
  - There are many different approaches to tackle a specific problem.

Discovering and understanding different isogeny representations :

- Bigger toolbox to build more efficient schemes
- Is required for thorough security assessment
- Funny and interesting !

Thank you for your attention !