An explicit CRS-like action with Drinfeld modules
Séminaire de l’équipe LFANT

Antoine Leudièrê   Pierre-Jean Spaenlehauer

INRIA Nancy-Grand Est

Juin 2022
Tristan and Isolde choose an abelian simply transitive group action $G \times X \to X$, and $x \in X$.

Protocol secure if (among other things) hard to compute $ab \cdot x$ knowing $x, a \cdot x, b \cdot x$.

**Definition (Couveignes, 1996)**

Under those hypotheses, this construction is called a hard homogeneous space.
Tristan and Isolde choose an abelian simply transitive group action $G \times X \to X$, and $x \in X$.

Protocol secure if (among other things) hard to compute $ab \cdot x$ knowing $x, a \cdot x, b \cdot x$.

**Definition (Couveignes, 1996)**

Under those hypotheses, this construction is called a **hard homogeneous space**.
Tristan and Isolde choose an abelian simply transitive group action $G \times X \to X$, and $x \in X$.

Both calculate $ab \cdot x$ (secret key)

Protocol secure if (among other things) hard to compute $ab \cdot x$ knowing $x, a \cdot x, b \cdot x$.

**Definition (Couveignes, 1996)**

Under those hypotheses, this construction is called a *hard homogeneous space*. 
Tristan and Isolde choose an abelian simply transitive group action $G \times X \rightarrow X$, and $x \in X$.

Both calculate $ab \cdot x$ (secret key).

Protocol secure if (among other things) hard to compute $ab \cdot x$ knowing $x, a \cdot x, b \cdot x$.

**Definition (Couveignes, 1996)**

Under those hypotheses, this construction is called a *hard homogeneous space.*
Tristan and Isolde choose an abelian simply transitive group action $G \times X \to X$, and $x \in X$.

Both calculate $ab \cdot x$ (secret key).

Protocol secure if (among other things) hard to compute $ab \cdot x$ knowing $x, a \cdot x, b \cdot x$.

**Definition (Couveignes, 1996)**

Under those hypotheses, this construction is called a *hard homogeneous space*. 
Couveignes (1996) then Rostovstev, Stolbunov (2006) used this action:

**Theorem (Classical result from class field theory)**

Let $E/\mathbb{F}_q$ be some ordinary elliptic curve. Fix $\mathcal{O} = \text{End}_{\mathbb{F}_q}(E)$. Then, $\text{Cl}(\mathcal{O})$ acts simply transitively on the set of $\mathbb{F}_q$-isomorphism classes of elliptic curves defined over $\mathbb{F}_q$ with same endomorphism ring and characteristic polynomial as $E$.

Computation explicit, but slow (De Feo, Kieffer, Smith, 2019).
Couveignes (1996) then Rostovstev, Stolbunov (2006) used this action:

**Theorem (Classical result from class field theory)**

Let $E/F_q$ be some ordinary elliptic curve. Fix $O = \text{End}_{F_q}(E)$.

Then, $\text{Cl}(O)$ acts simply transitively on the set of $\overline{F}_q$-isomorphism classes of elliptic curves defined over $\overline{F}_q$ with same endomorphism ring and characteristic polynomial as $E$.

Computation explicit, but slow (De Feo, Kieffer, Smith, 2019).
What about CSIDH?

CSIDH is way more efficient.
The acting group is the class group of an imaginary quadratic number field.
Group extremely hard to compute (Beullens, Kleinjung, Vercauteren, 2019).
What about CSIDH?

CSIDH is way more efficient.
The acting group is the class group of a imaginary quadratic number field.
Group extremely hard to compute (Beullens, Kleinjung, Vercauteren, 2019).
Idea: work in function fields instead of number fields.

In function fields, Jacobians of imaginary hyperelliptic curves are like class groups of imaginary quadratic number fields in number fields.
Idea: work in function fields instead of number fields.
In function fields, Jacobians of imaginary hyperelliptic curves are like class groups of imaginary quadratic number fields in number fields.
## Analogies (1/2)

<table>
<thead>
<tr>
<th>Number fields</th>
<th>Function fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathbb{Z}$</td>
<td>$\mathbb{F}_q[X]$</td>
</tr>
<tr>
<td>Imaginary quadratic number fields</td>
<td>Imaginary hyperelliptic curves</td>
</tr>
<tr>
<td>Class group (hard computation)</td>
<td>Jacobian (small characteristic: doable computation with Kedlaya’s algorithm)</td>
</tr>
<tr>
<td>Elliptic curves</td>
<td>Drinfeld modules</td>
</tr>
</tbody>
</table>
## Analogies (1/2)

<table>
<thead>
<tr>
<th>Number fields</th>
<th>Function fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \mathbb{Z} )</td>
<td>( \mathbb{F}_q[X] )</td>
</tr>
<tr>
<td>Imaginary quadratic number fields</td>
<td>Imaginary hyperelliptic curves</td>
</tr>
<tr>
<td>Class group (hard computation)</td>
<td>Jacobian (small characteristic: doable computation with Kedlaya’s algorithm)</td>
</tr>
<tr>
<td>Elliptic curves</td>
<td>Drinfeld modules</td>
</tr>
</tbody>
</table>
### Analogies (1/2)

<table>
<thead>
<tr>
<th>Number fields</th>
<th>Function fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathbb{Z}$</td>
<td>$\mathbb{F}_q[X]$</td>
</tr>
<tr>
<td>Imaginary quadratic number fields</td>
<td>Imaginary hyperelliptic curves</td>
</tr>
<tr>
<td>Class group (hard computation)</td>
<td>Jacobian (small characteristic: doable</td>
</tr>
<tr>
<td></td>
<td>computation with Kedlaya’s algorithm)</td>
</tr>
<tr>
<td>Elliptic curves</td>
<td>Drinfeld modules</td>
</tr>
</tbody>
</table>
### Analogies (1/2)

<table>
<thead>
<tr>
<th>Number fields</th>
<th>Function fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathbb{Z}$</td>
<td>$\mathbb{F}_q[X]$</td>
</tr>
<tr>
<td>Imaginary quadratic number fields</td>
<td>Imaginary hyperelliptic curves</td>
</tr>
<tr>
<td>Class group (hard computation)</td>
<td>Jacobian (small characteristic: doable computation with Kedlaya’s algorithm)</td>
</tr>
<tr>
<td>Elliptic curves</td>
<td>Drinfeld modules</td>
</tr>
</tbody>
</table>
**Analogies (1/2)**

<table>
<thead>
<tr>
<th>Number fields</th>
<th>Function fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \mathbb{Z} )</td>
<td>( \mathbb{F}_q[X] )</td>
</tr>
<tr>
<td>Imaginary quadratic number fields</td>
<td>Imaginary hyperelliptic curves</td>
</tr>
<tr>
<td>Class group (hard computation)</td>
<td>Jacobian (small characteristic: doable computation with Kedlaya’s algorithm)</td>
</tr>
<tr>
<td>Elliptic curves</td>
<td>Drinfeld modules</td>
</tr>
</tbody>
</table>
## Analogies (2/2)

<table>
<thead>
<tr>
<th>Elliptic curves over finite fields</th>
<th>Finite Drinfeld $\mathbb{F}_q[X]$-modules</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathbb{Z}$-module law on $E(\overline{\mathbb{F}_q})$</td>
<td>$\mathbb{F}_q[X]$-module law on $\overline{\mathbb{F}_q}$</td>
</tr>
<tr>
<td>$E[n] \simeq (\mathbb{Z}/n)^2$ if $p \nmid n$</td>
<td>$\phi[a] \simeq (\mathbb{F}_q[X]/a)^r$ if $p \nmid a$</td>
</tr>
<tr>
<td>$E[p] \simeq (\mathbb{Z}/p)^{s \in {0,1}}$</td>
<td>$\phi[p] \simeq (\mathbb{F}_q[X]/p)^{s \in {0,\ldots,r-1}}$</td>
</tr>
</tbody>
</table>

**Vélu formulae**

- j-invariant encoding $\mathbb{F}_q$-isomorphism classes
- Characteristic polynomial of the Frobenius endomorphism
- Theory of complex multiplication
- Two constructions: algebraic, analytic
### Analogies (2/2)

<table>
<thead>
<tr>
<th>Elliptic curves over finite fields</th>
<th>Finite Drinfeld $\mathbb{F}_q[X]$-modules</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathbb{Z}$-module law on $E(\overline{\mathbb{F}}_q)$</td>
<td>$\mathbb{F}_q[X]$-module law on $\overline{\mathbb{F}}_q$</td>
</tr>
<tr>
<td>$E[n] \simeq (\mathbb{Z}/n)^2$ if $p \nmid n$</td>
<td>$\phi[a] \simeq (\mathbb{F}_q[X]/a)^r$ if $p \nmid a$</td>
</tr>
<tr>
<td>$E[p] \simeq (\mathbb{Z}/p)^{s \in {0,1}}$</td>
<td>$\phi[p] \simeq (\mathbb{F}_q[X]/p)^{s \in {0,...,r-1}}$</td>
</tr>
</tbody>
</table>

Vélu formulae

- j-invariant encoding $\mathbb{F}_q$-isomorphism classes
- Characteristic polynomial of the Frobenius endomorphism
- Theory of complex multiplication
- Two constructions: algebraic, analytic
**Analogies (2/2)**

<table>
<thead>
<tr>
<th>Elliptic curves over finite fields</th>
<th>Finite Drinfeld $\mathbb{F}_q[X]$-modules</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathbb{Z}$-module law on $E(\overline{\mathbb{F}_q})$</td>
<td>$\mathbb{F}_q[X]$-module law on $\overline{\mathbb{F}_q}$</td>
</tr>
<tr>
<td>$E[n] \simeq (\mathbb{Z}/n)^2$ if $p \nmid n$</td>
<td>$\phi[a] \simeq (\mathbb{F}_q[X]/a)^r$ if $p \nmid a$</td>
</tr>
<tr>
<td>$E[p] \simeq (\mathbb{Z}/p)^{s \in {0,1}}$</td>
<td>$\phi[p] \simeq (\mathbb{F}_q[X]/p)^{s \in {0,\ldots,r-1}}$</td>
</tr>
</tbody>
</table>

Vélu formulae

- j-invariant encoding $\mathbb{F}_q$-isomorphism classes
- Characteristic polynomial of the Frobenius endomorphism
- Theory of complex multiplication
- Two constructions: algebraic, analytic
## Analogies (2/2)

<table>
<thead>
<tr>
<th>Elliptic curves over finite fields</th>
<th>Finite Drinfeld $\mathbb{F}_q[X]$-modules</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathbb{Z}$-module law on $E(\overline{\mathbb{F}_q})$</td>
<td>$\mathbb{F}_q[X]$-module law on $\overline{\mathbb{F}_q}$</td>
</tr>
<tr>
<td>$E[n] \simeq (\mathbb{Z}/n)^2$ if $p \nmid n$</td>
<td>$\phi[a] \simeq (\mathbb{F}_q[X]/a)^r$ if $p \nmid a$</td>
</tr>
<tr>
<td>$E[p] \simeq (\mathbb{Z}/p)^{s \in {0,1}}$</td>
<td>$\phi[p] \simeq (\mathbb{F}_q[X]/p)^{s \in {0,\ldots,r-1}}$</td>
</tr>
</tbody>
</table>

### Vélu formulae

- j-invariant encoding $\mathbb{F}_q$-isomorphism classes
- Characteristic polynomial of the Frobenius endomorphism
- Theory of complex multiplication
- Two constructions: algebraic, analytic
### Analogies (2/2)

<table>
<thead>
<tr>
<th>Elliptic curves over finite fields</th>
<th>Finite Drinfeld $\mathbb{F}_q[X]$-modules</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathbb{Z}$-module law on $E(\overline{\mathbb{F}_q})$</td>
<td>$\mathbb{F}_q[X]$-module law on $\overline{\mathbb{F}_q}$</td>
</tr>
<tr>
<td>$E[n] \simeq (\mathbb{Z}/n)^2$ if $p \nmid n$</td>
<td>$\phi[a] \simeq (\mathbb{F}_q[X]/a)^r$ if $p \nmid a$</td>
</tr>
<tr>
<td>$E[p] \simeq (\mathbb{Z}/p)^{s \in {0,1}}$</td>
<td>$\phi[p] \simeq (\mathbb{F}_q[X]/p)^{s \in {0,\ldots,r-1}}$</td>
</tr>
</tbody>
</table>

**Vélu formulae**

- $j$-invariant encoding $\overline{\mathbb{F}_q}$-isomorphism classes
- Characteristic polynomial of the Frobenius endomorphism
- Theory of complex multiplication
- Two constructions: algebraic, analytic
## Analogies (2/2)

<table>
<thead>
<tr>
<th><em>Elliptic curves over finite fields</em></th>
<th><em>Finite Drinfeld $\mathbb{F}_q[X]$-modules</em></th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathbb{Z}$-module law on $E(\overline{\mathbb{F}_q})$</td>
<td>$\mathbb{F}_q[X]$-module law on $\overline{\mathbb{F}_q}$</td>
</tr>
<tr>
<td>$E[n] \cong (\mathbb{Z}/n)^2$ if $p \nmid n$</td>
<td>$\phi[a] \cong (\mathbb{F}_q[X]/a)^r$ if $p \nmid a$</td>
</tr>
<tr>
<td>$E[p] \cong (\mathbb{Z}/p)^{s \in {0,1}}$</td>
<td>$\phi[p] \cong (\mathbb{F}_q[X]/p)^{s \in {0,\ldots,r-1}}$</td>
</tr>
</tbody>
</table>

### Vélu formulae
- j-invariant encoding $\overline{\mathbb{F}_q}$-isomorphism classes
- Characteristic polynomial of the Frobenius endomorphism
- Theory of complex multiplication
- Two constructions: algebraic, analytic
### Analogies (2/2)

<table>
<thead>
<tr>
<th>Elliptic curves over finite fields</th>
<th>Finite Drinfeld $\mathbb{F}_q[X]$-modules</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathbb{Z}$-module law on $E(\overline{\mathbb{F}_q})$</td>
<td>$\mathbb{F}_q[X]$-module law on $\overline{\mathbb{F}_q}$</td>
</tr>
<tr>
<td>$E[n] \simeq (\mathbb{Z}/n)^2$ if $p \nmid n$</td>
<td>$\phi[a] \simeq (\mathbb{F}_q[X]/a)^r$ if $p \nmid a$</td>
</tr>
<tr>
<td>$E[p] \simeq (\mathbb{Z}/p)^{s \in {0,1}}$</td>
<td>$\phi[p] \simeq (\mathbb{F}_q[X]/p)^{s \in {0,\ldots,r-1}}$</td>
</tr>
</tbody>
</table>

**Vélu formulae**

- $j$-invariant encoding $\overline{\mathbb{F}_q}$-isomorphism classes
- Characteristic polynomial of the Frobenius endomorphism
- Theory of complex multiplication

**Two constructions: algebraic, analytic**
## Analogies (2/2)

<table>
<thead>
<tr>
<th>Elliptic curves over finite fields</th>
<th>Finite Drinfeld $\mathbb{F}_q[X]$-modules</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathbb{Z}$-module law on $E(\overline{\mathbb{F}_q})$</td>
<td>$\mathbb{F}_q[X]$-module law on $\overline{\mathbb{F}_q}$</td>
</tr>
<tr>
<td>$E[n] \cong (\mathbb{Z}/n)^2$ if $p \nmid n$</td>
<td>$\phi[a] \cong (\mathbb{F}_q[X]/a)^r$ if $p \nmid a$</td>
</tr>
<tr>
<td>$E[p] \cong (\mathbb{Z}/p)^{s \in {0,1}}$</td>
<td>$\phi[p] \cong (\mathbb{F}_q[X]/p)^{s \in {0,\ldots,r-1}}$</td>
</tr>
</tbody>
</table>

**Vélu formulae**

- $j$-invariant encoding $\overline{\mathbb{F}_q}$-isomorphism classes
- Characteristic polynomial of the Frobenius endomorphism
- Theory of complex multiplication
- Two constructions: algebraic, analytic
Main results

Preprint ia.cr/2022/349.

Computer algebra:

- Definition of a CRS-like group action for Drinfeld modules. Proof that it is simply transitive.
- Algorithm to compute the action.
- Efficient C++/NTL implementation.

Cryptography:

- Reduction of the inverse problem to the isogeny-finding problem.
- Conjecture that the best (at the time) algorithm ran in exponential time. Wesolowski found a new polynomial algorithm (ia.cr/2022/438).
Main results

Preprint ia.cr/2022/349.

Computer algebra:

- Definition of a CRS-like group action for Drinfeld modules. Proof that it is simply transitive.
- Algorithm to compute the action.
- Efficient C++/NTL implementation.

Cryptography:

- Reduction of the inverse problem to the isogeny-finding problem.
- Conjecture that the best (at the time) algorithm ran in exponential time. Wesolowski found a new polynomial algorithm (ia.cr/2022/438).
Main results

Preprint ia.cr/2022/349.

Computer algebra:
- Definition of a CRS-like group action for Drinfeld modules. Proof that it is simply transitive.
- Algorithm to compute the action.
  - Efficient C++/NTL implementation.

Cryptography:
- Reduction of the inverse problem to the isogeny-finding problem.
- Conjecture that the best (at the time) algorithm ran in exponential time. Wesolowski found a new polynomial algorithm (ia.cr/2022/438).
Main results

Preprint ia.cr/2022/349.

Computer algebra:

- Definition of a CRS-like group action for Drinfeld modules. Proof that it is simply transitive.
- Algorithm to compute the action.
- Efficient C++/NTL implementation.

Cryptography:

- Reduction of the inverse problem to the isogeny-finding problem.
- Conjecture that the best (at the time) algorithm ran in exponential time.
  Wesolowski found a new polynomial algorithm (ia.cr/2022/438).
Main results

Preprint ia.cr/2022/349.

Computer algebra:
- Definition of a CRS-like group action for Drinfeld modules. Proof that it is simply transitive.
- Algorithm to compute the action.
- Efficient C++/NTL implementation.

Cryptography:
- Reduction of the inverse problem to the isogeny-finding problem.
- Conjecture that the best (at the time) algorithm ran in exponential time. Wesolowski found a new polynomial algorithm (ia.cr/2022/438).
MAIN RESULTS

Preprint ia.cr/2022/349.

Computer algebra:

- Definition of a CRS-like group action for Drinfeld modules. Proof that it is simply transitive.
- Algorithm to compute the action.
- Efficient C++/NTL implementation.

Cryptography:

- Reduction of the inverse problem to the isogeny-finding problem.
- Conjecture that the best (at the time) algorithm ran in exponential time. Wesolowski found a new polynomial algorithm (ia.cr/2022/438).
Main results

Preprint ia.cr/2022/349.

Computer algebra:

- Definition of a CRS-like group action for Drinfeld modules. Proof that it is simply transitive.
- Algorithm to compute the action.
- Efficient C++/NTL implementation.

Cryptography:

- Reduction of the inverse problem to the isogeny-finding problem.
- Conjecture that the best (at the time) algorithm ran in exponential time.
  Wesolowski found a new polynomial algorithm (ia.cr/2022/438).
Main results

Preprint ia.cr/2022/349.

Computer algebra:

- Definition of a CRS-like group action for Drinfeld modules. Proof that it is simply transitive.
- Algorithm to compute the action.
- Efficient C++/NTL implementation.

Cryptography:

- Reduction of the inverse problem to the isogeny-finding problem.
- Conjecture that the best (at the time) algorithm ran in exponential time. Wesolowski found a new polynomial algorithm (ia.cr/2022/438).
Let's define Drinfeld modules

Let:

- $\phi$: potential Drinfeld module;
- $a, b \in \mathbb{F}_q[X], x, y \in \mathbb{F}_q, \lambda \in \mathbb{F}_q$.

Act on $\mathbb{F}_q$ (instead of $E(\mathbb{F}_q)$):

**Goal 1:** $a \cdot (x + y) = a \cdot x + a \cdot y$;

**Goal 2:** $\lambda \cdot x = \lambda x$;

(1) + (2): $\phi(a) : (x \mapsto a \cdot x)$ is $\mathbb{F}_q$-linear ($\phi(a) \in \text{End}_{\mathbb{F}_q}(\mathbb{F}_q)$).

**Goal 3:** $a \cdot (b \cdot x) = (ab) \cdot x$;

(3): $a \mapsto \phi(a)$ is a ring morphism $\mathbb{F}_q[X] \to \text{End}_{\mathbb{F}_q}(\mathbb{F}_q)$. 
Let's define Drinfeld modules

Let:

- \( \phi: \text{potential Drinfeld module}; \)
- \( a, b \in \mathbb{F}_q[X], x, y \in \overline{\mathbb{F}_q}, \lambda \in \mathbb{F}_q. \)

Act on \( \overline{\mathbb{F}_q} \) (instead of \( E(\overline{\mathbb{F}_q}) \)):

**Goal 1:** \( a \cdot (x + y) = a \cdot x + a \cdot y; \)

**Goal 2:** \( \lambda \cdot x = \lambda x; \)

(1) + (2): \( \phi(a) : (x \mapsto a \cdot x) \) is \( \mathbb{F}_q \)-linear \( (\phi(a) \in \text{End}_{\mathbb{F}_q}(\overline{\mathbb{F}_q})). \)

**Goal 3:** \( a \cdot (b \cdot x) = (ab) \cdot x; \)

(3): \( a \mapsto \phi(a) \) is a ring morphism \( \mathbb{F}_q[X] \to \text{End}_{\mathbb{F}_q}(\overline{\mathbb{F}_q}). \)
Let’s define Drinfeld modules

Let:

- $\phi$: potential Drinfeld module;
- $a, b \in \mathbb{F}_q[X]$, $x, y \in \mathbb{F}_q$, $\lambda \in \mathbb{F}_q$.

Act on $\mathbb{F}_q$ (instead of $E(\mathbb{F}_q)$):

**Goal 1:** $a \cdot (x + y) = a \cdot x + a \cdot y$;

**Goal 2:** $\lambda \cdot x = \lambda x$;

(1) + (2): $\phi(a) : (x \mapsto a \cdot x)$ is $\mathbb{F}_q$-linear ($\phi(a) \in \text{End}_{\mathbb{F}_q}(\mathbb{F}_q)$).

**Goal 3:** $a \cdot (b \cdot x) = (ab) \cdot x$;

(3): $a \mapsto \phi(a)$ is a ring morphism $\mathbb{F}_q[X] \to \text{End}_{\mathbb{F}_q}(\mathbb{F}_q)$. 
Let's define Drinfeld modules

Let:

- $\phi$: potential Drinfeld module;
- $a, b \in \mathbb{F}_q[X]$, $x, y \in \overline{\mathbb{F}_q}$, $\lambda \in \mathbb{F}_q$.

Act on $\overline{\mathbb{F}_q}$ (instead of $E(\overline{\mathbb{F}_q})$):

**Goal 1:** $a \cdot (x + y) = a \cdot x + a \cdot y$;
**Goal 2:** $\lambda \cdot x = \lambda x$;

(1) + (2): $\phi(a) : (x \mapsto a \cdot x)$ is $\mathbb{F}_q$-linear ($\phi(a) \in \text{End}_{\mathbb{F}_q}(\overline{\mathbb{F}_q})$).

**Goal 3:** $a \cdot (b \cdot x) = (ab) \cdot x$;

(3): $a \mapsto \phi(a)$ is a ring morphism $\mathbb{F}_q[X] \to \text{End}_{\mathbb{F}_q}(\overline{\mathbb{F}_q})$. 
Let’s define Drinfeld modules

Let:

- $\phi$: potential Drinfeld module;
- $a, b \in \mathbb{F}_q[X], x, y \in \overline{\mathbb{F}}_q, \lambda \in \mathbb{F}_q$.

Act on $\overline{\mathbb{F}}_q$ (instead of $E(\overline{\mathbb{F}}_q)$):

**Goal 1:** $a \cdot (x + y) = a \cdot x + a \cdot y$;
**Goal 2:** $\lambda \cdot x = \lambda x$;

*(1) + (2):* $\phi(a) : (x \mapsto a \cdot x)$ is $\mathbb{F}_q$-linear ($\phi(a) \in \text{End}_{\mathbb{F}_q}(\overline{\mathbb{F}}_q)$).

**Goal 3:** $a \cdot (b \cdot x) = (ab) \cdot x$;

*(3):* $a \mapsto \phi(a)$ is a ring morphism $\mathbb{F}_q[X] \to \text{End}_{\mathbb{F}_q}(\overline{\mathbb{F}}_q)$. 
Let's define Drinfeld modules

Let:

- $\phi$: potential Drinfeld module;
- $a, b \in \mathbb{F}_q[X], x, y \in \overline{\mathbb{F}_q}, \lambda \in \mathbb{F}_q$.

Act on $\overline{\mathbb{F}_q}$ (instead of $E(\mathbb{F}_q)$):

**Goal 1:** $a \cdot (x + y) = a \cdot x + a \cdot y$;

**Goal 2:** $\lambda \cdot x = \lambda x$;

(1) + (2): $\phi(a): (x \mapsto a \cdot x)$ is $\mathbb{F}_q$-linear ($\phi(a) \in \text{End}_{\mathbb{F}_q}(\overline{\mathbb{F}_q})$).

**Goal 3:** $a \cdot (b \cdot x) = (ab) \cdot x$;

(3): $a \mapsto \phi(a)$ is a ring morphism $\mathbb{F}_q[X] \to \text{End}_{\mathbb{F}_q}(\overline{\mathbb{F}_q})$. 

Antoine Leudière
Let’s define Drinfeld modules

Let:
- $\phi$: potential Drinfeld module;
- $a, b \in \mathbb{F}_q[X]$, $x, y \in \mathbb{F}_q$, $\lambda \in \mathbb{F}_q$.

Act on $\mathbb{F}_q$ (instead of $E(\mathbb{F}_q)$):

**Goal 1:** $a \cdot (x + y) = a \cdot x + a \cdot y$;
**Goal 2:** $\lambda \cdot x = \lambda x$;

(1) + (2): $\phi(a) : (x \mapsto a \cdot x)$ is $\mathbb{F}_q$-linear ($\phi(a) \in \text{End}_{\mathbb{F}_q}(\mathbb{F}_q)$).

**Goal 3:** $a \cdot (b \cdot x) = (ab) \cdot x$;

(3): $a \mapsto \phi(a)$ is a ring morphism $\mathbb{F}_q[X] \to \text{End}_{\mathbb{F}_q}(\mathbb{F}_q)$. 
Linear endomorphisms of $\overline{F}_q$ (1/3)

Any $f \in \text{End}_{\overline{F}_q}(\overline{F}_q)$ is

$$f : x \mapsto l_n x^{q^n} + \cdots + l_2 x^q + l_1 x, \quad l_i \in \overline{F}_q.$$ 

Denote $\tau : x \mapsto x^q$.

$$f : x \mapsto l_n \tau^n(x) + \cdots + l_2 \tau(x) + l_1 1(x), \quad l_i \in \overline{F}_q.$$ 

So

$$\text{End}_{\overline{F}_q}(\overline{F}_q) = \left\{ \sum_{i=1}^{n} l_i \tau^i, \quad n \in \mathbb{Z}_{\geq 0}, l_i \in \overline{F}_q \right\}.$$
Linear endomorphisms of $\overline{\mathbb{F}_q}$ (1/3)

Any $f \in \text{End}_{\mathbb{F}_q}(\overline{\mathbb{F}_q})$ is

$$f : x \mapsto l_n x^{q^n} + \cdots + l_2 x^q + l_1 x, \quad l_i \in \overline{\mathbb{F}_q}.$$ 

Denote $\tau : x \mapsto x^q$.

$$f : x \mapsto l_n \tau^n(x) + \cdots + l_2 \tau(x) + l_1 1(x), \quad l_i \in \overline{\mathbb{F}_q}.$$ 

So

$$\text{End}_{\mathbb{F}_q}(\overline{\mathbb{F}_q}) = \left\{ \sum_{i=1}^{n} l_i \tau^i, \quad n \in \mathbb{Z}_{\geq 0}, l_i \in \overline{\mathbb{F}_q} \right\}.$$
Linear endomorphisms of $\overline{\mathbb{F}_q}$ (1/3)

Any $f \in \text{End}_{\mathbb{F}_q}(\overline{\mathbb{F}_q})$ is

$$f : x \mapsto l_n x^{q^n} + \cdots + l_2 x^q + l_1 x, \quad l_i \in \overline{\mathbb{F}_q}.$$ 

Denote $\tau : x \mapsto x^q$.

$$f : x \mapsto l_n \tau^n(x) + \cdots + l_2 \tau(x) + l_1 1(x), \quad l_i \in \overline{\mathbb{F}_q}.$$ 

So

$$\text{End}_{\mathbb{F}_q}(\overline{\mathbb{F}_q}) = \left\{ \sum_{i=1}^{n} l_i \tau^i, \quad n \in \mathbb{Z}_{\geq 0}, l_i \in \overline{\mathbb{F}_q} \right\}.$$
Linear endomorphisms of $\overline{\mathbb{F}_q}$ (1/3)

Any $f \in \text{End}_{\mathbb{F}_q}(\overline{\mathbb{F}_q})$ is

$$f : x \mapsto l_n x^{q^n} + \cdots + l_2 x^q + l_1 x, \quad l_i \in \overline{\mathbb{F}_q}.$$ 

Denote $\tau : x \mapsto x^q$.

$$f : x \mapsto l_n \tau^n(x) + \cdots + l_2 \tau(x) + l_1 1(x), \quad l_i \in \overline{\mathbb{F}_q}.$$ 

So

$$\text{End}_{\mathbb{F}_q}(\overline{\mathbb{F}_q}) = \left\{ \sum_{i=1}^{n} l_i \tau^i, \quad n \in \mathbb{Z}_{\geq 0}, l_i \in \overline{\mathbb{F}_q} \right\}.$$
Let $L/\overline{F}_q$ be finite. Denote

$$L\{\tau\} = \left\{ \sum_{i=1}^{n} l_i \tau^n, \quad n \in \mathbb{Z}_{\geq 0}, l_i \in L \right\}.$$ 

**Definition (Ore, 1933)**

The ring $(L\{\tau\}, +, \circ)$ is called the ring of Ore polynomials in $\tau$ with coefficients in $L$. 
Linear endomorphisms of $\overline{F_q}(2/3)$

Let $L/\mathbb{F}_q$ be finite. Denote

$$L\{\tau\} = \left\{ \sum_{i=1}^{n} l_i \tau^n, \quad n \in \mathbb{Z}_{\geq 0}, l_i \in L \right\}.$$

**Definition (Ore, 1933)**

The ring $(L\{\tau\},+,:)$ is called the *ring of Ore polynomials in $\tau$ with coefficients in $L$*. 
Linear endomorphisms of $\overline{F}_q$ (3/3)

$L\{\tau\}$ is left-euclidean: $\forall P_1, P_2 \in L\{\tau\}, \deg_\tau(P_1) \geq \deg_\tau(P_2)$, $\exists Q, R \in L\{\tau\}$ s.t.:

\[
\begin{cases}
P_1 = QP_2 + R, \\
\deg_\tau(R) < \deg_\tau(P_2).
\end{cases}
\]

We can compute $\text{RGCD}$ in $L\{\tau\}$.

$$\langle \{P_i(\tau)\} \rangle = \text{rgcd}(\{P_i(\tau)\})L\{\tau\}.$$  

SageMath implementation (Xavier Caruso).
Linear endomorphisms of $\overline{\mathbb{F}_q}$ (3/3)

$L\{\tau\}$ is left-euclidean: $\forall P_1, P_2 \in L\{\tau\}$, $\deg_{\tau}(P_1) \geq \deg_{\tau}(P_2)$, $\exists Q, R \in L\{\tau\}$ s.t.:

\[
\begin{cases}
P_1 = QP_2 + R, \\
\deg_{\tau}(R) < \deg_{\tau}(P_2).
\end{cases}
\]

We can compute RGCD in $L\{\tau\}$.

$$\langle\{P_i(\tau)\}\rangle = \text{rgcd}(\{P_i(\tau)\})L\{\tau\}.$$
Linear endomorphisms of $\overline{F_q}$ (3/3)

$L\{\tau\}$ is left-euclidean: $\forall P_1, P_2 \in L\{\tau\}, \deg_\tau(P_1) \geq \deg_\tau(P_2), \exists Q, R \in L\{\tau\}$ s.t.:

$$\begin{cases} P_1 = QP_2 + R, \\ \deg_\tau(R) < \deg_\tau(P_2). \end{cases}$$

We can compute RGCD in $L\{\tau\}$.

$$\langle\{P_i(\tau)\}\rangle = \text{rgcd}({\{P_i(\tau)\}})L\{\tau\}.$$ 

SageMath implementation (Xavier Caruso).
Definition of a finite Drinfeld \( F_q[X] \)-module

Fix \( \omega \in L^\times \).

**Definition (Drinfeld, 1974)**

A finite Drinfeld \( F_q[X] \)-module defined over \( L \) is an \( F_q \)-algebra morphism

\[
\phi : F_q[X] \to L(\tau)
\]

s.t. \( \text{Im}(\phi) \not\subset L \), \( \text{ConstCoeff}(\phi(X)) = \omega \).

**Theorem (Drinfeld, 1974)**

\( F_q \) is an \( F_q[X] \)-module with

\[
(a, x) \mapsto \phi(a)(x).
\]

There is a more general definition.
**Definition of a finite Drinfeld $\mathbb{F}_q[X]$-module**

Fix $\omega \in L^\times$.

**Definition (Drinfeld, 1974)**

A *finite Drinfeld $\mathbb{F}_q[X]$-module defined over $L$* is an $\mathbb{F}_q$-algebra morphism

$$\phi : \mathbb{F}_q[X] \to L\{\tau\}$$

s.t. $\text{Im}(\phi) \subset L$, $\text{ConstCoeff}(\phi(X)) = \omega$.

**Theorem (Drinfeld, 1974)**

$\mathbb{F}_q$ is an $\mathbb{F}_q[X]$-module with

$$(a, x) \mapsto \phi(a)(x).$$

There is a more general definition.
**Definition of a finite Drinfeld $\mathbb{F}_q[X]$-module**

Fix $\omega \in L^\times$.

**Definition (Drinfeld, 1974)**

A *finite Drinfeld $\mathbb{F}_q[X]$-module defined over $L$* is an $\mathbb{F}_q$-algebra morphism

$$\phi : \mathbb{F}_q[X] \rightarrow L\{\tau\}$$

s.t. $\text{Im}(\phi) \not\subset L$, $\text{ConstCoeff}(\phi(X)) = \omega$.

**Theorem (Drinfeld, 1974)**

$\overline{\mathbb{F}_q}$ is an $\mathbb{F}_q[X]$-module with

$$(a, x) \mapsto \phi(a)(x).$$

There is a more general definition.
**Definition of a finite Drinfeld $\mathbb{F}_q[X]$-module**

Fix $\omega \in \mathbb{L}^\times$.

**Definition (Drinfeld, 1974)**

A *finite Drinfeld $\mathbb{F}_q[X]$-module defined over $L$* is an $\mathbb{F}_q$-algebra morphism

$$\phi : \mathbb{F}_q[X] \rightarrow L\{\tau\}$$

s.t. $\text{Im}(\phi) \subset L$, $\text{ConstCoeff}(\phi(X)) = \omega$.

**Theorem (Drinfeld, 1974)**

$\mathbb{F}_q$ is an $\mathbb{F}_q[X]$-module with

$$(a, x) \mapsto \phi(a)(x).$$

There is a more general definition.
Generator of a Drinfeld module

Fix $\phi : \mathbb{F}_q[X] \to L\{\tau\}$ a finite Drinfeld $\mathbb{F}_q[X]$-module. $\phi$ uniquely determined by

$$\phi(X) = \phi_n \tau^n + \cdots + \phi_1 \tau + \omega, \quad \phi_n \neq 0.$$ 

**Definition**

The *rank of* $\phi$ is $n$.

Rank 2 finite Drinfeld modules are closest to elliptic curves over finite fields.
Generator of a Drinfeld module

Fix $\phi : \mathbb{F}_q[X] \rightarrow L\{\tau\}$ a finite Drinfeld $\mathbb{F}_q[X]$-module. $\phi$ uniquely determined by

$$\phi(X) = \phi_n \tau^n + \cdots + \phi_1 \tau + \omega, \quad \phi_n \neq 0.$$  

**Definition**

The *rank of $\phi$* is $n$.

Rank 2 finite Drinfeld modules are closest to elliptic curves over finite fields.
Fix $\phi : \mathbb{F}_q[X] \to L\{\tau\}$ a finite Drinfeld $\mathbb{F}_q[X]$-module.

$\phi$ uniquely determined by

$$\phi(X) = \phi_n \tau^n + \cdots + \phi_1 \tau + \omega, \quad \phi_n \neq 0.$$ 

**Definition**

The *rank of $\phi$* is $n$.

Rank 2 finite Drinfeld modules are closest to elliptic curves over finite fields.
**Morphisms and isogenies**

**Definition**

A *morphism of finite Drinfeld modules* $\phi \rightarrow \psi$ is an Ore polynomial $m \in L\{\tau\}$ such that

$$m\phi(X) = \psi(X)m.$$ 

An *isogeny* is a nonzero morphism.

Endomorphisms always contain $\mathbb{F}_q[X]$ and $\tau_L = x \mapsto x^#L$:

- $\phi(P)\phi(X) = \phi(PX) = \phi(XP) = \phi(X)\phi(P)$, $P \in \mathbb{F}_q[X]$;
- $\phi(X)\tau_L = \tau_L(\phi_i\tau^n + \cdots + \omega) = \phi_i^#L\tau^n\tau_L + \cdots + \omega^#L\tau_L = \phi(X)\tau_L$. 
Morphisms and isogenies

**Definition**

A *morphism of finite Drinfeld modules* $\phi \rightarrow \psi$ is an Ore polynomial $m \in L\{\tau\}$ such that

$$m\phi(X) = \psi(X)m.$$  

An *isogeny* is a nonzero morphism.

Endomorphisms always contain $\mathbb{F}_q[X]$ and $\tau_L = x \mapsto x^\#L$:

- $\phi(P)\phi(X) = \phi(PX) = \phi(XP) = \phi(X)\phi(P), \quad P \in \mathbb{F}_q[X]$;
- $\phi(X)\tau_L = \tau_L(\phi_i^{\tau^n} + \cdots + \omega) = \phi_i^{\#L}\tau^n\tau_L + \cdots + \omega^{\#L}\tau_L = \phi(X)\tau_L.$
**Morphisms and Isogenies**

**Definition**

A *morphism of finite Drinfeld modules* $\phi \to \psi$ is an Ore polynomial $m \in L\{\tau\}$ such that

$$m\phi(X) = \psi(X)m.$$  

An *isogeny* is a nonzero morphism.

Endomorphisms always contain $\mathbb{F}_q[X]$ and $\tau_L = x \mapsto x^#L$:

- $\phi(P)\phi(X) = \phi(PX) = \phi(XP) = \phi(X)\phi(P), \quad P \in \mathbb{F}_q[X]$;
- $\phi(X)\tau_L = \tau_L(\phi_1\tau^n + \cdots + \omega) = \phi_1^#L \tau^n \tau_L + \cdots + \omega^#L \tau_L = \phi(X)\tau_L$. 
Characteristic polynomial (1/2)

Assume $\text{rank}(\phi) = 2$.
There exists

$$\chi_{\phi}(X)(T) = T^2 - A(X)T + B(X) \in \mathbb{F}_q[X][T]$$

with

$$\chi_{\phi}(\phi(X))(\tau_L) = \tau_L^2 - \phi(A)\tau_L + \phi(B) = 0$$

and $\deg_X(A) \leq d/2$, $\deg_X(B) = d$ (Hasse bounds).

**Definition**

$\chi_{\phi}$ is the *characteristic polynomial of the Frobenius endomorphism of $\phi$.*

$\phi$ is *supersingular* if $p = \text{MinPol}_{\mathbb{F}_q}(\omega)$ divides $A$.

$\chi_{\phi}$ can be efficiently computed (Schost-Musleh, 2019).
Characteristic polynomial (1/2)

Assume \( \text{rank}(\phi) = 2 \).

There exists

\[
\chi_\phi(X)(T) = T^2 - A(X)T + B(X) \in \mathbb{F}_q[X][T]
\]

with

\[
\chi_\phi(\phi(X))(\tau_L) = \tau_L^2 - \phi(A)\tau_L + \phi(B) = 0
\]

and \( \deg_X(A) \leq d/2 \), \( \deg_X(B) = d \) (Hasse bounds).

**Definition**

\( \chi_\phi \) is the characteristic polynomial of the Frobenius endomorphism of \( \phi \).

\( \phi \) is supersingular iff \( \rho = \text{MinPol}_{\mathbb{F}_q}(\omega) \) divides \( A \).

\( \chi_\phi \) can be efficiently computed (Schost-Musleh, 2019).
Assume $\text{rank}(\phi) = 2$. 
There exists
\[ \chi_\phi(X)(T) = T^2 - A(X)T + B(X) \in \mathbb{F}_q[X][T] \]
with
\[ \chi_\phi(\phi(X))(\tau_L) = \tau_L^2 - \phi(A)\tau_L + \phi(B) = 0 \]
and $\deg_X(A) \leq d/2$, $\deg_X(B) = d$ (Hasse bounds).

**Definition**

$\chi_\phi$ is the *characteristic polynomial of the Frobenius endomorphism of $\phi$*. 

$\phi$ is *supersingular* iif $p = \text{MinPol}_{\mathbb{F}_q}(\omega)$ divides $A$. 
$
\chi_\phi$ can be efficiently computed (Schost-Musleh, 2019).
Assume $\text{rank}(\phi) = 2$. There exists

$$\chi_\phi(X)(T) = T^2 - A(X)T + B(X) \in \mathbb{F}_q[X][T]$$

with

$$\chi_\phi(\phi(X))(\tau_L) = \tau_L^2 - \phi(A)\tau_L + \phi(B) = 0$$

and $\deg_X(A) \leq d/2$, $\deg_X(B) = d$ (Hasse bounds).

**Definition**

$\chi_\phi$ is the *characteristic polynomial of the Frobenius endomorphism of* $\phi$.

$\phi$ is *supersingular* iif $p = \text{MinPol}_{\mathbb{F}_q}(\omega)$ divides $A$.

$\chi_\phi$ can be efficiently computed (Schost-Musleh, 2019).
Assume $\text{rank}(\phi) = 2$.
There exists

$$
\chi_\phi(X)(T) = T^2 - A(X)T + B(X) \in \mathbb{F}_q[X][T]
$$

with

$$
\chi_\phi(\phi(X))(\tau_L) = \tau_L^2 - \phi(A)\tau_L + \phi(B) = 0
$$

and $\deg_X(A) \leq d/2$, $\deg_X(B) = d$ (Hasse bounds).

**Definition**

$\chi_\phi$ is the *characteristic polynomial of the Frobenius endomorphism of $\phi$.*

$\phi$ is *supersingular* iif $\rho = \text{MinPol}_{\mathbb{F}_q}(\omega)$ divides $A$.

$\chi_\phi$ can be efficiently computed (Schost-Musleh, 2019).
Main result

**Theorem (Classical result from class field theory)**

Let $E/\mathbb{F}_q$ be some ordinary elliptic curve. Fix $\mathcal{O} = \text{End}_{\mathbb{F}_q}(E)$.

Then, $\text{Cl}(\mathcal{O})$ acts simply transitively on the set of $\mathcal{L}$-isomorphism classes of elliptic curves defined over $\mathbb{F}_q$ with same endomorphism ring and characteristic polynomial as $E$.

**Theorem (L., Spaenlehauer, 2022)**

Assume $[L : \mathbb{F}_q]$ is odd and $\geq 5$. Let $\phi$ be some ordinary rank two finite Drinfeld module. Fix $\mathcal{O} = \text{End}_L(\phi)$.

Assume $\chi_{\phi}$ defines an imaginary hyperelliptic curve $\mathcal{H}$.

Then, $\text{Cl}(\mathcal{O}) \cong \text{Pic}^0(\mathcal{H})$ and $\text{Cl}(\mathcal{O})$ acts simply transitively on the set of $\mathcal{L}$-isomorphism classes of rank 1 Drinfeld modules $\mathcal{O} \to L\{\tau\}$. 
Main result

Theorem (Classical result from class field theory)

Let $E / \mathbb{F}_q$ be some ordinary elliptic curve. Fix $\mathcal{O} = \text{End}_{\mathbb{F}_q}(E)$.

Then, $\text{Cl}(\mathcal{O})$ acts simply transitively on the set of $\overline{L}$-isomorphism classes of elliptic curves defined over $\mathbb{F}_q$ with same endomorphism ring and characteristic polynomial as $E$.

Theorem (L., Spaenlehauer, 2022)

Assume $[L : \mathbb{F}_q]$ is odd and $\geq 5$. Let $\phi$ be some ordinary rank two finite Drinfeld module. Fix $\mathcal{O} = \text{End}_L(\phi)$.

Assume $\chi_{\phi}$ defines an imaginary hyperelliptic curve $\mathcal{H}$.

Then, $\text{Cl}(\mathcal{O}) \simeq \text{Pic}^0(\mathcal{H})$ and $\text{Cl}(\mathcal{O})$ acts simply transitively on the set of $\overline{L}$-isomorphism classes of rank 1 Drinfeld modules $\mathcal{O} \rightarrow L[\tau]$. 
**Definition of the action**

Let $a \in \text{Id}(O)$, let $\phi'$ be a representative. Let 

$$V_a = \bigcap_{f \in a} \ker(f).$$

$V_a$ is the kernel of some isogeny $i_a$ with domain $\phi'$. We associate

$$a \star \phi' := \text{codomain of } i_a.$$

**Definition**

This map can be extended to the class group and to set of isomorphism classes. This defines our action.
**Definition of the action**

Let $a \in \text{Id}(O)$, let $\phi'$ be a representative. Let

$$V_a = \bigcap_{f \in a} \ker(f).$$

$V_a$ is the kernel of some isogeny $i_a$ with domain $\phi'$. We associate

$$a \star \phi' := \text{codomain of } i_a.$$

**Definition**

This map can be extended to the class group and to set of isomorphism classes. This defines our action.
**Definition of the action**

Let $a \in \text{Id}(O)$, let $\phi'$ be a representative. Let

$$V_a = \bigcap_{f \in a} \text{Ker}(f).$$

$V_a$ is the kernel of some isogeny $\iota_a$ with domain $\phi'$. We associate

$$a \star \phi' := \text{codomain of } \iota_a.$$

**Definition**

This map can be extended to the class group and to set of isomorphism classes. This defines our action.
Definition of the action

Let $a \in \text{Id}(O)$, let $\phi'$ be a representative. Let

$$V_a = \bigcap_{f \in a} \ker(f).$$

$V_a$ is the kernel of some isogeny $\iota_a$ with domain $\phi'$. We associate

$$a \star \phi' := \text{codomain of } \iota_a.$$

Definition

This map can be extended to the class group and to set of isomorphism classes. This defines our action.
Isomorphism $\text{Cl}(\mathcal{O}) \simeq \text{Pic}^0(\mathcal{H})$

$\text{End}(\phi) = \mathcal{O}$ always contains $\mathbb{F}_q[X]$ and $\tau_L$.

In our case, that’s it:

$$\mathcal{O} \simeq \mathbb{F}_q[X][Y]/\chi_\phi \simeq \text{ring of functions on } \mathcal{H} \text{ regular outside } \infty,$$

so that

$$\text{Cl}(\mathcal{O}) \simeq \text{Pic}^0(\mathcal{H}).$$
Isomorphism $\text{Cl}(\mathcal{O}) \cong \text{Pic}^0(\mathcal{H})$

$\text{End}(\phi) = \mathcal{O}$ always contains $\mathbb{F}_q[X]$ and $\tau_L$. In our case, that’s it:

$$\mathcal{O} \cong \mathbb{F}_q[X][Y]/\chi_{\phi} \cong \text{ring of functions on } \mathcal{H} \text{ regular outside } \infty,$$

so that

$$\text{Cl}(\mathcal{O}) \cong \text{Pic}^0(\mathcal{H}).$$
Isomorphism $\text{Cl}(\mathcal{O}) \simeq \text{Pic}^0(\mathcal{H})$

$\text{End}(\phi) = \mathcal{O}$ always contains $\mathbb{F}_q[X]$ and $\tau_L$.
In our case, that’s it:

$$\mathcal{O} \simeq \mathbb{F}_q[X][Y]/\chi_\phi \simeq \text{ring of functions on } \mathcal{H} \text{ regular outside } \infty,$$

so that

$$\text{Cl}(\mathcal{O}) \simeq \text{Pic}^0(\mathcal{H}).$$
Mumford coordinates for $\text{Pic}^0(\mathcal{H})$

Representation with Mumford coordinates:

$$\text{Pic}^0(\mathcal{H}) \leftrightarrow \text{Cl}(\mathbb{F}_q[X][Y]/\chi \phi)$$

$$(u, v) \leftrightarrow \text{Class of } \langle u(\overline{X}), \overline{Y} - v(\overline{X}) \rangle$$

with $u, v \in \mathbb{F}_q[X]$ and $u \neq 0$ is monic, $\deg(v) < \deg(u) \leq (d - 1)/2$, $u | \chi(X, v(X))$ and $d = [L : \mathbb{F}_q]$ (Hasse-Weil bounds)
Explicit computation

\[ V_a = \text{Ker}(\imath_a) = \bigcap_{f \in \mathfrak{a}} \text{Ker}(f) = \bigcap_{\overline{f} \in \langle \phi(X), \tau_L - \phi(v) \rangle} \text{Ker}(f(\phi(X), \tau_L)). \]

Therefore

\[ \imath_a = \text{rgcd}(\phi(u), \tau_L - \phi(v)). \]
**Explicit computation**

\[ \mathcal{V}_a = \ker(\iota_a) = \bigcap_{f \in \mathfrak{a}} \ker(f) = \bigcap_{\overline{f} \in \langle u(\overline{X}), Y-v(\overline{X}) \rangle} \ker(f(\phi(X), \tau_L)). \]

Therefore

\[ \iota_a = \text{rgcd}(\phi(u), \tau_L - \phi(v)). \]
**Algorithm**

**Input:** — A $j$-invariant $j \in L$.
— Mumford coordinates $(u, v) \in \mathbb{F}_q[X]^2$.

**Output:** A $j$-invariant.

1. $\tilde{u} \leftarrow u(j^{-1}\tau^2 + \tau + \omega) \in L\{\tau\}$;
2. $\tilde{v} \leftarrow v(j^{-1}\tau^2 + \tau + \omega) \in L\{\tau\}$;
3. $\iota \leftarrow \text{rgcd}(\tilde{u}, \tau^{[L:\mathbb{F}_q]} - \tilde{v})$;
4. $\hat{g} \leftarrow \iota_0^{-q}(\iota_0 + \iota_1(\omega^q - \omega))$;
5. $\hat{\Delta} \leftarrow j^{-q \deg{\tau}(\iota)}$;
6. Return $\hat{g}^{q+1}/\hat{\Delta}$.

C++ / NTL implementation of the action: computation in ~200 ms for $\mathbb{F}_q = \mathbb{F}_2$ and $[L: \mathbb{F}_q] = 521$. The hyperelliptic curve has genus $\frac{521-1}{2} = 260$, $\text{Pic}^0(\mathcal{H})$ has order $2 \times 3154131824675467260411631641504\ldots$

...7743350494962889744865259442943656024073295689.
**Algorithm**

**Input:** — A $j$-invariant $j \in L$.

| — Mumford coordinates $(u,v) \in \mathbb{F}_q[X]^2$. |

**Output:** A $j$-invariant.

1. $\tilde{u} \leftarrow u\left(j^{-1} \tau^2 + \tau + \omega\right) \in L\{\tau\}$;
2. $\tilde{v} \leftarrow v\left(j^{-1} \tau^2 + \tau + \omega\right) \in L\{\tau\}$;
3. $\iota \leftarrow \text{rgcd}(\tilde{u}, \tau^{[L:\mathbb{F}_q]} - \tilde{v})$;
4. $\hat{g} \leftarrow \iota_0^{-q}(\iota_0 + \iota_1(\omega^q - \omega))$;
5. $\hat{\Delta} \leftarrow j^{-\deg_\tau(\iota)}$;
6. Return $\hat{g}^{q+1}/\hat{\Delta}$.

C++ / NTL implementation of the action: computation in $\sim 200$ ms for $\mathbb{F}_q = \mathbb{F}_2$ and $[L : \mathbb{F}_q] = 521$. The hyperelliptic curve has genus $\frac{521 - 1}{2} = 260$, Pic$^0(\mathcal{H})$ has order $2 \times 31541318246754567260411631641504\ldots$

$\ldots7743350494962889744865259442943656024073295689$. 
**Theorem (L., Spaenlehauer, 2022)**

The problems of inverting the action and the problems of finding finite Drinfeld module polynomially reduce to one another.

Write \( \phi(X) = \Delta \tau^2 + g \tau + \omega \), \( \psi(X) = \Delta' \tau^2 + g' \tau + \omega \), \( l = l_a \tau^a + \cdots + l_0 \in L\{\tau\} \).

Then \( l \) is an isogeny \( \phi \to \psi \) iif

\[
\Delta' l_a^q - \Delta q^a l_a = 0, \\
\Delta' l_{a-1}^q - \Delta q^{a-1} l_{a-1} = l_a g^q - g' l_a, \\
\forall k \in \llbracket 2, a \rrbracket, \quad \Delta' l_{a-k}^q - \Delta q^{a-k} l_{a-k} = l_{a-k+1} g^q l_{a-k+1} - g' l_{a-k+1}^q + l_{a-k+2} (\omega q^{a-k+2} - \omega), \\
l_0 g + l_1 \omega^q = \omega l_1 + g' l_0^q.
\]
**Inverse problem**

**Theorem (L., Spaenlehauer, 2022)**

The problems of inverting the action and the problems of finding finite Drinfeld module polynomially reduce to one another.

Write \( \phi(X) = \Delta \tau^2 + g \tau + \omega \), \( \psi(X) = \Delta' \tau^2 + g' \tau + \omega \), \( \iota = \iota_a \tau^a + \cdots + \iota_0 \in \mathbb{L}\{\tau}\).

Then \( \iota \) is an isogeny \( \phi \to \psi \) if and only if

\[
\begin{align*}
\Delta' \iota_a^q - \Delta^a \iota_a &= 0, \\
\Delta' \iota_{a-1}^q - \Delta^{a-1} \iota_{a-1} &= \iota_a g^q - g' \iota_a, \\
\forall k \in [2, a], \quad \Delta' \iota_{a-k}^q - \Delta^{a-k} \iota_{a-k} &= \iota_{a-k+1} g^{q^{a-k+1}} - g' \iota_{a-k+1} + \iota_{a-k+2} (\omega^{q^{a-k+2}} - \omega), \\
\iota_0 g + \iota_1 \omega^q &= \omega \iota_1 + g' \iota_0^q.
\end{align*}
\]
Attacks on this problem

- Previous work (Joux, Narayanan, 2019; Caranay, Greenberg, Scheidler, 2020): the system is solved recursively.

- Wesolowski (2022): this is an $\mathbb{F}_q$-linear system of equations. We can find an $\mathbb{F}_q$-basis by writing each coefficient in an $\mathbb{F}_q$-basis of $L$.

Interpretation: endomorphisms act on isogenies; endomorphism contain $\mathbb{F}_q[X]$, and therefore the field $\mathbb{F}_q$. This is not possible for $\mathbb{Z}$ (field with one element).
Attacks on this problem

- Previous work (Joux, Narayanan, 2019; Caranay, Greenberg, Scheidler, 2020): the system is solved recursively.

- Wesolowski (2022): this is an $\mathbb{F}_q$-linear system of equations. We can find an $\mathbb{F}_q$-basis by writing each coefficient in an $\mathbb{F}_q$-basis of $L$.

Interpretation: endomorphisms act on isogenies; endomorphism contain $\mathbb{F}_q[X]$, and therefore the field $\mathbb{F}_q$. This is not possible for $\mathbb{Z}$ (field with one element).
Attacks on this problem

- Previous work (Joux, Narayanan, 2019; Caranay, Greenberg, Scheidler, 2020): the system is solved recursively.

- Wesolowski (2022): this is an $\mathbb{F}_q$-linear system of equations. We can find an $\mathbb{F}_q$-basis by writing each coefficient in an $\mathbb{F}_q$-basis of $L$.

Interpretation: endomorphisms act on isogenies; endomorphism contain $\mathbb{F}_q[X]$, and therefore the field $\mathbb{F}_q$. This is not possible for $\mathbb{Z}$ (field with one element).
Flourishing research on algorithmic aspects of Drinfeld modules: Gekeler (1998); Joux, Narayanan (2019); Caranay (thesis, 2018); Caranay, Greenberg, Scheidler (2019); Schost, Musleh (2019).

Unexpected applications: computer algebra (Schost, 2017; Narayanan, 2019) and cryptography (Scanlon, 2001; Joux, Narayanan, 2019; Bombar, Couvreur, Debris-Alazard, 2022).
Flourishing research on algorithmic aspects of Drinfeld modules: Gekeler (1998); Joux, Narayanan (2019); Caranay (thesis, 2018); Caranay, Greenberg, Scheidler (2019); Schost, Musleh (2019).

Unexpected applications: **computer algebra** (Schost, 2017; Narayanan, 2019) and **cryptography** (Scanlon, 2001; Joux, Narayanan, 2019; Bombar, Couvreur, Debris-Alazard, 2022).