An explicit CRS-like action with Drinfeld modules

Séminaire de l'équipe LFANT

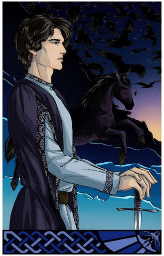
Antoine Leudière Pierre-Jean Spaenlehauer

INRIA Nancy-Grand Est

Juin 2022

Hard homogenous spaces (1/2)

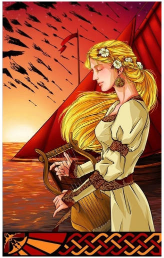
Tristan and Isolde choose an abelian simply transitive group action $G \times X \to X$, and $x \in X$.



$\longrightarrow$ $a \cdot x$ $\longrightarrow$

$\longleftarrow$ $b \cdot x$ $\longleftarrow$

$\leftarrow$ - - - - Both calculate $ab \cdot x$ (secret key) - - - - $\rightarrow$



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*.

The CRS action

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 $\mathcal{O} = \mathrm{End}_{\mathbb{F}_q}(E)$.
Then, $\mathrm{Cl}(\mathcal{O})$ acts simply transitively on the set of $\overline{\mathbb{F}_q}$-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).

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

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)

Number fields	Function fields
$\mathbb{Z}$	$\mathbb{F}_q[X]$
Imaginary quadratic number fields	Imaginary hyperelliptic curves
Class group (hard computation)	Jacobian (small characteristic: doable computation with Kedlaya's algorithm)
Elliptic curves	Drinfeld modules

Analogies (2/2)

Elliptic curves over finite fields	Finite Drinfeld $\mathbb{F}_q[X]$-modules
$\mathbb{Z}$-module law on $E(\overline{\mathbb{F}_q})$	$\mathbb{F}_q[X]$-module law on $\overline{\mathbb{F}_q}$
$E[n] \simeq (\mathbb{Z}/n)^2$ if $p \nmid n$ $E[p] \simeq (\mathbb{Z}/p)^{s \in \{0,1\}}$	$\phi[a] \simeq (\mathbb{F}_q[X]/a)^r$ if $\mathfrak{p} \nmid a$ $\phi[\mathfrak{p}] \simeq (\mathbb{F}_q[X]/\mathfrak{p})^{s \in \{0,\dots,r-1\}}$
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.
- SageMath implementation of Drinfeld modules (work in progress, `https://trac.sagemath.org/ticket/33713`).

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:

- ϕ: *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 ($\phi(a) \in \mathrm{End}_{\mathbb{F}_q}(\overline{\mathbb{F}_q})$).

Goal 3: $a \cdot (b \cdot x) = (ab) \cdot x$;
(3): $a \mapsto \phi(a)$ is a ring morphism $\mathbb{F}_q[X] \to \mathrm{End}_{\mathbb{F}_q}(\overline{\mathbb{F}_q})$.

Linear endomorphisms of $\overline{\mathbb{F}_q}$ (1/3)

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

$$\mathrm{End}_{\mathbb{F}_q}(\overline{\mathbb{F}_q}) = \left\{ \sum_{i=1}^{n} l_i \tau^i, \quad n \in \mathbb{Z}_{\geqslant 0}, l_i \in \overline{\mathbb{F}_q} \right\}.$$

Linear endomorphisms of $\overline{\mathbb{F}_q}$ (2/3)

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

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

Definition (Ore, 1933)

The ring $(L\{\tau\}, +, \circ)$ is called the *ring of Ore polynomials in τ with coefficients in L*.

Linear endomorphisms of $\overline{\mathbb{F}_q}$ (3/3)

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

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

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

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

SageMath implementation (Xavier Caruso).

Definition of a finite Drinfeld $\mathbb{F}_q[X]$-module

Fix $\omega \in Ł^\times$.

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

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.

Generator of a Drinfeld module

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

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

Definition

The *rank of ϕ* 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* $\phi \to \psi$ 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 $\tau_L = x \mapsto x^{\#L}$:

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

Characteristic polynomial (1/2)

Assume $\mathrm{rank}(\phi) = 2$.
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 $\deg_X(A) \leqslant d/2$, $\deg_X(B) = d$ (Hasse bounds).

Definition

χ_ϕ is the *characteristic polynomial of the Frobenius endomorphism of ϕ*.

ϕ is *supersingular iif* $\mathfrak{p} = \mathrm{MinPol}_{\mathbb{F}_q}(\omega)$ divides A.
χ_ϕ 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 $\mathcal{O} = \mathrm{End}_{\mathbb{F}_q}(E)$.
Then, $\mathrm{Cl}(\mathcal{O})$ 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 $\geqslant 5$. Let ϕ be some ordinary rank two finite Drinfeld module. Fix $\mathcal{O} = \mathrm{End}_L(\phi)$.
Assume χ_ϕ defines an imaginary hyperelliptic curve $\mathcal{H}$.
Then, $\mathrm{Cl}(\mathcal{O}) \simeq \mathrm{Pic}^0(\mathcal{H})$ and $\mathrm{Cl}(\mathcal{O})$ acts simply transitively on the set of $\overline{L}$-isomorphism classes of rank 1 Drinfeld modules $\mathcal{O} \to L\{\tau\}$.

Definition of the action

Let $\mathfrak{a} \in \mathrm{Id}(\mathcal{O})$, let ϕ' be a representative. Let

$$V_{\mathfrak{a}} = \bigcap_{f \in \mathfrak{a}} \mathrm{Ker}(f).$$

$V_{\mathfrak{a}}$ is the kernel of some isogeny $\iota_{\mathfrak{a}}$ with domain ϕ'. We associate

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

Definition

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

Isomorphism $\mathrm{Cl}(\mathcal{O}) \simeq \mathrm{Pic}^0(\mathcal{H})$

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

$$\mathrm{Cl}(\mathcal{O}) \simeq \mathrm{Pic}^0(\mathcal{H}).$$

Mumford coordinates for $\mathrm{Pic}^0(\mathcal{H})$

Representation with Mumford coordinates:

$$\mathrm{Pic}^0(\mathcal{H}) \longleftrightarrow \mathrm{Cl}(\mathbb{F}_q[X][Y]/\chi_\phi)$$
$$(u,v) \longleftrightarrow \text{Class of } \langle u(\overline{X}), \overline{Y} - v(\overline{X})\rangle$$

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

Explicit computation

$$V_{\mathfrak{a}} = \mathrm{Ker}(\iota_{\mathfrak{a}}) = \bigcap_{f \in \mathfrak{a}} \mathrm{Ker}(f) = \bigcap_{\overline{f} \in \langle u(\overline{X}), \overline{Y} - v(\overline{X}) \rangle} \mathrm{Ker}(f(\phi(X), \tau_L)).$$

Therefore

$$\iota_{\mathfrak{a}} = \mathrm{rgcd}\left(\phi(u), \tau_L - \phi(v)\right).$$

Algorithm

Input: — A j-invariant $j \in L$.

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

Output: A j-invariant.

$\widetilde{u} \leftarrow u(j^{-1}\tau^2 + \tau + \omega) \in L\{\tau\}$;

$\widetilde{v} \leftarrow v(j^{-1}\tau^2 + \tau + \omega) \in L\{\tau\}$;

$\iota \leftarrow \mathrm{rgcd}(\widetilde{u}, \tau^{[L:\mathbb{F}_q]} - \widetilde{v})$;

$\widehat{g} \leftarrow \iota_0^{-q}(\iota_0 + \iota_1(\omega^q - \omega))$;

$\widehat{\Delta} \leftarrow j^{-q^{\deg_\tau(\iota)}}$;

Return $\widehat{g}^{q+1}/\widehat{\Delta}$.

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 $\frac{521-1}{2} = 260$, $\mathrm{Pic}^0(\mathcal{H})$ has order

$$2 \times 31541318246754567260411631641504\ldots$$

$$\ldots 7743350494962889744865259442943656024073295689.$$

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 $\phi(X) = \Delta\tau^2 + g\tau + \omega$, $\psi(X) = \Delta'\tau^2 + g'\tau + \omega$, $\iota = \iota_a\tau^a + \cdots + \iota_0 \in L\{\tau\}$.
Then ι is an isogeny $\phi \to \psi$ *iif*

$$
\begin{aligned}
\Delta'\iota_a^{q^2} - \Delta^{q^a}\iota_a &= 0, \\
\Delta'\iota_{a-1}^{q^2} - \Delta^{q^{a-1}}\iota_{a-1} &= \iota_a g^{q^a} - g'\iota_a^q, \\
\forall k \in [\![2, a]\!], \quad \Delta'\iota_{a-k}^{q^2} - \Delta^{q^{a-k}}\iota_{a-k} &= \iota_{a-k+1}g^{q^{a-k+1}} - g'\iota_{a-k+1}^q + \iota_{a-k+2}(\omega^{q^{a-k+2}} - \omega), \\
\iota_0 g + \iota_1\omega^q &= \omega\iota_1 + g'\iota_0^q.
\end{aligned}
$$

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).

Conclusion

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).