An explicit CRS-like action with Drinfeld modules

Séminaire de l'équipe GRACE

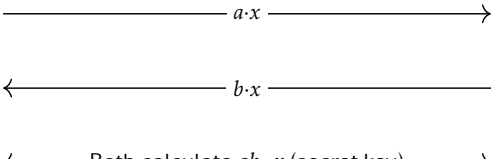
Antoine Leudière Pierre-Jean Spaenlehauer

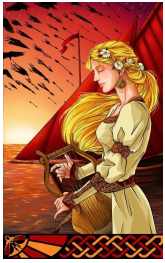
INRIA Nancy-Grand Est

Mai 2022

Hard homogenous spaces (1/2)

Tristan and Isolde choose an abelian group G acting freely and transitively on a set X, with an element $x \in X$.





The protocol is secure if (among other things) it is hard to compute $ab \cdot x$ knowing $x, a \cdot x$ and $b \cdot x$.

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.

The computation is explicit, but slow (De Feo, Kieffer, Smith, 2019).

What about CSIDH?

CSIDH is way more efficient.
But… (like for CRS) the corresponding group is the class group of a imaginary quadratic number field.
Those groups are extremely hard to compute (Beullens, Kleinjung, Vercauteren, 2019).

What if we used imaginary hyperelliptic curves instead of imaginary quadratic number fields?
The analogue of the class group would be the Jacobian: computable with Kedlaya's algorithm.
We could build post-quantum signature schemes (Beullens, Kleinjung, Vercauteren, 2019).

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: easy-ish 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 $p \nmid n$	$\phi[a] \simeq (\mathbb{F}_q[X]/a)^r$ if $\mathfrak{p} \nmid a$
$E[p] \simeq (\mathbb{Z}/p)^{s \in \{0,1\}}$	$\phi[\mathfrak{p}] \simeq (\mathbb{F}_q[X]/\mathfrak{p})^{s \in \{0,\ldots,r-1\}}$
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, and proof that it is simply transitive.
- Definition of an algorithm to compute the action.
- Efficient C++/NTL implementation.
- Ongoing SageMath implementation of Drinfeld modules (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 denote a *potential* Drinfeld module. Let $a, b \in \mathbb{F}_q[X]$, let $x, y \in \overline{\mathbb{F}_q}$, let $\lambda \in \mathbb{F}_q$. Let's choose to 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 $\overline{\mathbb{F}_q}$ (1/2)

A morphism in $\mathrm{End}_{\mathbb{F}_q}(\overline{\mathbb{F}_q})$ has the form

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

Denote

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

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

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

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

Let L be a sub-extension of $\overline{\mathbb{F}_q}/\mathbb{F}_q$. 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 $L\{\tau\}$ is called *ring of Ore polynomials in τ with coefficients in L*.

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

Let $L/\mathbb{F}_q$ be finite; fix $\omega \in \text{Ł}^\times$.

Definition (Drinfeld, 1974)

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

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

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

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

Let $\phi : \mathbb{F}_q[X] \to L\{\tau\}$ be a finite Drinfeld module. ϕ is uniquely determined by $\phi(X)$. Write:

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

The *rank of* ϕ is n.

Rank 2 finite Drinfeld modules are closest to elliptic curves over finite fields.

Properties of $L\{\tau\}$

- $L\{\tau\}$ is non commutative if $\mathbb{F}_q \neq L$:

$$\tau l = l^q \tau, \quad \forall l \in L.$$

- $L\{\tau\}$ is left-euclidean w.r.t. to the τ-degree: for all P_1, P_2 in $L\{\tau\}$ with $\deg_\tau(P_1) \geqslant \deg_\tau(P_2)$, there exists Q, R in $L\{\tau\}$ such that:

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

- We can compute RGCD in $L\{\tau\}$.
- SageMath implementation (Xavier Caruso).

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 $\tau_L = x \mapsto x^{\#L}$:

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

Complex multiplication

Assume ϕ has rank two.
The *characteristic polynomial of the Frobenius endomorphism of* ϕ is the unique polynomial

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

such that

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

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

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

χ 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

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

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

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

Endomorphisms always contain $\mathbb{F}_q[X]$ and the Frobenius endomorphism τ_L.
In our case, that's it, i.e.

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

Consequence:

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

Representation with Mumford coordinates:

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

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

Explicit computation

By definition, the isogeny $\iota_{\mathfrak{a}}$ is the one with kernel

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

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.

1 $\widetilde{u} \leftarrow u(j^{-1}\tau^2 + \tau + \omega) \in L\{\tau\}$;
2 $\widetilde{v} \leftarrow v(j^{-1}\tau^2 + \tau + \omega) \in L\{\tau\}$;
3 $\iota \leftarrow \mathrm{rgcd}(\widetilde{u}, \tau^{[L:\mathbb{F}_q]} - \widetilde{v})$;
4 $\widehat{g} \leftarrow \iota_0^{-q}(\iota_0 + \iota_1(\omega^q - \omega))$;
5 $\widehat{\Delta} \leftarrow j^{-q^{\deg_\tau(\iota)}}$;
6 **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

$$2 \times 3154131824675456726041163164150 4\ldots$$

$$\ldots 7743350494962889744865259442943656024073295689.$$

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

Drinfeld modules are already classical in abstract mathematics (arithmetic of function fields). There is a flourishing research focusing on algorithmic aspects: Gekeler (1998); Joux, Narayanan (2019); Caranay (thesis, 2018); Caranay, Greenberg, Scheidler (2019); Schost, Musleh (2019).
Yet vast algorithmic areæ remain unexplored (rank > 2, T-modules, general Drinfeld modules). We aim to develop algorithmic and software toolboxes.
We are looking at the links with class field theory, as suggested by Couveignes in 1996.