Hard Homogeneous Spaces from the Class Field Theory of Imaginary Hyperelliptic Function Fields

JNCF 2022

Antoine Leudière Pierre-Jean Spaenlehauer

INRIA Nancy-Grand Est

Diffie-Hellman (1976)

Tristan and Isolde create a private key on a public chanel. They choose a finite cyclic group $G = \langle g \rangle$.

Diffie-Hellman (1976)

Tristan and Isolde create a private key on a public chanel. They choose a finite cyclic group $G = \langle g \rangle$.

$$\xrightarrow{\quad g^a \quad}$$

Diffie-Hellman (1976)

Tristan and Isolde create a private key on a public chanel. They choose a finite cyclic group $G = \langle g \rangle$.

$$\xrightarrow{\quad g^a \quad}$$

$$\xleftarrow{\quad g^b \quad}$$

Diffie-Hellman (1976)

Tristan and Isolde create a private key on a public chanel. They choose a finite cyclic group $G = \langle g \rangle$.

$\xrightarrow{\quad g^a \quad}$

$\xleftarrow{\quad g^b \quad}$

$\leftarrow$ - - - - - - - - - Both calculate (g^{ab}) - - - - - - - - - $\rightarrow$

Diffie-Hellman (1976)

Tristan and Isolde create a private key on a public chanel. They choose a finite cyclic group $G = \langle g \rangle$.

$\longrightarrow$ g^a $\longrightarrow$

$\longleftarrow$ g^b $\longleftarrow$

$\leftarrow$ - - - - Both calculate (g^{ab}) - - - - $\rightarrow$

Secure if hard to compute g^{ab} knowing g, g^a and g^b.

Diffie-Hellman (1976)

Tristan and Isolde create a private key on a public chanel. They choose a finite cyclic group $G = \langle g \rangle$.

$\xrightarrow{\quad g^a \quad}$

$\xleftarrow{\quad g^b \quad}$

$\leftarrow$ - - - - - - - - - Both calculate (g^{ab}) - - - - - - - - - $\rightarrow$

Secure if hard to compute g^{ab} knowing g, g^a and g^b.

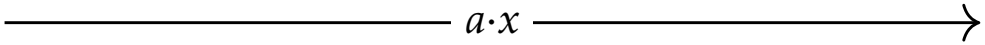
Shor's quantum algorithm breaks this problem for any group.

Hard homogeneous spaces (Couveignes, 1996)

Tristan and Isolde create a private key on a public chanel. They choose an abelian group G acting (freely and transitively) on a set X, with an element $x \in X$.

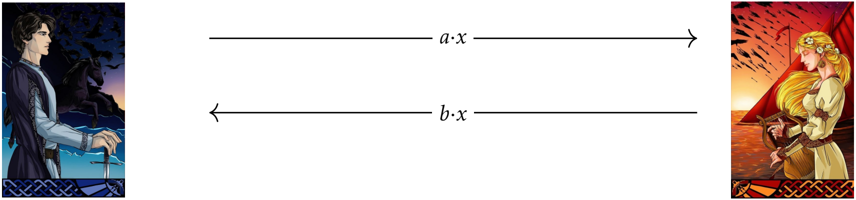
Hard homogeneous spaces (Couveignes, 1996)

Tristan and Isolde create a private key on a public chanel. They choose an abelian group G acting (freely and transitively) on a set X, with an element $x \in X$.



Hard homogeneous spaces (Couveignes, 1996)

Tristan and Isolde create a private key on a public chanel. They choose an abelian group G acting (freely and transitively) on a set X, with an element $x \in X$.



Hard homogeneous spaces (Couveignes, 1996)

Tristan and Isolde create a private key on a public chanel. They choose an abelian group G acting (freely and transitively) on a set X, with an element $x \in X$.

$a \cdot x$ →

← $b \cdot x$

← Both calculate $ab \cdot x$ →

Hard homogeneous spaces (Couveignes, 1996)

Tristan and Isolde create a private key on a public chanel. They choose an abelian group G acting (freely and transitively) on a set X, with an element $x \in X$.

$a \cdot x$ →

← $b \cdot x$

← Both calculate $ab \cdot x$ →

Secure if hard to compute $ab \cdot x$ knowing $x, a \cdot x$ and $b \cdot x$.

Hard homogeneous spaces (Couveignes, 1996)

Tristan and Isolde create a private key on a public chanel. They choose an abelian group G acting (freely and transitively) on a set X, with an element $x \in X$.

$\xrightarrow{\quad a \cdot x \quad}$

$\xleftarrow{\quad b \cdot x \quad}$

$\longleftarrow$ Both calculate $ab \cdot x$ $\longrightarrow$

Secure if hard to compute $ab \cdot x$ knowing $x, a \cdot x$ and $b \cdot x$.

Quantum attack in $\exp(c\sqrt{\log(\#G)})$ for some $c > 0$ (Kuperberg, 2005).

CRS

Couveignes, 1997; Rostovtsev, Stolbunov, 2006:

CRS

Couveignes, 1997; Rostovtsev, Stolbunov, 2006:

- X: subset of isomorphism classes of ordinary elliptic curves on $\mathbb{F}_q$ with prescribed endomorphism ring and Frobenius trace.

CRS

Couveignes, 1997; Rostovtsev, Stolbunov, 2006:

- X: subset of isomorphism classes of ordinary elliptic curves on $\mathbb{F}_q$ with prescribed endomorphism ring and Frobenius trace.
- G: Class group of their endomorphism ring.

CRS

Couveignes, 1997; Rostovtsev, Stolbunov, 2006:

- X: subset of isomorphism classes of ordinary elliptic curves on $\mathbb{F}_q$ with prescribed endomorphism ring and Frobenius trace.
- G: Class group of their endomorphism ring.

Despite recent improvements (De Feo, Kieffer, Smith, 2018), calculations are take several minutes.

CRS

Couveignes, 1997; Rostovtsev, Stolbunov, 2006:

- X: subset of isomorphism classes of ordinary elliptic curves on $\mathbb{F}_q$ with prescribed endomorphism ring and Frobenius trace.
- G: Class group of their endomorphism ring.

Despite recent improvements (De Feo, Kieffer, Smith, 2018), calculations are take several minutes.

CSIDH (Castryck, Lange, Martindale, Panny, Renes, 2018) does better, but the structure of thei G is very hard to compute.

Number fields and function fields

Number fields	Function fields

Number fields and function fields

Number fields	Function fields
$\mathbb{Z}$	$\mathbb{F}_q[X]$

Number fields and function fields

Number fields	Function fields
$\mathbb{Z}$	$\mathbb{F}_q[X]$
$\mathbb{Q}$	$\mathbb{F}_q(X)$

Number fields and function fields

Number fields	Function fields
$\mathbb{Z}$	$\mathbb{F}_q[X]$
$\mathbb{Q}$	$\mathbb{F}_q(X)$
Number field	Function field

Elliptic curves and Drinfeld modules

Elliptic curves over $\mathbb{F}_q$	Finite Drinfeld modules

Elliptic curves and Drinfeld modules

Elliptic curves over $\mathbb{F}_q$	Finite Drinfeld modules
$\mathbb{Z}$-module law on $\mathcal{E}(\overline{\mathbb{F}_q})$	$\mathbb{F}_q[X]$-module law on $\overline{\mathbb{F}_q}$

Elliptic curves and Drinfeld modules

Elliptic curves over $\mathbb{F}_q$	Finite Drinfeld modules
$\mathbb{Z}$-module law on $\mathcal{E}(\overline{\mathbb{F}_q})$	$\mathbb{F}_q[X]$-module law on $\overline{\mathbb{F}_q}$
Any finite $\mathbb{Z}$-module gives rise to a separable isogeny	Any finite sub-$\mathbb{F}_q[X]$-module of $\overline{\mathbb{F}_q}$ (+ technical condition)

Elliptic curves and Drinfeld modules

Elliptic curves over $\mathbb{F}_q$	Finite Drinfeld modules
$\mathbb{Z}$-module law on $\mathcal{E}(\overline{\mathbb{F}_q})$	$\mathbb{F}_q[X]$-module law on $\overline{\mathbb{F}_q}$
Any finite $\mathbb{Z}$-module gives rise to a separable isogeny	Any finite sub-$\mathbb{F}_q[X]$-module of $\overline{\mathbb{F}_q}$ (+ technical condition)
Endomorphisms form a free $\mathbb{Z}$-module of rank 2 or 4	Endomorphisms form a free $\mathbb{F}_q[X]$-module of rank 2 or 4

Elliptic curves and Drinfeld modules

Elliptic curves over $\mathbb{F}_q$	**Finite Drinfeld modules**
$\mathbb{Z}$-module law on $\mathcal{E}(\overline{\mathbb{F}_q})$	$\mathbb{F}_q[X]$-module law on $\overline{\mathbb{F}_q}$
Any finite $\mathbb{Z}$-module gives rise to a separable isogeny	Any finite sub-$\mathbb{F}_q[X]$-module of $\overline{\mathbb{F}_q}$ (+ technical condition)
Endomorphisms form a free $\mathbb{Z}$-module of rank 2 or 4	Endomorphisms form a free $\mathbb{F}_q[X]$-module of rank 2 or 4
j-invariant encoding $\overline{\mathbb{F}_q}$-isomorphism classes	

Elliptic curves and Drinfeld modules

Elliptic curves over $\mathbb{F}_q$	Finite Drinfeld modules
$\mathbb{Z}$-module law on $\mathcal{E}(\overline{\mathbb{F}_q})$	$\mathbb{F}_q[X]$-module law on $\overline{\mathbb{F}_q}$
Any finite $\mathbb{Z}$-module gives rise to a separable isogeny	Any finite sub-$\mathbb{F}_q[X]$-module of $\overline{\mathbb{F}_q}$ (+ technical condition)
Endomorphisms form a free $\mathbb{Z}$-module of rank 2 or 4	Endomorphisms form a free $\mathbb{F}_q[X]$-module of rank 2 or 4
j-invariant encoding $\overline{\mathbb{F}_q}$-isomorphism classes	
Characteristic polynomial	

Elliptic curves and Drinfeld modules

Elliptic curves over $\mathbb{F}_q$	Finite Drinfeld modules
$\mathbb{Z}$-module law on $\mathcal{E}(\overline{\mathbb{F}_q})$	$\mathbb{F}_q[X]$-module law on $\overline{\mathbb{F}_q}$
Any finite $\mathbb{Z}$-module gives rise to a separable isogeny	Any finite sub-$\mathbb{F}_q[X]$-module of $\overline{\mathbb{F}_q}$ (+ technical condition)
Endomorphisms form a free $\mathbb{Z}$-module of rank 2 or 4	Endomorphisms form a free $\mathbb{F}_q[X]$-module of rank 2 or 4
j-invariant encoding $\overline{\mathbb{F}_q}$-isomorphism classes	
Characteristic polynomial	
Two families: ordinary and supersingular	

Main results

- Description of a setting in which a general action is simply transitive; proof.

Main results

- Description of a setting in which a general action is simply transitive; proof.
- Efficient algorithm to compute the action.

Main results

- Description of a setting in which a general action is simply transitive; proof.
- Efficient algorithm to compute the action.
- C++/NTL implementation of the key-exchange; proof of concept.

Main results

- Description of a setting in which a general action is simply transitive; proof.
- Efficient algorithm to compute the action.
- C++/NTL implementation of the key-exchange; proof of concept.
- SageMath library for finite Drinfeld modules; we aim for an integration in SageMath.

Main results

- Description of a setting in which a general action is simply transitive; proof.
- Efficient algorithm to compute the action.
- C++/NTL implementation of the key-exchange; proof of concept.
- SageMath library for finite Drinfeld modules; we aim for an integration in SageMath.
- Numerical experiments suggest that the inverse problem of the action is hard.

Ore polynomials (1/2)

Fix $\mathbb{F}_q \hookrightarrow L \hookrightarrow \overline{\mathbb{F}_q}$ a finite field extension and

$$\begin{aligned} \tau : \overline{\mathbb{F}_q} &\to \overline{\mathbb{F}_q} \\ x &\mapsto x^q. \end{aligned}$$

Ore polynomials (1/2)

Fix $\mathbb{F}_q \hookrightarrow L \hookrightarrow \overline{\mathbb{F}_q}$ a finite field extension and

$$\begin{aligned} \tau : \overline{\mathbb{F}_q} &\to \overline{\mathbb{F}_q} \\ x &\mapsto x^q. \end{aligned}$$

Definition (Ore, 1933)

The set

$$L\{\tau\} := \left\{ \sum_{0 \leqslant i \leqslant n} a_n \tau^i \mid n \in \mathbb{Z}_{\geqslant 0}, a_i \in L \right\} \subset \mathrm{End}_{\mathbb{F}_q}(\overline{\mathbb{F}_q})$$

is a ring for addition and composition, called the *ring of Ore polynomials*.

Ore polynomials (2/2)

$$\begin{aligned} \tau : \overline{\mathbb{F}_q} &\to \overline{\mathbb{F}_q} \\ x &\mapsto x^q. \end{aligned}$$

$$L\{\tau\} := \left\{ \sum_{0 \leqslant i \leqslant n} a_n \tau^i \mid n \in \mathbb{Z}_{\geqslant 0}, a_i \in L \right\} \subset \mathrm{End}_{\mathbb{F}_q}(\overline{\mathbb{F}_q})$$

Properties:

Ore polynomials (2/2)

$$\begin{aligned} \tau : \overline{\mathbb{F}_q} &\to \overline{\mathbb{F}_q} \\ x &\mapsto x^q. \end{aligned}$$

$$L\{\tau\} := \left\{ \sum_{0 \leqslant i \leqslant n} a_n \tau^i \mid n \in \mathbb{Z}_{\geqslant 0}, a_i \in L \right\} \subset \mathrm{End}_{\mathbb{F}_q}(\overline{\mathbb{F}_q})$$

Properties:

- $L\{\tau\}$ is non commutative: $\tau a = a^q \tau, \quad \forall a \in L$.

Ore polynomials (2/2)

$$\begin{aligned} \tau : \overline{\mathbb{F}_q} &\to \overline{\mathbb{F}_q} \\ x &\mapsto x^q. \end{aligned}$$

$$L\{\tau\} := \left\{ \sum_{0 \leqslant i \leqslant n} a_n \tau^i \mid n \in \mathbb{Z}_{\geqslant 0}, a_i \in L \right\} \subset \mathrm{End}_{\mathbb{F}_q}(\overline{\mathbb{F}_q})$$

Properties:

- $L\{\tau\}$ is non commutative: $\tau a = a^q \tau, \quad \forall a \in L.$
- $L\{\tau\}$ is left-euclidean
  $\longrightarrow$ notion of rgcd
  $\longrightarrow$ many algorithmic perspectives!

Ore polynomials (2/2)

$$\begin{aligned} \tau : \overline{\mathbb{F}_q} &\to \overline{\mathbb{F}_q} \\ x &\mapsto x^q. \end{aligned}$$

$$L\{\tau\} := \left\{ \sum_{0 \leqslant i \leqslant n} a_n \tau^i \mid n \in \mathbb{Z}_{\geqslant 0}, a_i \in L \right\} \subset \mathrm{End}_{\mathbb{F}_q}(\overline{\mathbb{F}_q})$$

Properties:

- $L\{\tau\}$ is non commutative: $\tau a = a^q \tau, \quad \forall a \in L.$
- $L\{\tau\}$ is left-euclidean
  $\longrightarrow$ notion of rgcd
  $\longrightarrow$ many algorithmic perspectives!
- SageMath implementation by X. Caruso.

Drinfeld modules on $\mathbb{F}_q[X]$

Definition (Drinfeld, 1974)

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

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

such that

- there exists $a \in \mathbb{F}_q[X]$ such that $\deg_\tau(\phi(a)) > 0$,
- for all $a \in \mathbf{A}$ the constant term of $\phi(a)$ is $\overline{X}$.

Drinfeld modules on $\mathbb{F}_q[X]$

Definition (Drinfeld, 1974)

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

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

such that

- there exists $a \in \mathbb{F}_q[X]$ such that $\deg_\tau(\phi(a)) > 0$,
- for all $a \in \mathbf{A}$ the constant term of $\phi(a)$ is $\overline{X}$.

As a morphism, ϕ is uniquely determined by $\phi(X)$. We consider ϕ defined by

$$\phi(X) = \omega + g\tau + \Delta\tau^2, \quad g \in L, \Delta \in L^\times.$$

Drinfeld modules on $\mathbb{F}_q[X]$

Definition (Drinfeld, 1974)

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

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

such that

- there exists $a \in \mathbb{F}_q[X]$ such that $\deg_\tau(\phi(a)) > 0$,
- for all $a \in \mathbf{A}$ the constant term of $\phi(a)$ is $\overline{X}$.

As a morphism, ϕ is uniquely determined by $\phi(X)$. We consider ϕ defined by

$$\phi(X) = \omega + g\tau + \Delta\tau^2, \quad g \in L, \Delta \in L^\times.$$

Those are *rank 2* Drinfeld modules over L.

Characteristic polynomial (1/2)

Let:

Characteristic polynomial (1/2)

Let:

- ϕ: rank 2 Drinfeld module,

Characteristic polynomial (1/2)

Let:

- ϕ: rank 2 Drinfeld module,
- $\tau_L = \tau^{[L:\mathbb{F}_q]}$.

Characteristic polynomial (1/2)

Let:

- ϕ: rank 2 Drinfeld module,
- $\tau_L = \tau^{[L:\mathbb{F}_q]}$.

Theorem (Gekeler, 1991)

There exists $\xi \in \mathbb{F}_q[X][Y]$ such that:

$$\xi(\phi(X), \tau_L) = 0$$

Characteristic polynomial (1/2)

Let:

- ϕ: rank 2 Drinfeld module,
- $\tau_L = \tau^{[L:\mathbb{F}_q]}$.

Theorem (Gekeler, 1991)

There exists $\xi \in \mathbb{F}_q[X][Y]$ such that:

$$\xi(\phi(X), \tau_L) = 0$$

and

$$\begin{cases} \xi = Y^2 + h(X)Y - f(X), \\ \deg(f) = [L : \mathbb{F}_q], \quad \textit{(Hasse-Weil bounds)} \\ \deg(h) \leqslant [L : \mathbb{F}_q]/2. \end{cases}$$

Characteristic polynomial (1/2)

Let:

- ϕ: rank 2 Drinfeld module,
- $\tau_L = \tau^{[L:\mathbb{F}_q]}$.

Theorem (Gekeler, 1991)

There exists $\xi \in \mathbb{F}_q[X][Y]$ such that:

$$\xi(\phi(X), \tau_L) = 0$$

and

$$\begin{cases} \xi = Y^2 + h(X)Y - f(X), \\ \deg(f) = [L : \mathbb{F}_q], \quad \text{(Hasse-Weil bounds)} \\ \deg(h) \leqslant [L : \mathbb{F}_q]/2. \end{cases}$$

Characteristic polynomial (2/2)

If $2 \nmid [L : \mathbb{F}_q]$ and the curve defined by the characteristic polynomial ξ is smooth, then it is an *imaginary hyperelliptic curve*.

Characteristic polynomial (2/2)

If $2 \nmid [L : \mathbb{F}_q]$ and the curve defined by the characteristic polynomial ξ is smooth, then it is an *imaginary hyperelliptic curve*.

Efficiently computed (Musleh, Schost, 2019).

Definition of the action

Assume $\xi \in \mathbb{F}_q[X][Y]$ defines an hyperelliptic curve.

Definition of the action

Assume $\xi \in \mathbb{F}_q[X][Y]$ defines an hyperelliptic curve. Let:

- ϕ: rank 2 with characteristic polynomial ξ,

Definition of the action

Assume $\xi \in \mathbb{F}_q[X][Y]$ defines an hyperelliptic curve. Let:

- ϕ: rank 2 with characteristic polynomial ξ,
- I: ideal of $\mathbb{F}_q[X][Y]/\xi$,

Definition of the action

Assume $\xi \in \mathbb{F}_q[X][Y]$ defines an hyperelliptic curve. Let:

- ϕ: rank 2 with characteristic polynomial ξ,
- I: ideal of $\mathbb{F}_q[X][Y]/\xi$,
- $I \star \phi$: Drinfeld module ψ associated to ϕ and

$$\bigcap_{\overline{f} \in I} \mathrm{Ker}\left(f\left(\phi(X), \tau_L\right)\right).$$

Definition of the action

Assume $\xi \in \mathbb{F}_q[X][Y]$ defines an hyperelliptic curve. Let:

- ϕ: rank 2 with characteristic polynomial ξ,
- I: ideal of $\mathbb{F}_q[X][Y]/\xi$,
- $I \star \phi$: Drinfeld module ψ associated to ϕ and

$$\bigcap_{f \in I} \operatorname{Ker}(f(\phi(X), \tau_L)).$$

Theorem

If $2 \nmid [L : \mathbb{F}_q]$, the map $(I, \phi) \mapsto I \star \phi$ extends to a group action of

$$\mathrm{Cl}(\mathbb{F}_q[X][Y]/\xi)$$

to

$$\left\{ \mathrm{Isom}_{\overline{\mathbb{F}_q}}(\phi) \mid \mathrm{Rank}(\phi) = 2, \mathrm{CharPol}(\phi) = \xi \right\}.$$

Algorithm

Assume ξ defines an hyperelliptic curve $\mathcal{H}$.

Representation:

- Ideal classes: $\mathrm{Cl}(\mathbb{F}_q[X][Y]/\xi) \simeq \mathrm{Pic}_0(\mathcal{H})$

Algorithm

Assume ξ defines an hyperelliptic curve $\mathcal{H}$.
Representation:

- Ideal classes: $\mathrm{Cl}(\mathbb{F}_q[X][Y]/\xi) \simeq \mathrm{Pic}_0(\mathcal{H})$
  $\longrightarrow$ Mumford coordinates $(u, v) \in \mathbb{F}_q[X]^2$.

Algorithm

Assume ξ defines an hyperelliptic curve $\mathcal{H}$.
Representation:

- Ideal classes: $\mathrm{Cl}(\mathbb{F}_q[X][Y]/\xi) \simeq \mathrm{Pic}_0(\mathcal{H})$
  $\longrightarrow$ Mumford coordinates $(u, v) \in \mathbb{F}_q[X]^2$.
- Isomorphism classes: j-invariants in L.

Algorithm

Assume ξ defines an hyperelliptic curve $\mathcal{H}$.
Representation:

- Ideal classes: $\mathrm{Cl}(\mathbb{F}_q[X][Y]/\xi) \simeq \mathrm{Pic}_0(\mathcal{H})$
  $\longrightarrow$ Mumford coordinates $(u, v) \in \mathbb{F}_q[X]^2$.
- Isomorphism classes: j-invariants in L.

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

Output: A j-invariant.

$\widetilde{u} \leftarrow u(j^{-1}\tau^2 + \tau + \omega) \in L\{\tau\}$;
$\widetilde{v} \leftarrow v(j^{-1}\tau^2 + \tau + \omega) \in L\{\tau\}$;
$\iota \leftarrow \mathrm{rgcd}(\widetilde{u}, \tau_L - \widetilde{v})$;
$\widehat{g} \leftarrow \iota_0^{-q}(\iota_0 + \iota_1(\omega^q - \omega))$;
$\widehat{\Delta} \leftarrow j^{-q^{\deg_\tau(\iota)}}$;
Return $\widehat{g}^{q+1}/\widehat{\Delta}$.

Let:

Let:

- $\mathbf{k}$: algebraic function field with transcendance degree 1 over $\mathbb{F}_q$,

Let:

- $\mathbf{k}$: algebraic function field with transcendance degree 1 over $\mathbb{F}_q$,
- ∞: place of $\mathbf{k}$,

Let:

- $\mathbf{k}$: algebraic function field with transcendance degree 1 over $\mathbb{F}_q$,
- ∞: place of $\mathbf{k}$,
- $\mathbf{A}$: ring of functions that are regular outside ∞,

Let:

- $\mathbf{k}$: algebraic function field with transcendance degree 1 over $\mathbb{F}_q$,
- ∞: place of $\mathbf{k}$,
- $\mathbf{A}$: ring of functions that are regular outside ∞,
- $\gamma : \mathbf{A} \to L$: $\mathbb{F}_q$-algebra morphism.

Let:

- $\mathbf{k}$: algebraic function field with transcendance degree 1 over $\mathbb{F}_q$,
- ∞: place of $\mathbf{k}$,
- $\mathbf{A}$: ring of functions that are regular outside ∞,
- $\gamma : \mathbf{A} \to L$: $\mathbb{F}_q$-algebra morphism.

Definition

A *Drinfeld $\mathbf{A}$-module over L* is an $\mathbb{F}_q$-algebra morphism $\phi : \mathbf{A} \to L$ such that:

- there exists $a \in \mathbf{A}$ such that $\deg_\tau(\phi(a)) > 0$,
- for all $a \in \mathbf{A}$ the constant term of $\phi(a)$ is $\gamma(a)$.

Let:

- $\mathbf{k}$: algebraic function field with transcendance degree 1 over $\mathbb{F}_q$,
- ∞: place of $\mathbf{k}$,
- $\mathbf{A}$: ring of functions that are regular outside ∞,
- $\gamma : \mathbf{A} \to L$: $\mathbb{F}_q$-algebra morphism.

Definition

A *Drinfeld $\mathbf{A}$-module over L* is an $\mathbb{F}_q$-algebra morphism $\phi : \mathbf{A} \to L$ such that:

- there exists $a \in \mathbf{A}$ such that $\deg_\tau(\phi(a)) > 0$,
- for all $a \in \mathbf{A}$ the constant term of $\phi(a)$ is $\gamma(a)$.

Theorem (Drinfeld, 1974)

The group $\mathrm{Cl}(\mathbf{A})$ acts on the set of $\overline{\mathbb{F}_q}$-isomorphism classes of Drinfeld $\mathbf{A}$-modules over L with rank r.

Let:

- $\mathbf{k}$: algebraic function field with transcendance degree 1 over $\mathbb{F}_q$,
- ∞: place of $\mathbf{k}$,
- $\mathbf{A}$: ring of functions that are regular outside ∞,
- $\gamma : \mathbf{A} \to L$: $\mathbb{F}_q$-algebra morphism.

Definition

A *Drinfeld $\mathbf{A}$-module over L* is an $\mathbb{F}_q$-algebra morphism $\phi : \mathbf{A} \to L$ such that:

- there exists $a \in \mathbf{A}$ such that $\deg_\tau(\phi(a)) > 0$,
- for all $a \in \mathbf{A}$ the constant term of $\phi(a)$ is $\gamma(a)$.

Theorem (Drinfeld, 1974)

The group $\mathrm{Cl}(\mathbf{A})$ acts on the set of $\overline{\mathbb{F}_q}$-isomorphism classes of Drinfeld $\mathbf{A}$-modules over L with rank r.

Our action is realized with $\mathbf{A} = \mathbb{F}_q[X][Y]/\xi$ and $r = 1$.

Conclusion

- The group action is a adaptation of Couveignes-Rostovtsev-Stolbunov to Drinfeld modules.

Conclusion

- The group action is a adaptation of Couveignes-Rostovtsev-Stolbunov to Drinfeld modules.
- The algorithm only requires elementary arithmetic tools.

Conclusion

- The group action is a adaptation of Couveignes-Rostovtsev-Stolbunov to Drinfeld modules.
- The algorithm only requires elementary arithmetic tools.
- After partial results and numerical experiments, we conjecture that the problem of inverting the action is hard (studied by Joux, Narayanan, 2019; and by Caranay, Greenberg, Scheidler, 2020).

Conclusion

- The group action is a adaptation of Couveignes-Rostovtsev-Stolbunov to Drinfeld modules.
- The algorithm only requires elementary arithmetic tools.
- After partial results and numerical experiments, we conjecture that the problem of inverting the action is hard (studied by Joux, Narayanan, 2019; and by Caranay, Greenberg, Scheidler, 2020).
- With $q = 2$ and $L = \mathbb{F}_{2^{521}}$, the key exchange is calculated in $\simeq 200$ ms with our C++ / NTL implementation.

Conclusion

- The group action is a adaptation of Couveignes-Rostovtsev-Stolbunov to Drinfeld modules.
- The algorithm only requires elementary arithmetic tools.
- After partial results and numerical experiments, we conjecture that the problem of inverting the action is hard (studied by Joux, Narayanan, 2019; and by Caranay, Greenberg, Scheidler, 2020).
- With $q = 2$ and $L = \mathbb{F}_{2^{521}}$, the key exchange is calculated in $\simeq 200$ ms with our C++ / NTL implementation.
- The structure of the group is calculated in 53 hours in our case (Kedlaya-Vercauteren alg.); 52 CPU-years for CSIDH-512 (Beullens, Kleinjung, Vercauteren, 2019).

Perspectives

- Proving that the current best known algorithm to solve the inverse problem runs in exponential time.

Perspectives

- Proving that the current best known algorithm to solve the inverse problem runs in exponential time.
- Finding optimal cryptographic parameters.

Perspectives

- Proving that the current best known algorithm to solve the inverse problem runs in exponential time.
- Finding optimal cryptographic parameters.
- Contributing to SageMath with our framework for Drinfeld modules.

Perspectives

- Proving that the current best known algorithm to solve the inverse problem runs in exponential time.
- Finding optimal cryptographic parameters.
- Contributing to SageMath with our framework for Drinfeld modules.

Thank you!