Function field analogue of the CRS key exchange

Journées C2 2022

Antoine Leudière Pierre-Jean Spaenlehauer

INRIA Nancy-Grand Est

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 (finite ext.)	Function field (finite ext.)

Number fields and function fields

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

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

Number fields and function fields

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

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

Number fields and function fields

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

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

Number fields and function fields

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

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

Number fields and function fields

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

Elliptic curves over $\mathbb{F}_q$	Finite Drinfeld modules
$\mathbb{Z}$-module law on $E(\overline{\mathbb{F}_q})$	$\mathbb{F}_q[X]$-module law on $\overline{\mathbb{F}_q}$
Any finite $\mathbb{Z}$-module gives rise to an isogeny	Any finite sub-$\mathbb{F}_q[X]$-module of $\overline{\mathbb{F}_q}$ (+ technical condition) gives rise to an isogeny
j-invariant encoding $\overline{\mathbb{F}_q}$-isomorphism classes	
Theory of complex multiplication	

Class field theory of number fields

Couveignes showed (1996) that the class field theory of number fields provided a unifying vision for:

Class field theory of number fields

Couveignes showed (1996) that the class field theory of number fields provided a unifying vision for:

- the DLP on multiplicative groups $\mathbb{F}_q^\times$,

Class field theory of number fields

Couveignes showed (1996) that the class field theory of number fields provided a unifying vision for:

- the DLP on multiplicative groups $\mathbb{F}_q^\times$,
- the DLP on elliptic curves $E(\mathbb{F}_q)$,

Class field theory of number fields

Couveignes showed (1996) that the class field theory of number fields provided a unifying vision for:

- the DLP on multiplicative groups $\mathbb{F}_q^\times$,
- the DLP on elliptic curves $E(\mathbb{F}_q)$,
- the Couveignes-Rostovtsev-Stolbunov (CRS) key-exchange scheme.

Class field theory of number fields

Couveignes showed (1996) that the class field theory of number fields provided a unifying vision for:

- the DLP on multiplicative groups $\mathbb{F}_q^\times$,
- the DLP on elliptic curves $E(\mathbb{F}_q)$,
- the Couveignes-Rostovtsev-Stolbunov (CRS) key-exchange scheme.

This unification is made with the notion of *hard homogeneous space (HHS)*.

Hard homogeneous spaces (Couveignes, 1996)

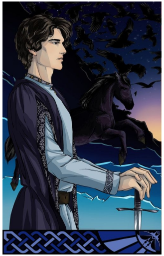
Tristan and Isolde create a private key on a public channel.

Hard homogeneous spaces (Couveignes, 1996)

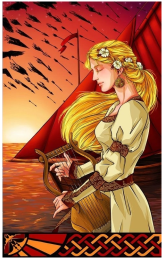
Tristan and Isolde create a private key on a public channel. They choose an abelian group G acting (freely and transitively) on a set X, with an element $x \in X$.

Hard homogeneous spaces (Couveignes, 1996)

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

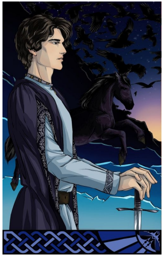


$$\xrightarrow{\quad a \cdot x \quad}$$



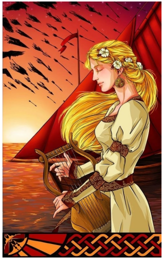
Hard homogeneous spaces (Couveignes, 1996)

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



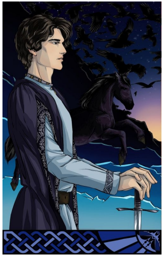
$$\xrightarrow{\quad a\cdot x \quad}$$

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



Hard homogeneous spaces (Couveignes, 1996)

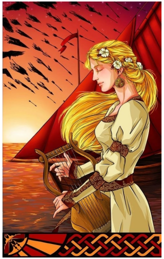
Tristan and Isolde create a private key on a public channel. They choose an abelian group G acting (freely and transitively) on a set X, with an element $x \in X$.



$a \cdot x$ ⟶

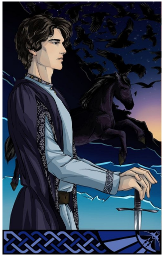
⟵ $b \cdot x$

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



Hard homogeneous spaces (Couveignes, 1996)

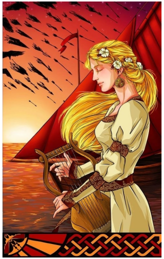
Tristan and Isolde create a private key on a public channel. They choose an abelian group G acting (freely and transitively) on a set X, with an element $x \in X$.



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

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

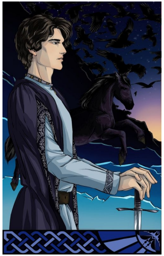
⇠ Both calculate $ab \cdot x$ (secret key) ⇢



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

Hard homogeneous spaces (Couveignes, 1996)

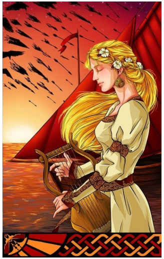
Tristan and Isolde create a private key on a public channel. They choose an abelian group G acting (freely and transitively) on a set X, with an element $x \in X$.



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

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

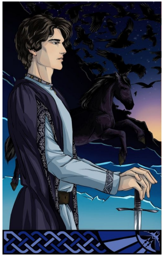
⇠ Both calculate $ab \cdot x$ (secret key) ⇢



Secure if hard to compute $ab \cdot x$ knowing $x, a \cdot x$ and $b \cdot x$.
Generalizes Diffie-Hellman on a cyclic group H: $G = \mathbb{Z}/\#H\mathbb{Z}$, $X = H$.

Hard homogeneous spaces (Couveignes, 1996)

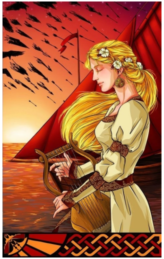
Tristan and Isolde create a private key on a public channel. They choose an abelian group G acting (freely and transitively) on a set X, with an element $x \in X$.



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

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

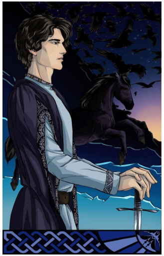
⇠ Both calculate $ab \cdot x$ (secret key) ⇢



Secure if hard to compute $ab \cdot x$ knowing $x, a \cdot x$ and $b \cdot x$.
Generalizes Diffie-Hellman on a cyclic group H: $G = \mathbb{Z}/\#H\mathbb{Z}$, $X = H$.
CRS and CSIDH are built as hard homogeneous spaces.

Hard homogeneous spaces (Couveignes, 1996)

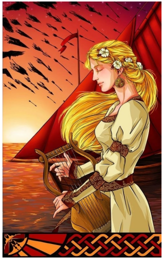
Tristan and Isolde create a private key on a public channel. They choose an abelian group G acting (freely and transitively) on a set X, with an element $x \in X$.



$a \cdot x$ →

← $b \cdot x$

← - - - - Both calculate $ab \cdot x$ (secret key) - - - - →



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

Generalizes Diffie-Hellman on a cyclic group H: $G = \mathbb{Z}/\#H\mathbb{Z}$, $X = H$.

CRS and CSIDH are built as hard homogeneous spaces.

Quantum attack in $\exp(c\sqrt{\log(\#G)})$ for some $c > 0$ (Kuperberg, 2005; Bonnetain, Schrottenloher, 2020).

Main results

In `ia.cr/2022/349`:

- Construction of the function field analogue of CRS.

Main results

In `ia.cr/2022/349`:

- Construction of the function field analogue of CRS.
- Efficient C++ implementation.

Main results

In `ia.cr/2022/349`:

- Construction of the function field analogue of CRS.
- Efficient C++ implementation.
- Reduction of the security to the isogeny finding problem.

Main results

In `ia.cr/2022/349`:

- Construction of the function field analogue of CRS.
- Efficient C++ implementation.
- Reduction of the security to the isogeny finding problem.
- Enhancements on the analysis of the recursive algorithm to find isogenies (Joux, Narayanan, 2019; Caranay, Greenberg, Scheidler, 2020).

Main results

In `ia.cr/2022/349`:

- Construction of the function field analogue of CRS.
- Efficient C++ implementation.
- Reduction of the security to the isogeny finding problem.
- Enhancements on the analysis of the recursive algorithm to find isogenies (Joux, Narayanan, 2019; Caranay, Greenberg, Scheidler, 2020).

But this new CRS is now broken (Wesolowski, three weeks ago; `ia.cr/2022/438`)!

Main results

In `ia.cr/2022/349`:

- Construction of the function field analogue of CRS.
- Efficient C++ implementation.
- Reduction of the security to the isogeny finding problem.
- Enhancements on the analysis of the recursive algorithm to find isogenies (Joux, Narayanan, 2019; Caranay, Greenberg, Scheidler, 2020).

But this new CRS is now broken (Wesolowski, three weeks ago; `ia.cr/2022/438`)!

Furthermore:

- SageMath library for finite Drinfeld modules (work in progress).

Main result

Let $L/\mathbb{F}_q$ be a finite extension with odd degree.

Main result

Let $L/\mathbb{F}_q$ be a finite extension with odd degree. Let $\mathcal{H}$ be an imaginary hyperelliptic curve on $\mathbb{F}_q$.

Main result

Let $L/\mathbb{F}_q$ be a finite extension with odd degree. Let $\mathcal{H}$ be an imaginary hyperelliptic curve on $\mathbb{F}_q$. Let $\mathbf{A}_{\mathcal{H}}$ be the ring of function of $\mathcal{H}$ regular outside ∞.

Main result

Let $L/\mathbb{F}_q$ be a finite extension with odd degree. Let $\mathcal{H}$ be an imaginary hyperelliptic curve on $\mathbb{F}_q$. Let $\mathbf{A}_{\mathcal{H}}$ be the ring of function of $\mathcal{H}$ regular outside ∞.

Theorem

There is an explicit and computable group action of $\mathrm{Pic}^0(\mathcal{H}) \simeq \mathrm{Cl}(\mathbf{A}_{\mathcal{H}})$ *to the set of* $\overline{\mathbb{F}_q}$*-isomorphism classes of rank* 1 $\mathbf{A}_{\mathcal{H}}$*-Drinfeld modules defined over* L*.*

Ore polynomials

Let $L/\mathbb{F}_q$ be a finite extension with odd degree.

Ore polynomials

Let $L/\mathbb{F}_q$ be a finite extension with odd degree.

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

Ore polynomials

Let $L/\mathbb{F}_q$ be a finite extension with odd degree.

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

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

Ore polynomials

Let $L/\mathbb{F}_q$ be a finite extension with odd degree.

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

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

Properties:

Ore polynomials

Let $L/\mathbb{F}_q$ be a finite extension with odd degree.

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

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

Properties:

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

Ore polynomials

Let $L/\mathbb{F}_q$ be a finite extension with odd degree.

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

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

Properties:

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

Ore polynomials

Let $L/\mathbb{F}_q$ be a finite extension with odd degree.

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

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

Properties:

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

One function field analogue: CRS (3/3)

Representation:

- isomorphism classes of Drinfeld modules are represented by a j-invariant,

One function field analogue: CRS (3/3)

Representation:

- isomorphism classes of Drinfeld modules are represented by a j-invariant,
- points in $\mathrm{Pic}^0(\mathcal{H})$ are represented by Mumford coordinates.

One function field analogue: CRS (3/3)

Representation:

- isomorphism classes of Drinfeld modules are represented by a j-invariant,
- points in $\mathrm{Pic}^0(\mathcal{H})$ are represented by Mumford coordinates.

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

Output: A j-invariant.

```
// ω is a global constant
```

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

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

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

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

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

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

How secure is it? Not that much...

The security of the protocol reduces to the problem of finding an isogeny between two isogenous Drinfeld modules.

How secure is it? Not that much…

The security of the protocol reduces to the problem of finding an isogeny between two isogenous Drinfeld modules.

Previous work (Joux, Narayanan, 2019; Caranay, Greenberg, Scheidler, 2020) solve a recursive equation by exploring a research tree with exponential size (in the degree of the desired isogeny). We studied this algorithm and heuristically concluded that it ran in exponential time.

How secure is it? Not that much...

The security of the protocol reduces to the problem of finding an isogeny between two isogenous Drinfeld modules.

Previous work (Joux, Narayanan, 2019; Caranay, Greenberg, Scheidler, 2020) solve a recursive equation by exploring a research tree with exponential size (in the degree of the desired isogeny). We studied this algorithm and heuristically concluded that it ran in exponential time.

But two weeks ago... Wesolowski, solved this problem in polynomial time, reducing the isogeny-search problem to a linear algebra problem.

Recap of the situation

Number fields		Function fields	
Problem	Security	Problem	Security

Recap of the situation

Number fields		Function fields	
Problem	**Security**	**Problem**	**Security**
DLP on $\mathbb{F}_q^\times$	Broken in small characteristic		
DLP on $E(\mathbb{F}_q)$	Secure		
CRS	Secure		

Recap of the situation

Number fields		Function fields	
Problem	**Security**	**Problem**	**Security**
DLP on $\mathbb{F}_q^\times$	Broken in small characteristic	*Same problem!*	
DLP on $E(\mathbb{F}_q)$	Secure		
CRS	Secure		

Recap of the situation

Number fields		Function fields	
Problem	**Security**	**Problem**	**Security**
DLP on $\mathbb{F}_q^\times$	Broken in small characteristic	*Same problem!*	
DLP on $E(\mathbb{F}_q)$	Secure	Analogue with Drinfeld modules	Broken (Scanlon, 1999)
CRS	Secure		

Recap of the situation

Number fields		Function fields	
Problem	**Security**	**Problem**	**Security**
DLP on $\mathbb{F}_q^\times$	Broken in small characteristic	*Same problem!*	
DLP on $E(\mathbb{F}_q)$	Secure	Analogue with Drinfeld modules	Broken (Scanlon, 1999)
CRS	Secure	Analogue with Drinfeld modules	Broken (Wesolowski, 2022)

Conclusion

Function fields / Drinfeld modules analogues of elliptic curve isogeny-based cryptosystems presented here seem very well broken. . .

Conclusion

Function fields / Drinfeld modules analogues of elliptic curve isogeny-based cryptosystems presented here seem very well broken...

It also seems to be the case for CSIDH and SIDH (Joux, Narayanan, 2019).

Conclusion

Function fields / Drinfeld modules analogues of elliptic curve isogeny-based cryptosystems presented here seem very well broken...

It also seems to be the case for CSIDH and SIDH (Joux, Narayanan, 2019).

However, many algorithmic aspects of Drinfeld modules are yet to be explored for cryptographic purposes: higher ranks, abelian varieties...

Conclusion

Function fields / Drinfeld modules analogues of elliptic curve isogeny-based cryptosystems presented here seem very well broken...

It also seems to be the case for CSIDH and SIDH (Joux, Narayanan, 2019).

However, many algorithmic aspects of Drinfeld modules are yet to be explored for cryptographic purposes: higher ranks, abelian varieties...

Thank you!