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

Antoine Leudière and Pierre-Jean Spaenlehauer

Université de Lorraine, Inria, CNRS

Edit (April 7th 2022)**.** A few weeks after we made our work public, Benjamin Wesolowski found an efficient algorithm for computing isogenies of finite Drinfeld modules; see `https://eprint.iacr.org/2022/438`. This makes obsolete the cryptographic applications (non-interactive post-quantum key exchange) described below.

Abstract

We explore algorithmic aspects of a free and transitive commutative group action coming from the class field theory of imaginary hyperelliptic function fields. Namely, the Jacobian of an imaginary hyperelliptic curve defined over $\mathbb{F}_q$ acts on a subset of isomorphism classes of Drinfeld modules. We describe an algorithm to compute the group action efficiently. This is a function field analog of the Couveignes-Rostovtsev-Stolbunov group action. Our proof-of-concept C++/NTL implementation only requires a fraction of a second on a standard computer. Also, we state a conjecture — supported by experiments — which implies that the current fastest algorithm to solve its inverse problem runs in exponential time. This action is therefore a promising candidate for the construction of *Hard Homogeneous Spaces*, which are the building blocks of several post-quantum cryptographic protocols. This demonstrates the relevance of using imaginary hyperelliptic curves and Drinfeld modules as an alternative to the standard setting of imaginary quadratic number fields and elliptic curves for isogeny-based cryptographic applications. Moreover, our function field setting enables the use of Kedlaya's algorithm and its variants for computing the order of the group in polynomial time when q is fixed. No such polynomial-time algorithm for imaginary quadratic number fields is known. For $q = 2$ and parameters similar to CSIDH-512, we compute this order more than 8500 times faster than the record computation for CSIDH-512 by Beullens, Kleinjung and Vercauteren.

Introduction

Context and motivation. A *principal homogeneous space* for a finite commutative group G is a set S on which G acts simply transitively. A *Hard Homogeneous Space* (HHS), as introduced by Couveignes in [Cou06], is a principal homogeneous space such that calculating the action is computationally easy, and the problem of finding $g \in G$ such that $g \cdot x = y$ given $x, y \in S$ is computationally hard. HHS emerge naturally in the context of cryptography, as we can build a non-interactive Diffie-Hellman-like key exchange protocol from any HHS [Cou06][RS06]. One of the features of this construction is that the fastest known generic quantum attack relies on Kuperberg's algorithm and it has subexponential complexity [Kup05]. Therefore, HHS are promising candidates for being a strong mathematical basis for post-quantum cryptosystems.

Couveignes [Cou06] and Rostovtsev-Stolbunov [RS06] independently proposed a HHS via the action of the class group of an imaginary quadratic number field on isomorphism classes of

ordinary elliptic curves defined over a finite field. This construction takes its roots in number theory; it is an emanation of the class field theory of imaginary quadratic number fields, where the class group is in fact the Galois group of a class field of an imaginary quadratic number field. For cryptographic parameters, this group action unfortunately appeared to be not efficient enough to compete with other post-quantum cryptosystems [DFKS18]. In an attempt to avoid those shortcomings, this idea was adapted in [CLM$^+$18] to the case of supersingular elliptic curves. This lead to a new HHS, and a new key-exchange protocol named CSIDH [CLM$^+$18]. Supersingular elliptic curves provide substantial computational speed-ups, making them eligible for practical use.

A major drawback of current isogeny-based cryptosystems based on HHS is that computing the order and the structure of the class group of an imaginary quadratic number field is hard: the best known algorithms run in subexponential time. Being able to compute the structure of the class group is a desirable feature for cryptographic applications. For instance, we would like to be sure that G contains a large prime cyclic subgroup. Also, the knowledge of this order is needed to build efficient post-quantum signatures protocols [BKV19]. The authors of [BKV19] managed to compute the group structure of CSIDH-512, in a 52 core-years record computation. The implementation was heavily optimized, which raises the question of whether similar group orders could be computed in practice for larger parameters.

Main results. We propose a function field analog of the Couveignes-Rostovtsev-Stolbunov (CRS) construction. In this setting, imaginary quadratic function fields and Drinfeld modules play respectively the roles of imaginary quadratic number fields and elliptic curves. Although Drinfeld modules might seem more abstract than elliptic curves, they appear to be very convenient for concrete computations. Drinfeld modules have a theory of complex multiplication, which shares many similarities with that of elliptic curves: rank-2 Drinfeld modules defined over a finite extension L of $\mathbb{F}_q$ have a Frobenius endomorphism whose characteristic polynomial has degree 2 in $\mathbb{F}_q[X][Y]$ and therefore defines a quadratic extension $\mathbf{k}$ of $\mathbb{F}_q(X)$. If $[L : \mathbb{F}_q]$ is odd, then this polynomial defines an imaginary quadratic function field $\mathbf{k}$, and its class field theory provides us with a free and transitive group action — whose underlying group is the Galois group G of an abelian extension which is unramified at all finite places and for which the place at infinity splits completely [Hay91, Thm. 15.6] — on the set S of isomorphism classes of Drinfeld modules having complex multiplication by $\mathbf{k}$. For simplicity, we restrict our work to the case of imaginary hyperelliptic function fields; in this case, G is the degree-0 Picard group $\mathrm{Pic}^0(\mathcal{H})$ of the underlying hyperelliptic curve $\mathcal{H}$.

Our main objective is to make this group action effective, and to study the difficulty of the *inverse problem*, i.e. computing an element $g \in G$ such that $g \cdot x = y$, where $x, y \in S$ are given. We provide an algorithm to compute this group action. Surprisingly, it is quite easy both to describe and to implement: it relies mainly on computing the right-GCD of two Ore polynomials. We also implemented and tested the best known methods for solving the inverse problem [CGS20, Sec. 8][JN19, Sec. 5.2], as the security of cryptographic applications relies on its difficulty. It appears that they run experimentally in exponential time since they require to browse a full tree of arity q and whose depth corresponds to the size of the representation of the isogeny. Based on our experimental observations, we formulate a conjecture which states that no branch can be pruned during this tree search. Therefore, we argue that this group action is a good candidate for being an HHS.

We finish our investigation by measuring the practical efficiency of a C++/NTL prototype implementation of our function field HHS for typical cryptographic parameters[1]. To this end, we set $q = 2$ and we consider Drinfeld modules defined over $\mathbb{F}_{2^{521}}$, which provide a security

[1]Our code is freely available at `https://gitlab.inria.fr/pspaenle/crs-drinfeld-521`.

similar to that of CSIDH-512 (i.e. a group of order $\approx 2^{256}$). On an 8-core standard laptop, our prototype implementation requires approximately 216 ms to perform a full group action, which means that a full key-exchange can be done in approximately 432 ms with our non-optimized software. Although this is slower than CSIDH by a considerable factor, we believe that it is still fast enough to be considered as a potential cryptographic alternative to existing cryptosystems. There is still a lot of work to do on cryptographic aspects: code optimization, countermeasures against side-channel attacks, fine-tuning of the parameters, etc. These aspects are outside the scope of this paper and we leave this for future work.

Finally, we mention a major advantage of our function field variant over CSIDH: Kedlaya's algorithm [Ked01] (or Denef-Vercauteren's variant in characteristic 2 [DV06]) can compute the group order in polynomial time. In fact, for our cryptographic instantiation ($q = 2$, $L = \mathbb{F}_{2^{521}}$), we were able to compute the order of the group in about 53 hours on a single core. This is more than 8500 faster than the 52 core-years which were required to compute the order of the group in CSIDH-512 [BKV19].

Organization of the paper. Section 1 recalls the algebraic construction of Drinfeld modules and the basic tools that we need throughout this paper. Section 2 focuses on complex multiplication and on the class field theory of imaginary hyperelliptic function fields. The main result of this section is a reduction of the group action from class field theory to finite Drinfeld modules. This yields a way to algorithmically handle this group action with finite objects. Section 3 describes the main algorithms that we propose to compute this action. We also give a method to recover the ideal class corresponding to a given isogeny of ordinary Drinfeld modules. Finally, Section 4 investigates applications of this group action to post-quantum cryptography, and we discuss practical parameters and timings.

Acknowledgements. We are grateful to Emmanuel Thomé and Pierrick Gaudry for fruitful discussions. This work is partly funded by the project PEPR PQ-TLS.

1 Drinfeld modules

Classical textbooks on Drinfeld modules are [Gos98] and [Ros02]. Finite Drinfeld modules are studied in depth in [Gek91]. For algorithmic perspectives, see [MS19], [Car18] and [CGS20].

Throughout this paper, $\mathbb{F}_q$ is the finite field with q elements.

1.1 Ore polynomials

The core mathematical object for the algebraic construction of Drinfeld modules is the ring of univariate Ore polynomials. Let $\mathbb{F}_q \hookrightarrow K$ be a field extension. We let $\tau : x \mapsto x^q$ denote the Frobenius endomorphism of $\overline{K}$, which is $\mathbb{F}_q$-linear.

Definition 1.1 ([Gos98, Def. 1.1.3])**.** *The* ring of Ore polynomials $K\{\tau\}$ *is the subring of* $\mathbb{F}_q$*-linear endomorphisms of* $\overline{K}$ *of the form*

$$\sum_{0 \leqslant i \leqslant n} a_i \tau^i, \quad n \in \mathbb{Z}_{\geqslant 0}, a_i \in K,$$

equipped with the addition and the composition of $\mathbb{F}_q$*-linear endomorphisms.*

In Definition 1.1, and if $a_n \neq 0$, the integer n is called the τ-degree of P, and we say that P is *monic* if $a_n = 1$. In $K\{\tau\}$, we write $1 = \tau^0$ for the identity endomorphism. For $i, j \in \mathbb{Z}_{\geqslant 0}$,

$\tau^i\tau^j = \tau^{i+j}$. For every $a \in K$, the equality $\tau a = a^q\tau$ holds true. Therefore, the ring $K\{\tau\}$ is not commutative as soon as $\mathbb{F}_q \neq K$. The center of $K\{\tau\}$ is $\mathbb{F}_q\left[\tau^{[K:\mathbb{F}_q]}\right]$ if K is finite, otherwise it is $\mathbb{F}_q$. The ring $K\{\tau\}$ is left-Euclidean [Gos98, Prop. 1.6.2] for the τ-degree, i.e. for every $P_1, P_2 \in K\{\tau\}$, there exist $Q, R \in K\{\tau\}$ satisfying

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

We therefore define the *right-greatest common divisor*, abbreviated rgcd, of any non-empty subset $S \subset K\{\tau\}$ as the unique monic generator of the left-ideal generated by S in $K\{\tau\}$.

We say that P is *separable* if the coefficient of τ^0 is nonzero, i.e. τ does not right-divide P; we say that P is *inseparable* if it is not separable; we say that P is *purely inseparable* if $P = \alpha\tau^i$ for some $\alpha \in K^\times, i \in \mathbb{Z}_{>0}$. Consequently, for any $P \in K\{\tau\}$ there exists $\ell \in \mathbb{Z}_{\geqslant 0}$ and some separable $s \in K\{\tau\}$ such that $P = \tau^\ell s$. The integer ℓ is called the *height* of P and denoted $\mathrm{h}(P)$. Using left-Euclidean division, it can be proved that for any $P_1, P_2 \in K\{\tau\}$ such that P_1 is separable, $\mathrm{Ker}(P_2) \subset \mathrm{Ker}(P_1)$ if and only if P_2 right-divides P_1.

1.2 General Drinfeld modules

Let $\mathbf{k}$ be an algebraic function field of transcendence degree 1 over $\mathbb{F}_q$ (i.e. a finite field extension of $\mathbb{F}_q(X)$), ∞ be a place of $\mathbf{k}$, and $\mathbf{A} \subset \mathbf{k}$ be the ring of functions that are regular outside ∞. Let $K/\mathbb{F}_q$ be a field extension equipped with a $\mathbb{F}_q$-algebra morphism $\gamma : \mathbf{A} \to K$. The kernel of γ is a prime ideal called the $\mathbf{A}$-*characteristic of* K. There are mainly two cases which are of interest for Drinfeld modules:

(i) The field K is a finite extension of $\mathbf{A}/\mathfrak{p}$ for some nonzero prime ideal $\mathfrak{p} \subset \mathbf{A}$, γ is the composition $\mathbf{A} \twoheadrightarrow \mathbf{A}/\mathfrak{p} \hookrightarrow K$, the $\mathbf{A}$-characteristic of K is $\mathfrak{p}$; in this case, we will write L instead of K (see Section 1.3).
(ii) The field K is a finite extension of $\mathbf{k}$ and the morphism γ is injective.

By [Lor96, Ch. 7, Cor. 2.7], quotients of $\mathbf{A}$ by nonzero ideals $\mathfrak{a}$ are finite-dimensional $\mathbb{F}_q$-vector spaces. The *degree of* $\mathfrak{a}$ is $\deg(\mathfrak{a}) := \log_q(\#(\mathbf{A}/\mathfrak{a}))$. For a nonzero $a \in \mathbf{A}$, we set $\deg(a) := \deg(a\mathbf{A})$.

Definition 1.2 ([Gos98, Def. 4.4.2], [Gek91, Def. 1.1])**.** *A* Drinfeld $\mathbf{A}$-module over K *is an* $\mathbb{F}_q$*-algebra morphism* $\phi : \mathbf{A} \to K\{\tau\}$ *such that,*

— *for all* $a \in \mathbf{A}$*, the coefficient of* τ^0 *in* $\phi(a)$ *is* $\gamma(a)$*;*
— *there exists* $a \in \mathbf{A}$ *such that* $\deg_\tau(\phi(a)) > 0$.

Let ϕ be a Drinfeld $\mathbf{A}$-module over K. For any $a \in \mathbf{A}$, the image $\phi(a)$ is denoted ϕ_a. An important feature of Drinfeld modules is that there exists an integer $r \in \mathbb{Z}_{>0}$ called *the rank of* ϕ such that $\deg_\tau(\phi_a) = r\deg(a)$ for any $a \in \mathbf{A}$ [Gos98, Def. 4.5.4]. We let $\mathrm{Dr}_r(\mathbf{A}, K)$ denote the set of Drinfeld $\mathbf{A}$-modules over K with rank r. A special case of interest is when $\mathbf{A} = \mathbb{F}_q[X]$, in which ϕ is uniquely determined by ϕ_X and its rank is $\deg_\tau(\phi_X)$.

A Drinfeld $\mathbf{A}$-module ϕ induces a $\mathbf{A}$-module law on $\overline{K}$, defined by $a \cdot_\phi x = \phi_a(x)$, where $a \in \mathbf{A}, x \in \overline{K}$. When $\mathbf{A} = \mathbb{F}_q[X]$, this structure of $\mathbb{F}_q[X]$-module on $\overline{K}$ can be viewed as an analog of the $\mathbb{Z}$-module law on the group of points $\mathcal{E}(\overline{K})$ of an elliptic curve defined over K.

Let ψ be another Drinfeld $\mathbf{A}$-module over K. A *morphism of Drinfeld modules* $\iota : \phi \to \psi$ is an Ore polynomial $\iota \in K\{\tau\}$ such that $\iota\phi_a = \psi_a\iota$ for all $a \in \mathbf{A}$. An *isogeny* is a nonzero morphism. If K'/K is a field extension, a K'*-morphism* $\phi \to \psi$ is a morphism that lives in $K'\{\tau\}$. The endomorphisms of ϕ form a ring denoted $\mathrm{End}(\phi)$ which always contains $\mathbb{F}_q$ and elements of the form ϕ_a, $a \in \mathbf{A}$. Said otherwise, $\mathbf{A}$ is isomorphic to a subring of $\mathrm{End}(\phi)$. When $\mathbf{A} = \mathbb{F}_q[X]$, endomorphisms ϕ_a are analogs of integer multiplication on elliptic curves.

1.3 Finite Drinfeld modules

In this section, we specialize in Drinfeld $\mathbf{A}$-modules over a finite field L, which are also called *finite Drinfeld modules*. In that case, we fix $\mathfrak{p} \subset \mathbf{A}$ a prime ideal and L a finite extension of $\mathbf{A}/\mathfrak{p}$, equipped with the canonical morphism $\gamma : \mathbf{A} \twoheadrightarrow \mathbf{A}/\mathfrak{p} \hookrightarrow L$. Finite Drinfeld modules have a special endomorphism $\tau_L \coloneqq \tau^{[L:\mathbb{F}_q]}$, called the *Frobenius endomorphism*. It is worth noticing that for any Drinfeld $\mathbf{A}$-module ϕ over L, $\mathrm{End}(\phi)$ contains $\mathbb{F}_q[\tau_L]$. Any isogeny $\iota : \phi \to \psi$ can be written $\tau^{\ell \deg(\mathfrak{p})} s$ for some $\ell \in \mathbb{Z}_{\geqslant 0}$ and a separable $s \in L\{\tau\}$ [Gek91, §(1.4), Eq. (ii)]. Furthermore, the endomorphism ϕ_a is separable if and only if a is not contained in $\mathrm{Ker}(\gamma) = \mathfrak{p}$.

We define now the norm of an isogeny $\iota : \phi \to \psi$ of finite Drinfeld modules, which is linked to the Euler-Poincaré characteristic of its kernel. By [Lan02, Th. III.8.1], there exists a map χ, called the *Euler-Poincaré characteristic*, which sends finite $\mathbf{A}$-modules to ideals in $\mathbf{A}$ and which satisfy the following properties for any finite $\mathbf{A}$-modules M_1, M_2, M_3:

(i) $\chi(0) = \mathbf{A}$ and $\chi(\mathbf{A}/\mathfrak{q}) = \mathfrak{q}$ if $\mathfrak{q}$ is prime,
(ii) $\chi(M_1) = \chi(M_2)$ if $M_1 \simeq M_2$,
(iii) $\chi(M_1) = \chi(M_2)\chi(M_3)$ if $0 \to M_2 \to M_1 \to M_3 \to 0$ is a short exact sequence.

The *norm of* ι is defined in [Gek91, §(3.9)] as $\mathfrak{n}(\iota) \coloneqq \mathfrak{p}^{\mathrm{h}(\iota)/\deg(\mathfrak{p})}\chi(\mathrm{Ker}(\iota))$. See [Gek91, Lem. 3.10] for its properties. The following lemma is technical, but it is also quite useful and it will play a role in several proofs throughout this paper.

Lemma 1.3. *If ϕ and ψ are isogenous, then there exists a separable isogeny between them. Furthermore,* $\mathrm{rgcd}\,(\mathrm{Hom}(\psi, \phi)) = 1$.

Proof. Let $f : \phi \to \psi$ be an isogeny, set $V = \bigcap_{u \in \mathrm{Hom}(\psi,\phi)} \mathrm{Ker}(u)$, and let g be an isogeny in $\mathrm{Hom}(\psi, \phi)$. The sequence of A-modules $0 \to V \to \mathrm{Ker}(g) \to \mathrm{Ker}(g)/V \to 0$ is exact, so that $\chi(V)$ divides $\chi(\mathrm{Ker}(g))$. Consequently, $\chi(V)\mathfrak{p}^{\mathrm{h}(g)/\deg(\mathfrak{p})}\mathfrak{n}(f)$ divides $\mathfrak{n}(fg)$. In particular, $\chi(V)\mathfrak{n}(f) \mid \mathfrak{n}(fg)$. By [Gek91, Lem. 3.10.(iv)], we have $\sum_{g \in \mathrm{Hom}(\psi,\phi)} \mathfrak{n}(fg) = \mathfrak{n}(f)$. Since $\mathfrak{n}(f) \neq (0)$, $\chi(V)$ must equal $\mathbf{A}$ and hence $V = 0$.

We now prove that there exists a separable isogeny $g \in \mathrm{Hom}(\psi, \phi)$. Let $h = \min \mathrm{h}(g)$ be the minimal height over all isogenies $g : \psi \to \phi$. Then $\mathfrak{p}^{h/\deg(\mathfrak{p})}\mathfrak{n}(f) \mid \mathfrak{n}(fg)$ for all isogenies g. By the same argument as above, we conclude that $\mathfrak{p}^h = \mathbf{A}$, thus $h = 0$.

Finally, notice that $\mathrm{Ker}(\mathrm{rgcd}(\mathrm{Hom}(\psi, \phi))) = V = 0$. Therefore, $\mathrm{rgcd}(\mathrm{Hom}(\psi, \phi))$ divides $\tau^{\deg(\mathfrak{p})\ell}$ for some $\ell \in \mathbb{Z}_{\geqslant 0}$. Since we proved that there exists a separable isogeny $\phi \to \psi$, $\ell = 0$ and $\mathrm{rgcd}\,(\mathrm{Hom}(\psi, \phi)) = 1$. □

As for elliptic curves, "being isogenous" is an equivalence relation. For $a \in \mathbf{A}$, we say that $\iota : \phi \to \psi$ is *an a-isogeny* if ι right-divides ϕ_a in $L\{\tau\}$. Every isogeny is an a-isogeny for some nonzero $a \in \mathbf{A}$. If ι is separable, then there exists another separable isogeny $\hat{\iota} : \psi \to \phi$, called the dual a-isogeny, such that $\hat{\iota} \cdot \iota = \phi_a$ and $\iota \cdot \hat{\iota} = \psi_a$. See e.g. [DH87, §(4.1)].

Drinfeld modules have an analog for Vélu's formula. Let $\iota \in L\{\tau\}$ be nonzero. There exists a finite Drinfeld $\mathbf{A}$-module ψ defined over L such that ι is an isogeny $\phi \to \psi$ if and only if $\mathrm{Ker}\,\iota$ is an $\mathbf{A}$-submodule of $\overline{L}$ (endowed with the $\mathbf{A}$-module structure $(a, x) \mapsto \phi_a(x)$ for $a \in \mathbf{A}, x \in \overline{L}$) and $\deg(\mathfrak{p})$ divides $\mathrm{h}(\iota)$ [Gek91, §(1.4)]. We emphasize that for any $a \in \mathbf{A}$, the Ore polynomial ψ_a in can be explicitly computed. The τ-degrees of ϕ_a and ψ_a are equal. By equating the coefficients of $\iota \cdot \phi_a$ and $\psi_a \cdot \iota$, we obtain simple formulas for computing iteratively the coefficients of ψ_a. For instance, if ι is separable, by writing

$$\begin{cases} \iota = \sum_{0 \leqslant i \leqslant \deg_\tau(\iota)} \iota_i \tau^i, \\ \phi_a = \sum_{0 \leqslant i \leqslant \deg_\tau(\phi_a)} \lambda_i \tau^i, \\ \psi_a = \sum_{0 \leqslant i \leqslant \deg_\tau(\phi_a)} \mu_i \tau^i, \end{cases}$$

we obtain the following formulas for $i \in [\![0, \deg_\tau(\phi_a)]\!]$:

$$\mu_i = \frac{1}{\iota_0^{q^i}} \left(\sum_{0 \leqslant j \leqslant i} \iota_j \lambda_{i-j}^{q^j} - \sum_{0 \leqslant j \leqslant i-1} \mu_j \iota_{i-j}^{q^j} \right). \tag{1.1}$$

2 Class field theory of imaginary hyperelliptic function fields

2.1 Complex multiplication for rank-two finite Drinfeld modules

Rank-two Drinfeld modules over finite fields enjoy a theory of complex multiplication which shares many similarities with elliptic curves defined over finite fields. The main difference is that imaginary quadratic number fields are replaced by imaginary quadratic function fields, namely quadratic extensions of $\mathbb{F}_q(X)$ for which the place at infinity

$$\{f/g \mid f, g \in \mathbb{F}_q[X],\ \deg(g) \geqslant \deg(f)\} \subset \mathbb{F}_q(X)$$

does not split.

We start by fixing a nonzero prime ideal $\mathfrak{p} \subset \mathbb{F}_q[X]$ and by considering Drinfeld modules in $\mathrm{Dr}_2(\mathbb{F}_q[X], L)$, where L is a finite extension of $\mathbb{F}_q[X]/\mathfrak{p}$ endowed with the canonical map $\gamma : \mathbb{F}_q[X] \twoheadrightarrow \mathbb{F}_q[X]/\mathfrak{p} \hookrightarrow L$. A Drinfeld module $\phi \in \mathrm{Dr}_2(\mathbb{F}_q[X], L)$ is completely described by the image ϕ_X of X, which is an Ore polynomial of the form

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

The Frobenius endomorphism $\tau_L \in \mathrm{End}(\phi)$ satisfies a quadratic equation [Gek91, Cor. 3.4] [MS19, Th. 1]; for any $\phi \in \mathrm{Dr}_2(\mathbb{F}_q[X], L)$, there is a unique monic polynomial ξ in $\mathbb{F}_q[X][Y]$ of the form

$$\xi = Y^2 + h(X)Y - f(X) \in \mathbb{F}_q[X][Y],$$

such that

$$\begin{cases} \xi(\phi_X, \tau_L) = 0, \\ \deg(f) = [L : \mathbb{F}_q], \\ \deg(h) \leqslant [L : \mathbb{F}_q]/2. \end{cases} \tag{2.1}$$

The polynomial ξ is called the *characteristic polynomial of the Frobenius endomorphism.*

Definition 2.1 ([Gek83, Lemma (5.2) and Satz (5.3)])**.** *Let $\phi \in \mathrm{Dr}_2(\mathbb{F}_q[X], L)$, and let $\xi = Y^2 + h(X)Y - f(X)$ be the characteristic polynomial of its Frobenius endomorphism. Then ϕ is called* supersingular *if $h \in \mathfrak{p}$, otherwise it is called* ordinary*.*

If $[L : \mathbb{F}_q]$ is odd and the curve defined by ξ does not have any singularity in the affine plane, then the degree bounds in (2.1) imply that ξ defines a hyperelliptic curve over $\mathbb{F}_q$ [CFA+05, Def. 14.1]. In this case, we have a complete description of the endomorphism ring:

Proposition 2.2. *Assume $[L : \mathbb{F}_q]$ is odd, let $\phi \in \mathrm{Dr}_2(\mathbb{F}_q[X], L)$ be an ordinary rank-2 Drinfeld module, and assume that ξ defines an imaginary hyperelliptic curve $\mathcal{H}$. Then $\mathrm{End}_{\overline{L}}(\phi) = \mathrm{End}_L(\phi)$. Writing $\mathbf{A}_\mathcal{H} = \mathbb{F}_q[X][Y]/(\xi)$, the $\mathbb{F}_q$-algebras $\mathrm{End}_L(\phi)$ and $\mathbf{A}_\mathcal{H}$ are isomorphic via*

$$\begin{array}{rcl} \mathbf{A}_\mathcal{H} & \to & \mathrm{End}_L(\phi) \\ \overline{X} & \mapsto & \phi_X \\ \overline{Y} & \mapsto & \tau_L. \end{array}$$

Furthermore, $\mathbf{A}_\mathcal{H}$ is isomorphic to the ring of functions of $\mathcal{H}$ that are regular outside its place ∞ at infinity.

Proof. By [Gek91, Lem. 3.3], the minimal polynomial of τ_L over $\mathbb{F}_q[X]$ is ξ, which implies that the kernel of the map

$$\begin{array}{rcl} \mathbb{F}_q[X][Y] & \to & \mathrm{End}_L(\phi) \\ X & \mapsto & \phi_X \\ Y & \mapsto & \tau_L \end{array}$$

is the ideal generated by ξ and hence $\mathbb{F}_q[\phi_X, \tau_L]$ is isomorphic to $\mathbf{A}_{\mathcal{H}}$.

By [Lor96, Chap. 5, Th. 10.8], $\mathbf{A}_{\mathcal{H}}$ is the integral closure of $\mathbb{F}_q[X]$ in the function field $\mathbb{F}_q(\mathcal{H})$. Let $\mathcal{O}$ be an $\mathbb{F}_q[X]$-order in $\mathbb{F}_q(\mathcal{H})$. Since the canonical field extension $\mathbb{F}_q(X) \hookrightarrow \mathbb{F}_q(\mathcal{H}) = \mathrm{Frac}(\mathbf{A}_{\mathcal{H}})$ has degree 2, $\mathcal{O}$ must be a rank-2 $\mathbb{F}_q[X]$-module. Let $1, \alpha \in \mathbb{F}_q(\mathcal{H})$ be an $\mathbb{F}_q[X]$-basis of $\mathcal{O}$. Then $\alpha^2 = a + b\alpha$ for some $a, b \in \mathbb{F}_q[X]$, which implies that α belongs to the $\mathbb{F}_q[X]$-integral closure of $\mathbb{F}_q[X]$ in $\mathbb{F}_q(\mathcal{H})$, which is $\mathbf{A}_{\mathcal{H}}$. This implies that $\mathcal{O} \subset \mathbf{A}_{\mathcal{H}}$. Hence, $\mathbf{A}_{\mathcal{H}}$ is maximal.

Since τ_L is not in the image of the map $g \mapsto \phi_g$, $\mathbb{F}_q[\phi_X, \tau_L] \subset \mathrm{End}_L(\phi)$ is a 2-dimensional $\mathbb{F}_q[X]$-module in $\mathrm{End}_L(\phi) \otimes \mathbb{F}_q(X)$. By [Car18, Th. 6.4.2.(iii)], $\mathrm{End}_L(\phi) \otimes \mathbb{F}_q(X)$ is an imaginary quadratic function field and $\mathrm{End}_L(\phi)$ is an $\mathbb{F}_q[X]$-order in it. Therefore, $\mathbb{F}_q[\phi_X, \tau_L]$ is an $\mathbb{F}_q[X]$-order in $\mathrm{End}_L(\phi) \otimes \mathbb{F}_q(X) \simeq (\mathbb{F}_q[X][Y]/\xi) \otimes \mathbb{F}_q(X) \simeq \mathbb{F}_q(\mathcal{H})$. Finally, notice that $\mathrm{End}_L(\phi)$ contains the maximal order $\mathbb{F}_q[\phi_X, \tau_L]$, so it must be equal to it.

It remains to prove that $\mathrm{End}_{\overline{L}}(\phi) = \mathrm{End}_L(\phi)$. For any finite extension L' of L, by [Car18, Th. 6.4.2.(iii)], $\mathrm{End}_L(\phi)$ is a sub-order of $\mathrm{End}_{L'}(\phi)$. As $\mathrm{End}_L(\phi)$ is maximal, $\mathrm{End}_L(\phi) = \mathrm{End}_{L'}(\phi)$. □

The j-*invariant of* ϕ, denoted $\mathrm{j}(\phi)$, is the quantity g^{q+1}/Δ [Car18, Def. 5.4.1]. For every $j \in L$, there exists a Drinfeld module $\phi \in \mathrm{Dr}_2(\mathbb{F}_q[X], L)$ whose j-invariant is j; it is defined by $j^{-1}\tau^2 + \tau + \gamma(X)$ if $j \neq 0$, and $\tau^2 + \gamma(X)$ otherwise. The j-invariant and the characteristic polynomial serve as classifying criterion [Car18, Rem. 5.4.2], [Gek91, Th. 3.5]; two Drinfeld modules $\phi, \psi \in \mathrm{Dr}_2(\mathbb{F}_q[X], L)$ are:

(i) $\overline{L}$-isomorphic if and only if they have the same j-invariant,
(ii) L-isogenous if and only if they have the same characteristic polynomial.

Proposition 2.3. *If two ordinary Drinfeld modules in* $\mathrm{Dr}_2(\mathbb{F}_q[X], L)$ *are* L*-isogenous and* $\overline{L}$*-isomorphic, then they are* L*-isomorphic.*

Proof. Let $\phi, \psi \in \mathrm{Dr}_2(\mathbb{F}_q[X], L)$ be two ordinary Drinfeld modules which are L-isogenous and $\overline{L}$-isomorphic. Let $\lambda : \phi \to \psi$ be an $\overline{L}$-isomorphism and $\iota : \phi \to \psi$ be a separable L-isogeny (see Lemma 1.3), then $\lambda^{-1}\iota \in \mathrm{End}_{\overline{L}}(\phi)$. By Proposition 2.2, $\mathrm{End}_{\overline{L}}(\phi) = \mathrm{End}_L(\phi)$, so $\lambda^{-1}\iota \in L\{\tau\}$, and therefore $\lambda \in L$. □

2.2 Rank-one Drinfeld modules on imaginary hyperelliptic curves

Let $d \geqslant 5$ be an odd integer and let m be a positive divisor of d. Let $p \in \mathbb{F}_q[X]$ be a monic irreducible polynomial of degree d/m and let $f = \alpha p(X)^m \in \mathbb{F}_q[X]$ for some $\alpha \in \mathbb{F}_q^\times$. Finally, let $h \in \mathbb{F}_q[X]$ be a nonzero polynomial of degree at most $(d-1)/2$ which is not divisible by p. This assumption on h is especially important as it ensures that we will encounter only ordinary Drinfeld modules, see Definition 2.1. Fix $\xi = Y^2 + h(X)Y - f(X)$ and assume that ξ defines an imaginary hyperelliptic curve $\mathcal{H}$, i.e. the curve is smooth in the affine plane [CFA+05, Def. 14.1]. As in Proposition 2.2, set $\mathbf{A}_{\mathcal{H}} = \mathbb{F}_q[X][Y]/(\xi)$, which is isomorphic to the ring of functions of $\mathcal{H}$ regular outside the place at infinity. Let $\mathfrak{p}$ be the prime ideal $\langle p(X), Y \rangle$, which has degree d. Let L be a degree-m extension of $\mathbb{F}_q[X][Y]/\mathfrak{p}$; notice that $[L : \mathbb{F}_q] = d$ is odd; this will have several technical consequences. Set $\gamma : \mathbf{A}_{\mathcal{H}} \twoheadrightarrow \mathbf{A}_{\mathcal{H}}/\mathfrak{p} \simeq \mathbb{F}_q[X]/(p) \hookrightarrow L$.

The aim of this section is to prove the following correspondence:

Proposition 2.4. *There is a bijection between the set of $\overline{L}$-isomorphism classes in $\mathrm{Dr}_2(\mathbb{F}_q[X], L)$ containing a representative whose characteristic polynomial of the Frobenius endomorphism is ξ, and the set of $\overline{L}$-isomorphism classes in $\mathrm{Dr}_1(\mathbf{A}_\mathcal{H}, L)$.*

This bijection sends the class of a Drinfeld module $\phi \in \mathrm{Dr}_2(\mathbb{F}_q[X], L)$ whose characteristic polynomial of the Frobenius is ξ to the class of $\psi \in \mathrm{Dr}_1(\mathbf{A}_\mathcal{H}, L)$ where $\psi_{\overline{X}} = \phi_X$ and $\psi_{\overline{Y}} = \tau_L$.

The proof of Proposition 2.4 is postponed to the end of this section.

Lemma 2.5. *Any $\phi \in \mathrm{Dr}_1(\mathbf{A}_\mathcal{H}, L)$ has the following form*

$$\begin{cases} \phi_{\overline{X}} = \Delta\tau^2 + g\tau + \gamma(\overline{X}) \\ \phi_{\overline{Y}} = \beta\tau_L, \end{cases}$$

where $\Delta \in L^\times$, $g \in L$, $\beta \in \mathbb{F}_q^\times$. Moreover, β is a squareroot of $\alpha\,\mathrm{Norm}_{L/\mathbb{F}_q}(\Delta) \in \mathbb{F}_q^\times$ and it is uniquely determined by Δ and g.

Proof. Since $\overline{X}$ has degree 2 in $\mathbf{A}_\mathcal{H}$ and ϕ has rank 1, $\phi_{\overline{X}}$ must be an Ore polynomial of τ-degree 2. Therefore, $\phi_{\overline{X}} = \Delta\tau^2 + g\tau + \gamma(\overline{X})$ for some $\Delta \in L^\times$, $g \in L$.

Next, we show that $\phi_{\overline{Y}} = \beta\tau_L$ for some $\beta \in \mathbb{F}_q^\times$. We start by noticing that since ϕ has rank 1 and $\overline{Y}$ has degree d, we must have $\deg_\tau(\phi_{\overline{Y}}) = d$. As $\phi_{\overline{p}}$ has constant coefficient zero, [Gek91, (1.4), Eq. (ii)] implies that $\tau^{d/m}$ right-divides $\phi_{\overline{p}}$. Therefore $\phi_{\overline{f}} = \alpha\phi_{\overline{p}}^m$ is right-divisible by $\tau^d = \tau_L$. Since $\overline{f}$ has degree $2d$ and ϕ has rank 1, this implies that $\phi_{\overline{f}} = w\tau^d$ for some $w \in L\{\tau\}$ of τ-degree d, and consequently $\phi_{\overline{Y}}\phi_{\overline{Y}+\overline{h}} = \phi_{\overline{f}} = w\tau_L$. Since h is not divisible by p, $\overline{Y} + \overline{h} \notin \mathfrak{p}$ and therefore $\phi_{\overline{Y}+\overline{h}}$ is separable. Consequently, $\phi_{\overline{Y}+\overline{h}} = w/\beta$ for some $\beta \in L^\times$ and $\phi_{\overline{Y}} = \beta\tau_L$.

By examinating the coefficient of τ^{2d} in the equation $\phi_{\overline{Y}}^2 + \phi_{\overline{Y}}\phi_{\overline{h}} = \phi_{\overline{f}}$ we obtain that $\beta^2 = \alpha\,\mathrm{Norm}_{L/\mathbb{F}_q}(\Delta)$ (as $[L : \mathbb{F}_q]$ is odd, τ^2 is a generator of $\mathrm{Gal}(L/\mathbb{F}_q)$). Since d is odd, there is no subfield of L of degree 2 over $\mathbb{F}_q$, and hence $\beta \in \mathbb{F}_q^\times$. We then prove that only one squareroot β of $\alpha\,\mathrm{Norm}_{L/\mathbb{F}_q}(\Delta)$ is suitable. If q is a power of 2, then there is only one squareroot. Therefore, let us assume now that q is odd, and let $\pm\delta$ be the two distinct squareroots of $\alpha\,\mathrm{Norm}_{L/\mathbb{F}_q}(\Delta)$. By contradiction, assume that there exists Drinfeld modules $\psi, \psi' \in \mathrm{Dr}_1(\mathbf{A}_\mathcal{H}, L)$ such that $\psi_{\overline{X}} = \psi'_{\overline{X}} = \Delta\tau^2 + g + \gamma(\overline{X})$ and $\psi_{\overline{Y}} = \delta\tau_L$, $\psi_{\overline{Y}} = -\delta\tau_L$. Then $0 = \psi_{\overline{Y}^2+\overline{h}\overline{Y}-\overline{f}} - \psi'_{\overline{Y}^2+\overline{h}\overline{Y}-\overline{f}} = 2\delta\psi'_h\tau_L = 0$, which contradicts the fact that $h \neq 0$. □

Lemma 2.6. *Any $\phi \in \mathrm{Dr}_1(\mathbf{A}_\mathcal{H}, L)$ is $\overline{L}$-isomorphic to a Drinfeld module $\psi \in \mathrm{Dr}_1(\mathbf{A}_\mathcal{H}, L)$ such that $\psi_{\overline{Y}} = \tau_L$.*

Proof. By Lemma 2.5, $\phi_{\overline{Y}} = \beta\tau_L$ for some $\beta \in \mathbb{F}_q^\times$. Let $\mu \in L^\times$ be an element such that $\mathrm{Norm}_{L/\mathbb{F}_q}(\mu) = \beta$ and let $\lambda \in \overline{L}^\times$ be a $(q-1)$th-root of μ. Then $\lambda^{q^d-1} = (\lambda^{q-1})^{1+q+q^2+\cdots+q^{d-1}} = \mathrm{Norm}_{L/\mathbb{F}_q}(\mu) = \beta$. Direct computations show that the Drinfeld module $\psi \in \mathrm{Dr}_1(\mathbf{A}_\mathcal{H}, L)$ defined for all $a \in \mathbf{A}_\mathcal{H}$ by $\psi_a = \mu\phi_a\mu^{-1}$ satisfies the desired property. □

Proof of Proposition 2.4. To a Drinfeld module $\phi \in \mathrm{Dr}_2(\mathbb{F}_q[X], L)$ with characteristic polynomial ξ, we associate a Drinfeld module $\psi \in \mathrm{Dr}_1(\mathbf{A}_\mathcal{H}, L)$ defined by $\psi_{\overline{X}} = \phi_X$ and $\psi_{\overline{Y}} = \tau_L$.

Let $\phi' = \alpha\phi\alpha^{-1} \in \mathrm{Dr}_2(\mathbb{F}_q[X], L)$, $\alpha \in \overline{L}$, be a Drinfeld module $\overline{L}$-isomorphic to ϕ. Note that the characteristic polynomial of the Frobenius endomorphism of ϕ' need not be ξ. We prove that ψ' defined by $\psi'_{\overline{X}} = \phi'_X$ and $\psi'_{\overline{Y}} = \alpha\tau_L\alpha^{-1} = \alpha^{1-q^d}\tau_L$ is a Drinfeld module in $\mathrm{Dr}_1(\mathbf{A}_\mathcal{H}, L)$. Writing $\phi_X = \Delta\tau^2 + g\tau + \gamma(X)$, we must have $g \neq 0$ since otherwise ϕ would have j-invariant 0; ϕ would be supersingular [BK92, Lem. 3.2], which contradicts our assumption that h is not divisible by p (see Definition 2.1). Since the coefficient of τ in ϕ'_X equals $\alpha^{q-1}g$ and is in L, we obtain that $\alpha^{q-1} \in L$. Then $\alpha^{1-q^d} \in L$ as a power of $\alpha^{q-1} \in L$. Therefore, $\psi' \in \mathrm{Dr}_1(\mathbf{A}_\mathcal{H}, L)$.

Notice that if $\xi(\phi'_X, \tau_L) = 0$, then $\alpha \in L$ (Proposition 2.3), so that $\alpha\tau_L\alpha^{-1} = \tau_L$. The Drinfeld modules ψ and ψ' are $\overline{L}$-isomorphic, and we extend our association to a well-defined map from the set $\overline{L}$-isomorphism classes of Drinfeld modules in $\mathrm{Dr}_2(\mathbb{F}_q[X], L)$ containing a representative whose characteristic polynomial of the Frobenius endomorphism is ξ, to the set of $\overline{L}$-isomorphism classes of Drinfeld modules in $\mathrm{Dr}_1(\mathbf{A}_\mathcal{H}, L)$. It remains to prove that this map is bijective. Injectivity comes easily and surjectivity is a direct consequence of Lemma 2.6. □

By using Proposition 2.4, we can define the j-*invariant* of a Drinfeld module in $\mathrm{Dr}_1(\mathbf{A}_\mathcal{H}, L)$ as the j-invariant of its corresponding $\overline{L}$-isomorphism class in $\mathrm{Dr}_2(\mathbb{F}_q[X], L)$.

2.3 A group action from class field theory

Our object of study is a group action of $\mathrm{Cl}(\mathbf{A})$ on the set of isomorphism classes of $\mathrm{Dr}_r(\mathbf{A}, K)$, where $\mathbf{A}$ and K are like in Section 1.2. Indeed, if $\mathfrak{a} \subset \mathbf{A}$ is a nonzero ideal, we define

$$\iota_\mathfrak{a} = \mathrm{rgcd}\left(\{\phi_f : f \in \mathfrak{a}\}\right).$$

By [Hay91, Sec. 4], $\iota_\mathfrak{a}$ is a well-defined isogeny from ϕ to some Drinfeld module in $\mathrm{Dr}_r(\mathbf{A}, K)$ denoted $\mathfrak{a} \star_K \phi$. This map actually has multiplicative properties, and we can show that principal ideals lead to isogenies that are actually K-isomorphisms. Therefore this map can be extended to a group action of $\mathrm{Cl}(\mathbf{A})$ on the set of K-isomorphism classes of Drinfeld modules in $\mathrm{Dr}_r(\mathbf{A}, K)$. A similar group action in fact appears to be one of the main motivations in the landmark paper by Drinfeld for making explicit the class field theory of function fields, see [Dri74, Th. 1].

In this section, $d, m, p, h, f, \xi, \mathcal{H}, \mathbf{A}_\mathcal{H}, \mathfrak{p}, L$ are as in Section 2.2.

Theorem 2.7. *If $\mathrm{Dr}_1(\mathbf{A}_\mathcal{H}, L)$ is nonempty, then the set of $\overline{L}$-isomorphism classes of Drinfeld modules in $\mathrm{Dr}_1(\mathbf{A}_\mathcal{H}, L)$ is a principal homogeneous space for $\mathrm{Cl}(\mathbf{A}_\mathcal{H})$ under the $\star_L$ action.*

The proof of Theorem 2.7 is postponed to the end of this section.

This theorem can be seen as a reduction modulo prime ideals of the following general theorem, which might itself be seen as an analog of [Sil94, Prop. 2.4, Lem. 2.5.1] for function fields. We emphasize that this theorem holds in greater generality than what we need here; it holds for any function field and it is not restricted to hyperelliptic curves.

Theorem 2.8 ([Hay91, Th. 9.3])**.** *Let $\mathbf{k}$ be the function field of $\mathcal{H}$, $\mathbf{K}$ be the completion of $\mathbf{k}$ at the place ∞, and $\mathbf{C}$ be the completion of an algebraic closure $\overline{\mathbf{K}}$. Then the set of $\mathbf{C}$-isomorphism classes of Drinfeld modules in $\mathrm{Dr}_1(\mathbf{A}_\mathcal{H}, \mathbf{C})$ is a principal homogeneous space for $\mathrm{Cl}(\mathbf{A}_\mathcal{H})$ under the $\star_\mathbf{C}$ action.*

Our strategy to prove Theorem 2.7 is to use the reduction and lifting properties of ordinary Drinfeld modules [Hay91, Sec. 11][BK92, Th. 3.4].

Let K be a finite extension of $\mathbf{k}$. Let $\mathfrak{P}$ be a place of K above $\mathfrak{p} \subset \mathbf{A}_\mathcal{H}$ and $\mathcal{O}_\mathfrak{P}$ be the associated discrete valuation ring, with the associated reduction morphism $\mathrm{red}_\mathfrak{P} : \mathcal{O}_\mathfrak{P} \twoheadrightarrow \mathcal{O}_\mathfrak{P}/\mathfrak{P}$. An Ore polynomial $f \in K\{\tau\}$ is said to be *defined over* $\mathcal{O}_\mathfrak{P}$ and its coefficients lie in $\mathcal{O}_\mathfrak{P}$ and its leading coefficient is invertible in $\mathcal{O}_\mathfrak{P}$. A Drinfeld $\mathbf{A}_\mathcal{H}$-module ϕ over K is said to be *defined over* $\mathcal{O}_\mathfrak{P}$ if for all $a \in \mathbf{A}_\mathcal{H}$, ϕ_a is defined over $\mathcal{O}_\mathfrak{P}$. Let $\mathrm{Dr}_{r,\mathfrak{P}}(\mathbf{A}_\mathcal{H}, K)$ be the set of Drinfeld modules defined over $\mathcal{O}_\mathfrak{P}$. By considering the morphism $\gamma : \mathbf{A}_\mathcal{H} \twoheadrightarrow \mathbf{A}_\mathcal{H}/\mathfrak{p} \hookrightarrow \mathcal{O}_\mathfrak{P}/\mathfrak{P}$, the reduction map $\mathrm{red}_\mathfrak{P}$ extends canonically to a map $\mathrm{Dr}_{r,\mathfrak{P}}(\mathbf{A}_\mathcal{H}, K) \to \mathrm{Dr}_r(\mathbf{A}_\mathcal{H}, \mathcal{O}_\mathfrak{P}/\mathfrak{P})$.

Lemma 2.9. *For any $\phi \in \mathrm{Dr}_{r,\mathfrak{P}}(\mathbf{A}_\mathcal{H}, K)$ and any ideal $\mathfrak{a} \subset \mathbf{A}_\mathcal{H}$, the Drinfeld module $\mathfrak{a} \star_K \phi$ is defined over $\mathcal{O}_\mathfrak{P}$ and*

$$\mathrm{red}_\mathfrak{P}(\mathfrak{a} \star_K \phi) = \mathfrak{a} \star_{(\mathcal{O}_\mathfrak{P}/\mathfrak{P})} \mathrm{red}_\mathfrak{P}(\phi).$$

Proof. The Drinfeld module $\mathfrak{a} \star_K \phi$ is defined over $\mathcal{O}_\mathfrak{P}$ by [Hay91, Prop. 11.2], hence $\mathrm{red}_\mathfrak{P}(\mathfrak{a} \star_K \phi)$ is well-defined. Let $\iota_\mathfrak{a}$ be the monic generator of the left-ideal in $K\{\tau\}$ generated by $\{\phi_g : g \in \mathfrak{a}\}$. Since ϕ is defined over $\mathcal{O}_\mathfrak{P}$, we deduce that $\iota_\mathfrak{a}$ must have coefficients in $\mathcal{O}_\mathfrak{P}$ and that its reduction generates the left-ideal in $(\mathcal{O}_\mathfrak{P}/\mathfrak{P})\{\tau\}$ generated by $\{\mathrm{red}_\mathfrak{P}(\phi_g) : g \in \mathfrak{a}\}$. Consequently, $\mathrm{red}_\mathfrak{P}(\iota_\mathfrak{a})$ is the isogeny associated to $\mathfrak{a} \star_{(\mathcal{O}_\mathfrak{P}/\mathfrak{P})} \mathrm{red}_\mathfrak{P}(\phi)$, which concludes the proof. □

Proof of Theorem 2.7. Using the correspondence established in Proposition 2.4 between $\overline{L}$-isomorphism classes of Drinfeld modules, we can associate to any Drinfeld module in $\mathrm{Dr}_1(\mathbf{A}_\mathcal{H}, L)$ a Drinfeld module in $\mathrm{Dr}_2(\mathbb{F}_q[X], L)$ whose characteristic polynomial of the Frobenius endomorphism is ξ. Throughout this proof, we fix a place $\mathfrak{P}$ of $\overline{\mathbb{F}_q(X)}$ above $\mathfrak{p}$. Such a place defines a compatible discrete valuation ring $\mathcal{O}_\mathfrak{P}^{(K)}$ in any finite extension K of $\mathbb{F}_q(X)$.

Let us prove the transitivity of the action. Let $j_1, j_2 \in L$ be the j-invariants of two Drinfeld modules $\phi, \psi \in \mathrm{Dr}_2(\mathbb{F}_q[X], L)$, whose characteristic polynomial of the Frobenius is ξ. Since the ideal $\langle p(\overline{X})\rangle$ splits in $\mathbf{A}_\mathcal{H}$ ($\langle p(\overline{X})\rangle = \langle p(\overline{X}), \overline{Y}\rangle \cdot \langle p(\overline{X}), \overline{Y} + h(\overline{X})\rangle$), Deuring's lifting theorems for Drinfeld modules [BK92, Th. 3.4, Th. 3.5] (see [Lan87, Ch. 13, §4] for the analogs for elliptic curves) imply that there exists a finite extension K of $\mathbb{F}_q(X)$ and two $\mathbf{C}$-isomorphism classes of Drinfeld modules in $\mathrm{Dr}_2(\mathbb{F}_q[X], K)$, whose j-invariants reduce to j_1, j_2 modulo $\mathfrak{P}$. Those j-invariants are algebraic integers in $\mathbf{C}$ [Gek83, §(4.3)]. Moreover, those classes contain Drinfeld modules $\phi', \psi' \in \mathrm{Dr}_2(\mathbb{F}_q[X], K)$ whose endomorphism rings are isomorphic to $\mathrm{End}(\phi) \simeq \mathrm{End}(\psi) \simeq \mathbf{A}_\mathcal{H}$. Therefore those Drinfeld modules can be regarded as Drinfeld modules in $\mathrm{Dr}_{1,\mathfrak{P}}(\mathbf{A}_\mathcal{H}, K)$. Since $\star_K$ acts on $\mathrm{Dr}_{1,\mathfrak{P}}(\mathbf{A}_\mathcal{H}, K)$ [Hay91, Prop. 11.2], and the group action associated to $\star_\mathbf{C}$ is transitive (Theorem 2.8), there is an ideal $\mathfrak{a} \subset \mathbf{A}_\mathcal{H}$ such that $\mathfrak{a} \star_K \phi'$ is isomorphic to ψ'. Consequently, the j-invariants $\mathfrak{a} \star_K \phi'$ and ψ' are equal, and therefore their reduction modulo $\mathfrak{P}$ equals j_2. Using Lemma 2.9, the j-invariant of $\mathfrak{a} \star_K \phi'$ reduces modulo $\mathfrak{P}$ to the j-invariant of $\mathfrak{a} \star_{\mathcal{O}_\mathfrak{P}^{(K)}/\mathfrak{P}} \phi$, which therefore also equals j_2. Hence $\mathfrak{a}$ sends the $\overline{L}$-isomorphism class of ϕ to that of ψ via the $\star_{\overline{L}}$ action (which is the same as the $\star_L$-action on ϕ, since ϕ is defined over L).

Finally, let us prove the freeness of the action. Let $\phi \in \mathrm{Dr}_1(\mathbf{A}_\mathcal{H}, L)$ be a Drinfeld module, and set $\psi = \mathfrak{a} \star_L \phi$. Assume that ϕ and ψ are $\overline{L}$-isomorphic. Since ϕ and ψ are L-isogenous, by Proposition 2.3 they must be L-isomorphic. Let $\alpha \in L$ be such an isomorphism, i.e. $\alpha\phi\alpha^{-1} = \psi$. Using [BK92, Th. 3.4] as above, the lifting procedure provides us with $\phi' \in \mathrm{Dr}_{1,\mathfrak{P}}(\mathbf{A}_\mathcal{H}, K)$ which reduces to ϕ modulo $\mathfrak{P}$. Then set $\psi' = \mathfrak{a} \star_K \phi'$, and let $\iota_\mathfrak{a}$ be the associated isogeny. By the same argument as in the proof of Lemma 2.9, we obtain that $\iota_\mathfrak{a}$ is defined over $\mathcal{O}_\mathfrak{P}^{(K)}$ and that $\mathrm{red}_\mathfrak{P}(\iota_\mathfrak{a}) = \alpha$ which implies that $\iota_\mathfrak{a} \in K$, and therefore ϕ' and ψ' are isomorphic. Consequently, $\mathfrak{a}$ is principal (Theorem 2.8), and hence the group action associated to $\star_L$ is free. □

3 Algorithms

In this section, $d, m, p, h, f, \xi, \mathcal{H}, \mathbf{A}_\mathcal{H}, \mathfrak{p}, L$ are as in Section 2.2. We also fix $\omega \coloneqq \gamma(X) \in L$.

3.1 Computation of the group action

Before describing the algorithm for computing the group action in Theorem 2.7, we need data structures to represent elements in $\mathrm{Cl}(\mathbf{A}_\mathcal{H})$ and $\overline{L}$-isomorphism classes. Thanks to Proposition 2.4, we can use j-invariants — which are elements of L — to represent $\overline{L}$-isomorphism classes of Drinfeld modules in $\mathrm{Dr}_1(\mathbf{A}_\mathcal{H}, L)$. For representing elements in $\mathrm{Cl}(\mathbf{A}_\mathcal{H})$, we shall use Mumford coordinates [CFA+05, Th. 14.5], since in our case $\mathrm{Cl}(\mathbf{A}_\mathcal{H})$ is isomorphic to $\mathrm{Pic}^0(\mathcal{H})$:

Lemma 3.1. *The ring $\mathbf{A}_\mathcal{H}$ is a Dedekind domain, and $\mathrm{Cl}(\mathbf{A}_\mathcal{H}) \simeq \mathrm{Pic}^0(\mathcal{H})$.*

Proof. The ring $\mathbf{A}_{\mathcal{H}}$ is a Dedekind domain because $\mathcal{H}$ is smooth in the affine plane [Lor96, Ch. 7, Cor. 2.7]. The isomorphism $\mathrm{Cl}(\mathbf{A}_{\mathcal{H}}) \simeq \mathrm{Pic}^0(\mathcal{H})$ comes from the fact that there is a unique degree-1 place ∞ at infinity. Indeed, the group of affine divisors $\mathrm{Div}(\mathbf{A}_{\mathcal{H}})$ (i.e. the subgroup of divisors whose valuation at infinity is 0) is isomorphic to the group of degree-0 divisors in $\mathrm{Div}_0(\mathcal{H})$ via the map which sends a divisor D in $\mathrm{Div}(\mathbf{A}_{\mathcal{H}})$ to $D - \deg(D)\infty$. Next, we notice that D is principal in $\mathrm{Div}(\mathbf{A}_{\mathcal{H}})$ if and only if its image in $\mathrm{Div}_0(\mathcal{H})$ is principal. We conclude by using the isomorphism in [Lor96, Ch. 7, Prop. 7.1], which shows that the quotient of $\mathrm{Div}(\mathbf{A}_{\mathcal{H}})$ by principal divisors is isomorphic to $\mathrm{Cl}(R)$. □

Since $\mathcal{H}$ has genus $\lfloor([L:\mathbb{F}_q]-1)/2\rfloor$, elements in $\mathrm{Pic}(\mathcal{H})^0$ can be represented by *Mumford coordinates* [CFA+05, Th. 14.5], which are pairs of polynomials $(u, v) \in \mathbb{F}_q[X]^2$ such that:

(i) u is a nonzero monic polynomial of degree at most $([L:\mathbb{F}_q]-1)/2$,
(ii) $\deg(v) < \deg(u)$,
(iii) u divides $\xi(X, v(X))$.

Mumford coordinates (u, v) encode the class of the ideal $\langle u(\overline{X}), \overline{Y} - v(\overline{X})\rangle \subset \mathbf{A}_{\mathcal{H}}$.

Algorithm 1: GroupAction

Input:
— A j-invariant $j \in L$ encoding an isomorphism class $\mathcal{C}$ in $\mathrm{Dr}_1(\mathbf{A}_{\mathcal{H}}, L)$.
— Mumford coordinates $(u, v) \in \mathbb{F}_q[X]^2$ for a divisor class $[D]$ in $\mathrm{Pic}^0(\mathcal{H})$.

Output: The j-invariant obtained by making $[D]$ act on $\mathcal{C}$ by the $\star_L$ action.

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 $\iota \leftarrow \mathrm{EuclideRGCD}(\widetilde{u}, \tau_L - \widetilde{v})$; /* $\iota = \sum_{0 \leqslant k \leqslant \deg_\tau(\iota)} \iota_k \tau^k$ */
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** $\widehat{g}^{q+1}/\widehat{\Delta}$.

Proposition 3.2. *Algorithm 1 (*GroupAction*) is correct.*

Proof. A representative of the class in $\mathrm{Cl}(\mathbf{A}_{\mathcal{H}}) \simeq \mathrm{Pic}^0(\mathcal{H})$ represented by the Mumford coordinates (u, v) is the ideal $\langle u(\overline{X}), \overline{Y} - v(\overline{X})\rangle \subset \mathbf{A}_{\mathcal{H}}$. A representative of the isomorphism class of Drinfeld modules represented by the j-invariant j is a Drinfeld module $\phi \in \mathrm{Dr}_1(\mathbf{A}_{\mathcal{H}}, L)$ such that $\phi_{\overline{X}} = j^{-1}\tau^2 + \tau + \omega$ and $\phi_{\overline{Y}} = \beta\tau_L$ for some $\beta \in \mathbb{F}_q^\times$ (see Section 2.2). Note that $j \neq 0$ by [BK92, Lem. 3.2]. We shall prove that $\langle u(\overline{X}), \overline{Y} - v(\overline{X})\rangle \star_L \phi = \psi$, where $\psi \in \mathrm{Dr}_1(\mathbf{A}_{\mathcal{H}}, L)$ is the Drinfeld module such that $\psi_{\overline{X}} = \widehat{\Delta}\tau^2 + \widehat{g}\tau + \omega$ and $\psi_{\overline{Y}} = \beta\tau_L$.

Assuming the correctness of the subroutine EuclideRGCD (Proposition 3.3), the Ore polynomial ι computed at Step 3 is $\mathrm{rgcd}(\phi_{u(\overline{X})}, \tau_L - \phi_{v(\overline{X})})$, which is by construction the monic Ore polynomial defining the isogeny. Since we need to invert the coefficient ι_0 (at Step 4), we need to prove that ι is separable. This is indeed true: ι right-divides $\phi_{u(\overline{X})}$, which is separable because $\deg(u) < d$. Hence u cannot be a multiple of p, which is a generator of $\mathrm{Ker}(\gamma)$.

Since ι is an isogeny [Hay91, Cor. 5.10], there exists $\psi \in \mathrm{Dr}_1(\mathbf{A}_{\mathcal{H}}, L)$ such that $\iota \cdot \phi_{\overline{X}} = \psi_{\overline{X}} \cdot \iota$ where $\psi_{\overline{X}}$ has τ-degree 2. It remains to prove that $\psi_{\overline{X}} = \widehat{\Delta}\tau^2 + \widehat{g}\tau + \omega$. This is done by extracting as in Equations (1.1) the coefficients of τ and $\tau^{\deg_\tau(\iota)+2}$ in the equality $\iota \cdot \phi_{\overline{X}} = \psi_{\overline{X}} \cdot \iota$, which provides us with:

$$\begin{cases} \iota_0\, g + \iota_1\, \omega^q &= \widehat{g}\, \iota_0^q + \omega\, \iota_1, \\ j^{-q^{\deg_\tau(\iota)}} &= \widehat{\Delta}. \end{cases}$$

There is only one pair $(\widehat{\Delta}, \widehat{g}) \in L^2$ which satisfies these two equalities, and the associated Drinfeld module has j-invariant $\widehat{g}^{q+1}/\widehat{\Delta}$. □

Algorithm 2: EUCLIDERGCD
Input: Two Ore polynomials $a, b \in L\{\tau\}$, $a \neq 0$.
Output: The right-gcd of a and b.

```
if b = 0 then
    return a.
if deg_τ(b) > deg_τ(a) then
    return EUCLIDERGCD(b, a).
μ_a ← leading coefficient of a;
μ_b ← leading coefficient of b;
return EUCLIDERGCD(a − τ^(deg_τ(a)−deg_τ(b)) (μ_a/μ_b) b, b).
```

Proposition 3.3. *Algorithm 2 (*EUCLIDERGCD*) is correct.*

Proof. Algorithm 2 is the classical Euclide's algorithm for computing a gcd. It relies on the fact that an Ore polynomial right-divides a and b if and only if it right-divides $a - \tau^{\deg_\tau(a)-\deg_\tau(b)}(\mu_a/\mu_b)b$ and b, which implies that the right-gcd of a and b does not change at each recursive call. Consequently, if the algorithm terminates, then it returns the right-gcd of a and b. Noticing that the integer $\max(\deg_\tau(a), \deg_\tau(b))$ decreases at each recursive call shows that the algorithm must terminate. □

3.2 Computation of the ideal corresponding to an isogeny

In this section, we make explicit the transitivity of the group action: for two Drinfeld modules $\phi, \psi \in \mathrm{Dr}_1(\mathbf{A}_\mathcal{H}, L)$ and an isogeny $\iota : \phi \to \psi$, we study the computation of Mumford coordinates $(u, v) \in \mathbb{F}_q[X]^2$ such that the class of $\langle u(\overline{X}), \overline{Y} - v(\overline{X})\rangle \subset \mathbf{A}_\mathcal{H}$ sends the $\overline{L}$-isomorphism class of ϕ to that of ψ via $\star_L$.

We use the shorthand notation $\mathrm{Dr}_2(\mathbb{F}_q[X], L)_\xi$ to denote the subset of Drinfeld modules in $\mathrm{Dr}_2(\mathbb{F}_q[X], L)$ whose characteristic polynomial of the Frobenius endomorphism is ξ. By Proposition 2.4, to any $\phi \in \mathrm{Dr}_1(\mathbf{A}_\mathcal{H}, L)$, we can associate a Drinfeld module $\phi' \in \mathrm{Dr}_2(\mathbb{F}_q[X], L)_\xi$. Notice that $\star_L$ leaves $\mathrm{Dr}_2(\mathbb{F}_q[X], L)_\xi$ globally invariant. Hence, by slight abuse of notation, we shall use the $\star_L$ notation to also denote the corresponding action of nonzero ideals in $\mathbf{A}_\mathcal{H}$ over $\mathrm{Dr}_2(\mathbb{F}_q[X], L)_\xi$. Another useful remark is that computing Mumford coordinates for the class of a given ideal in $\mathbf{A}_\mathcal{H}$ can be done efficiently by using the reduction step of Cantor's algorithm [CFA+05, Algo. 14.7]. Therefore, our main algorithmic task is to construct the ideal in $\mathbf{A}_\mathcal{H}$ corresponding to a given isogeny.

We start by the following lemma, which establishes a correspondence between ideals in $\mathbf{A}_\mathcal{H}$ and isogenies:

Lemma 3.4. *Let $\phi \in \mathrm{Dr}_2(\mathbb{F}_q[X], L)_\xi$ be an ordinary Drinfeld module. Then there is a one-to-one correspondence between monic isogenies with domain ϕ and nonzero ideals in $\mathbf{A}_\mathcal{H}$. Moreover, given Drinfeld modules $\phi_1, \phi_2, \phi_3 \in \mathrm{Dr}_2(\mathbb{F}_q[X], L)_\xi$ and isogenies $\iota_1 : \phi_1 \to \phi_2$,*

$\iota_2 : \phi_2 \to \phi_3$, the ideal associated to $\iota_2 \cdot \iota_1$ in $\mathbf{A}_{\mathcal{H}}$ is the product of the ideals associated to ι_1 and ι_2.

Proof. To any monic isogeny $\iota : \phi \to \psi$, we associate the nonzero ideal $\mathrm{Hom}(\psi, \phi)\iota \subset \mathrm{End}(\phi) \simeq \mathbf{A}_{\mathcal{H}}$. Notice that $\psi \in \mathrm{Dr}_2(\mathbb{F}_q[X], L)_\xi$ (Section 2). Reciprocally, to any nonzero ideal $\mathfrak{a} \subset \mathbf{A}_{\mathcal{H}}$ corresponds the isogeny which is the monic generator of the left-ideal in $L\{\tau\}$ generated by $\{g(\phi_X, \tau_L) : g \in \mathfrak{a}\}$. We refer to [Gek91, §(3.6)] for more details.

To prove the second statement, we start by letting Ξ denote the isomorphism between $\mathrm{End}(\phi)$ and $\mathrm{End}(\psi)$ which sends $g(\phi_X, \tau_L)$ to $g(\psi_X, \tau_L)$ for any $g \in \mathbf{A}_{\mathcal{H}}$. Let $\widehat{\iota}$ be a u-dual isogeny for ι, for some $u \in \mathbb{F}_q[X]$ such that ι right-divides ϕ_u (see Section 1.3). Notice that for all $g \in \mathbf{A}_{\mathcal{H}}$, ϕ_u right-divides $g(\phi_X, \tau_L) \cdot \widehat{\iota}$ if and only if ψ_u left-divides $\widehat{\iota} \cdot g(\psi_X, \tau_L)$. Said otherwise, Ξ sends the ideal $\mathrm{Hom}(\psi, \phi)\iota \subset \mathrm{End}(\phi)$ to the ideal $\iota \,\mathrm{Hom}(\psi, \phi) \subset \mathrm{End}(\psi)$. By considering the isomorphism $\Xi_{1,2} : \mathrm{End}(\phi_1) \to \mathrm{End}(\phi_2)$ and by using the commutativity of $\mathrm{End}(\phi_2)$, we obtain

$$\begin{aligned}
\mathrm{Hom}(\phi_3, \phi_2)\iota_2 \cdot \Xi_{1,2}(\mathrm{Hom}(\phi_2, \phi_1)\iota_1) &= (\mathrm{Hom}(\phi_3, \phi_2)\iota_2) \cdot (\iota_1 \,\mathrm{Hom}(\phi_2, \phi_1)) \\
&= (\iota_1 \,\mathrm{Hom}(\phi_2, \phi_1)) \cdot (\mathrm{Hom}(\phi_3, \phi_2)\iota_2) \\
&= \Xi_{1,2}(\mathrm{Hom}(\phi_3, \phi_2) \,\mathrm{Hom}(\phi_2, \phi_1)\iota_2\iota_1) \\
&\subset \Xi_{1,2}(\mathrm{Hom}(\phi_3, \phi_1)\iota_2\iota_1).
\end{aligned}$$

To conclude, we use the properties of the norm of isogenies: the norm is multiplicative [Gek91, Lem. 3.10.(i)] and it corresponds to the norm of the associated ideal in $\mathbf{A}_{\mathcal{H}}$ [Gek91, Lem. 3.10.(iv)]. Consequently, the norms on both sides of the inclusion are equal. This implies that the last inclusion is in fact an equality. □

The algorithm we describe below computes prime factors of the ideal in $\mathbf{A}_{\mathcal{H}}$ corresponding to the given isogeny, in order to recover the full factorization. Each prime non-principal factor is treated independently by the subroutine PrimeIsogenyToPrimeIdeal (Algorithm 3).

Algorithm 3: PrimeIsogenyToPrimeIdeal

Input:
- An ordinary Drinfeld module $\phi \in \mathrm{Dr}_2(\mathbb{F}_q[X], L)_\xi$,
- A separable isogeny $\iota : \phi \to \psi$ between $\phi, \psi \in \mathrm{Dr}_2(\mathbb{F}_q[X], L)_\xi$, with $\deg_\tau(\iota) = \deg(r)$,
- A monic prime $r \in \mathbb{F}_q[X]$.

Output: A polynomial $v \in \mathbb{F}_q[X]$ such that the left-ideal $\langle \phi_u, \tau_L - \phi_v \rangle \subset L\{\tau\}$ is generated by ι.

1 $y \leftarrow$ remainder in the right-division of τ_L by ι;
2 $\iota^{(0)}, \ldots, \iota^{(n)} \leftarrow$ remainders in the right-divisions of $\varphi_{X^0}, \ldots, \varphi_{X^{\deg(r)-1}}$ by ι;
3 using linear algebra, find $(v_0, \ldots, v_{\deg(r)-1}) \in \mathbb{F}_q^{\deg(r)}$ such that $y - (v_0\iota^{(0)} + \cdots + v_{\deg(r)-1}\iota^{(\deg(r)-1)}) = 0$;
4 **return** $v_0 + v_1 X + \cdots + v_{\deg(r)-1} X^{\deg(r)-1}$.

Proposition 3.5. *Algorithm 3 (PrimeIsogenyToPrimeIdeal) is correct.*

Proof. Since ι is an r-isogeny, $\phi_r \in \mathrm{Hom}(\psi, \phi)\iota$. Since $\mathbf{A}_{\mathcal{H}}$ is a Dedekind ring in a quadratic extension of $\mathbb{F}_q(X)$, the ideal $\mathrm{Hom}(\psi, \phi)\iota$ — regarded as an ideal in $\mathbf{A}_{\mathcal{H}}$ by Lemma 3.4 — contains the prime r. Therefore, it can only be either the full ring $\mathbf{A}_{\mathcal{H}}$, the principal ideal $\langle r \rangle$, or a prime ideal of degree 1 above $\langle r \rangle$.

By Lemma 1.3, the left-ideal in $L\{\tau\}$ generated by elements in $\mathrm{Hom}(\psi, \phi)\iota$ equals $L\{\tau\}\iota$, which is neither the full ring $L\{\tau\}$, nor $L\{\tau\}\phi_r$ since $\deg_\tau(\phi_r) = 2\deg(r) > \deg(\iota)$. Consequently, using the correspondence in Lemma 3.4, $\mathrm{Hom}(\psi, \phi)\iota$ must be a degree-1 prime ideal

Algorithm 4: IsogenyToIdeal

Input:
- An ordinary Drinfeld module $\phi \in \mathrm{Dr}_2(\mathbb{F}_q[X], L)_\xi$,
- A separable isogeny $\iota : \phi \to \psi$ between ordinary Drinfeld modules in $\mathrm{Dr}_2(\mathbb{F}_q[X], L)_\xi$,
- A (non-necessarily prime) monic polynomial $u \in \mathbb{F}_q[X]$ such that ι right-divides ϕ_u.

Output: The ideal $\mathfrak{a} \subset \mathbb{F}_q[X,Y]/(\xi)$ associated to ι in Lemma 3.4.

1 **if** $u = 1$ **then**
2 **return** $\mathbb{F}_q[X,Y]/(\xi)$.
3 $r \leftarrow$ a nonconstant monic prime factor of u;
4 $\widetilde{\iota} \leftarrow \mathrm{rgcd}(\iota, \phi_r)$;
5 **if** $\widetilde{\iota} = 1$ **then**
6 **return** IsogenyToIdeal$(\phi, \iota, u/r^{\mathrm{val}_r(u)})$.
7 **else if** $\widetilde{\iota} = \lambda\phi_r$ *for some* $\lambda \in L^\times$ **then**
8 **return** $\langle r(\overline{X})\rangle \cdot$ IsogenyToIdeal$(\phi, \iota \cdot \phi_r^{-1}, u/r)$.
9 **else**
10 $v \leftarrow$ IsogenyToPrimeIdeal$(\phi, \widetilde{\iota}, r)$;
11 $\widetilde{\phi} \leftarrow$ the codomain of $\widetilde{\iota}$, computed from ϕ and $\widetilde{\iota}$ with Formulas (1.1);
12 **return** $\langle u(\overline{X}), \overline{Y} - v(\overline{X})\rangle \cdot$ IsogenyToIdeal$(\widetilde{\phi}, \iota \cdot \widetilde{\iota}^{-1}, u/r)$.

above the principal ideal associated to r. Said otherwise, the polynomial $Y^2 + h(X)Y - f(X)$ factors over $(\mathbb{F}_q[X]/(r))[Y]$, and a prime ideal above $\langle r\rangle$ in $\mathbf{A}_\mathcal{H}$ has the form $\langle r(\overline{X}), Y - v(\overline{X})\rangle$, where $v \in \mathbb{F}_q[X]$ satisfies $\xi(\overline{X}, \overline{v}) = 0$ in $\mathbb{F}_q[X]/(r)$. Note that up to reducing v modulo r, we can assume that $\deg(v) < \deg(r)$; under this assumption, v is uniquely defined.

We now prove that the coefficients of v satisfy the equality in Step 3, so that it can indeed be computed via linear algebra. To this end, we need to prove that ι right-divides $\tau_L - \phi_v$. This is a direct consequence of the fact that the ideal $\mathrm{Hom}(\psi, \phi)\iota \subset \mathrm{End}(\phi)$ corresponds to the ideal $\langle r(\overline{X}), Y - v(\overline{X})\rangle \subset \mathbf{A}_\mathcal{H}$. □

Algorithm 4 needs as input a polynomial $u \in \mathbb{F}_q[X]$ such that ι right-divides ϕ_u. It can be found by looking for a non-trivial $\mathbb{F}_q$-linear relation between the remainders of $\phi_{X^0}, \phi_{X^1}, \ldots, \phi_{X^\ell}$ in the right-division by ι. When $\ell \geqslant \deg_\tau(\iota)$, such a non-trivial linear combination exists.

Proposition 3.6. *Algorithm 4 (*IsogenyToIdeal*) terminates and is correct.*

Proof. The proof is done by induction on the degree of u. The termination comes from the fact that the degree of u decreases in each recursive call.

By Lemma 3.4, there is a uniquely defined ideal $\mathfrak{a} \subset \mathbf{A}_\mathcal{H}$ corresponding to ι. Since $\mathbf{A}_\mathcal{H}$ is Dedekind (Lemma 3.1), $\mathfrak{a}$ factors as a product of prime ideals. For $r \in \mathbb{F}_q[X]$ an irreducible polynomial, we let $\mathfrak{a}_r$ denote the product of all primes in the factorization of $\mathfrak{a}$ which contain $\overline{r} \in \mathbf{A}_\mathcal{H}$. Consequently, since $\overline{u} \in \mathfrak{a}$, we have

$$\mathfrak{a} = \prod_{\substack{r \text{ prime} \\ r \text{ divides } u}} \mathfrak{a}_r.$$

Let r be a prime factor of u. Then there are three possible cases, depending on whether r is inert, splits, or ramifies in $\mathbf{A}_\mathcal{H}$.

If r is inert, then $\mathfrak{a}_r = \langle \overline{r}\rangle^\ell$ for some $\ell \geqslant 0$. If $\ell = 0$ then $\mathfrak{a}_r = \mathbf{A}_\mathcal{H}$. In this case, if $u \neq 1$, then $\overline{r} \notin \mathfrak{a}$ and therefore $\mathrm{rgcd}(\iota, \phi_r) = 1$. Consequently, $\overline{r}$ is invertible in $\mathfrak{a}$, and therefore

$\overline{u}/\overline{r}^{\mathrm{val}_r(u)}$ belongs to $\mathfrak{a}$ and we can apply our induction hypothesis. If $\ell > 0$, then $\overline{r}$ divides all elements in $\mathfrak{a}$. Therefore ϕ_r right-divides ι and hence $\widetilde{\iota} = \lambda\phi_r$ for some $\lambda \in L^\times$. Since ϕ_r is an endomorphism of ϕ, $\iota \cdot \phi_r^{-1}$ is a well-defined isogeny between ϕ and ψ and its corresponding ideal in $\mathbf{A}_{\mathcal{H}}$ is $\{g : g \in \mathbf{A}_{\mathcal{H}} \mid g \cdot \overline{r} \in \mathfrak{a}\}$. This ideal contains $\overline{u}/\overline{r}$, hence we can apply our induction hypothesis.

If r splits then the ideal $\langle \overline{r} \rangle \subset \mathbf{A}_{\mathcal{H}}$ factors as a product $\mathfrak{p}_1 \cdot \mathfrak{p}_2$ of two distinct prime ideals. Therefore, $\mathfrak{a}_r = \mathfrak{p}_1^\alpha \cdot \mathfrak{p}_2^\beta$ for some $\alpha, \beta \geqslant 0$. First, if both α and β are nonzero, then $\mathfrak{a}_r = \langle \overline{r} \rangle \cdot \mathfrak{p}_1^{\alpha-1}\mathfrak{p}_2^{\beta-1}$. Consequently, ι is right-divisible by ϕ_r, $\widetilde{\iota} = \lambda\phi_r$ for some $\lambda \in L^\times$ and we can apply our induction hypothesis on the isogeny $\iota \cdot \phi_r^{-1}$. Now, we study the case where either α or β is zero. Without loss of generality, let us assume that $\beta = 0$. Then $\mathfrak{a}_r = \mathfrak{p}_1^\alpha$. In this case, $\widetilde{\iota}$ cannot be right-divisible by ϕ_r: this would contradict the fact that $\langle \overline{r} \rangle$ does not divide $\mathfrak{a}$. On the other hand, $\widetilde{\iota}$ cannot equal 1 since for any element $g \in \mathfrak{p}_1$, $g(\phi_X, \tau_L)$ must right-divide both ϕ_r and ι. Since ι is an isogeny, $\mathrm{Ker}(\iota)$ is an $\mathbb{F}_q[X]$-submodule of $\overline{L}$ (for the module law induced by ϕ), and hence so is $\mathrm{Ker}(\widetilde{\iota}) = \mathrm{Ker}(\iota) \cap \mathrm{Ker}(\phi_r)$. Consequently, $\widetilde{\iota}$ is an isogeny from ϕ to some other Drinfeld module $\phi' \in \mathrm{Dr}_2(\mathbb{F}_q[X], L)_\xi$. The Drinfeld module ϕ' can be computed using Formulas (1.1), and the ideal corresponding to this isogeny can be computed using Algorithm 3, which is correct by Proposition 3.5. To apply the induction hypothesis on ℓ, it remains to prove that $\iota' \coloneqq \iota \cdot \widetilde{\iota}^{-1}$ defines an isogeny $\iota' : \phi' \to \psi$ which right-divides $\phi'_{u/r}$. To this end, let ι_{dual} denote the dual u-isogeny of ι, and let $\widetilde{\iota}_{\mathrm{dual}}$ be the dual r-isogeny of $\widetilde{\iota}$. We have

$$\begin{array}{rcccccl} \phi'_u\phi'_r & = & \widetilde{\iota} \cdot \widetilde{\iota}_{\mathrm{dual}} \cdot \phi'_u & = & \widetilde{\iota} \cdot \phi_u \cdot \widetilde{\iota}_{\mathrm{dual}} & = & \widetilde{\iota} \cdot \iota_{\mathrm{dual}} \cdot \iota \cdot \widetilde{\iota}_{\mathrm{dual}} \\ & = & \widetilde{\iota} \cdot \iota_{\mathrm{dual}} \cdot \iota' \cdot \widetilde{\iota} \cdot \widetilde{\iota}_{\mathrm{dual}} & = & \widetilde{\iota} \cdot \iota_{\mathrm{dual}} \cdot \iota' \cdot \phi'_r. & & \end{array}$$

By dividing on the right by ϕ'_r, we obtain that ι' divides ϕ_u and that it is the u-dual of the composed isogeny $\widetilde{\iota} \cdot \iota_{\mathrm{dual}}$. This proves that ι' is a well-defined isogeny. By using the second statement in Lemma 3.4, we obtain that the ideal associated to ι' is

$$\mathfrak{p}_1^{\alpha-1} \cdot \prod_{\substack{r' \text{ prime} \\ r' \text{ divides } u \\ r' \neq r}} \mathfrak{a}_{r'},$$

which contains $\overline{u}/\overline{r}$, so that we can apply our induction hypothesis.

Finally, the ramified case is proved similarly than the split case. The main difference is that $\mathfrak{p}_1 = \mathfrak{p}_2$, so that $\mathfrak{a}_r = \langle r \rangle^\ell \cdot \mathfrak{p}_1^\alpha$, for some $\ell \geqslant 0$ and $\alpha \in \{0, 1\}$; this does not change the proof. □

4 Post-quantum key exchange

4.1 Protocol and parameters

In order to find suitable cryptographic parameters, we start by fixing $q = 2$. We then choose an extension L of $\mathbb{F}_2$ of prime extension degree $d \geqslant 5$. The order of our group will be of order of magnitude $\approx 2^{d/2}$. To avoid Baby-Step Giant-Step attacks, we need it to be larger than 2^{256}; we choose $d = 521$. We emphasize that choosing a prime extension degree is a desirable feature in a cryptographic context since it avoids any potential attack which would use the existence of subfields between $\mathbb{F}_2$ and L. In what follows, we let ω denote the class of X in $\mathbb{F}_2[X]/\mathfrak{p} \simeq L$.

Then we randomly choose $j \in L^\times$, and we consider the Drinfeld module $\phi \in \mathrm{Dr}_2(\mathbb{F}_q[X], L)$ such that $\phi_X = j^{-1}\tau^2 + \tau + \omega$. We compute the characteristic polynomial $\xi = Y^2 + h(X)Y - f(X)$ of its Frobenius endomorphism, by using for instance the algorithms described in [MS19]. This is very efficient and it costs only a fraction of seconds. We check that $h \neq 0$ (so that our class of Drinfeld modules is not supersingular), and that the curve $\mathcal{H}$ defined by ξ is smooth in the

affine plane, so that it is hyperelliptic. We also check that h is irreducible: this is done to minimize the 2-torsion in $\mathrm{Pic}^0(\mathcal{H})$. If these conditions are not satisfied, then we choose another j-invariant at random in $L^\times$ and we repeat this procedure until the requirements are satisfied.

Finally, we compute the order of $\mathrm{Pic}^0(\mathcal{H})$ using the Denef-Kedlaya-Vercauteren algorithm [Ked01][DV06]; it is implemented in the Magma computer algebra software. This computation costs 53 hours on a Intel(R) Xeon(R) CPU E7-4850. Since the order of $\mathrm{Pic}^0(\mathcal{H})$ is always even [CST14, Cor. 25], we repeat the whole procedure until we find a hyperelliptic curve whose order is "as prime as possible", i.e. until $|\mathrm{Pic}^0(\mathcal{H})|/2$ is prime. We had to run 107 times the Kedlaya-Vercauteren algorithm until we found an $\overline{L}$-isomorphism class of Drinfeld modules (represented by j) satisfying all the desired properties.

We now describe this class. Set $L = \mathbb{F}_2[X]/\mathfrak{p}$, where $\mathfrak{p}$ is the ideal generated by $X^{521} + X^{32} + 1 \in \mathbb{F}_2[X]$. We encode polynomials by using the hexadecimal NTL notation: for instance, `0x4bc` denotes the polynomial $X^2 + X^4 + X^5 + X^7 + X^{10} + X^{11} \in \mathbb{F}_2[X]$. By extension, we also denote elements in L by the NTL hexadecimal convention, implicitly using the reduction modulo the ideal $\mathfrak{p}$. Our isomorphism class of Drinfeld modules has j-invariant (in L)

$$j_0 = \begin{array}{c}\texttt{0xb985b4ce23bd9cf992f1176e17c27dab7ae6727013112a2804cb64abccc7cce06}\\ \texttt{1e12786bb3248809922da35d3b624d67d08087e07c260fcaa9807a420ca83fa95}.\end{array}$$

The coefficients of the characteristic polynomial of the Frobenius endomorphism of the Drinfeld module $\phi \in \mathrm{Dr}_2(\mathbb{F}_2[X], L)$ defined by $\phi_X = j_0^{-1}\tau^2 + \tau + \omega$ are:

$$\begin{cases} h = \texttt{0xb1ffea4ab7e58b96adf4e4972d7db9184821c1d64b375df52669c60973bb80dee} \in \mathbb{F}_2[X], \\ f = X^{521} + X^{32} + 1 \in \mathbb{F}_2[X]. \end{cases}$$

The polynomial $Y^2 + h(X)Y - f(X)$ defines a genus-260 hyperelliptic curve $\mathcal{H}$ over $\mathbb{F}_2$, whose Picard group $\mathrm{Pic}^0(\mathcal{H})$ is cyclic and has almost-prime order

$$2 \times 3154131824675456726041163164150477433504949628897448652594429436560240732956 89.$$

As a proof-of-concept, we implemented Algorithm 1 for computing the group action in C++/NTL. Our code is available at `https://gitlab.inria.fr/pspaenle/crs-drinfeld-521`.

In order to instanciate the non-interactive key exchange protocol based on this HHS, we proceed as follows: Alice and Bob both pick 9 random places $\{P_{A,i}\}_{1\leqslant i\leqslant 9}$, $\{P_{B,i}\}_{1\leqslant i\leqslant 9}$ of degree 35 on $\mathcal{H}$. Then Alice sets $j_{A,0} = j_0$ and she computes inductively $j_{A,i} = [P_{A,i}] \cdot j_{A,i-1}$ for $i \in [\![1, 9]\!]$, where $[P_{A,i}] \in \mathrm{Pic}^0(\mathcal{H})$ denotes the class of the place $P_{A,i}$. Bobs does the same to compute $j_{B,9}$. Then Alice and Bob exchange publicly the values of $j_{A,9}$ and $j_{B,9}$. Finally, Alice sets $j_{A,B,0} = j_{B,9}$ and she computes inductively $j_{A,B,j} = [P_{A,i}] \cdot j_{A,B,i-1}$. Bob does the same by setting $j_{B,A,0} = j_{A,9}$ and by computing $j_{B,A,j} = [P_{B,i}] \cdot j_{B,A,i-1}$. Finally, since $\mathrm{Pic}^0(\mathcal{H})$ is commutative, $j_{B,A,9} = j_{A,B,9}$ and both Alice and Bob can use this data as a shared secret key in L. It is reasonable to assume that the number of places of degree 35 on $\mathcal{H}$ is approximately equal to the number of irreducible polynomials of degree 35 in $\mathbb{F}_2$, which is $(2^{35} - 2)/35 \approx 2^{29.87}$.

The number of possible choices for 9 such places is $\approx (2^{29.87})^9/9! \approx 2^{250.36}$. By making the reasonable assumption that their sum in $\mathrm{Pic}^0(\mathcal{H})$ is well-distributed, we obtain that the key spaces for Alice and Bob (i.e. the sets of all possible values of $j_{A,9}$ and $j_{B,9}$) is a set whose cardinality approximately equals $2^{250.36}$.

We ran experiments on a laptop with an 8-core Intel i5-8365U@1.60GHz CPU, with 16 GB RAM. The most costly step in practice is the first step of Euclide's algorithm: it starts by computing τ^{521} modulo ϕ_u, which has τ-degree 70. Unfortunately, in our non-commutative setting we cannot use binary exponentiation to speed-up this step. Therefore, we implemented

a subroutine specialized for this task, which can be parallelized by precomputing the remainders of $\tau^{70}, \tau^{71}, \ldots, \tau^{70+\mathsf{NbCores}-1}$. By using the 8 cores of the laptop, computing the group action for a place of degree 35 takes 24 ms. Consequently, a full group action (using 9 places of degree 35) takes approximately 216 ms, and a full key-exchange requires two such group actions, which requires approximately 432 ms.

This seems fast enough for considering this non-interactive key exchange protocols as potential alternative to existing isogeny-based cryptosystems. We emphasize that our code is only a proof-of-concept prototype. On one hand, it is not optimized, and further work might lead to better performances. For instance, choosing a subset of well-suited places on the curve — instead of choosing them at random — may provide substancial speed-ups by allowing some precomputations. On the other hand, our implementation is not side-channel resistant and some required countermeasures to side-channel attacks might decrease the efficiency. Also, further investigation is required to fine-tune the parameters that would be suitable for potential cryptographic applications. We leave all of this for future work.

4.2 Hardness of the inverse problem

Given two Drinfeld modules $\phi, \psi \in \mathrm{Dr}_2(\mathbb{F}_q[X], L)_\xi$, we have seen in Section 3.2 how — having access to an Ore polynomial $\iota : \phi \to \psi$ defining an isogeny — we can compute an ideal $\mathfrak{a} \subset \mathbf{A}_{\mathcal{H}}$ such that $\mathfrak{a} \star_L \phi = \psi$. Consequently, inverting the group action reduces to the problem of computing an isogeny between two isogenous Drinfeld modules. There is a natural algorithm to search for such an isogeny, which has been investigated in [CGS20, Sec. 8] and [JN19, Sec. 5.1].

Let $\phi, \psi \in \mathrm{Dr}_2(\mathbb{F}_q[X], L)$ with $\phi_X = \Delta\tau^2 + g\tau + \omega$ and $\psi_X = \Delta'\tau^2 + g'\tau + \omega$. Let $\iota = \iota_a\tau^a + \cdots + \iota_0 \in L\{\tau\}$ be an Ore polynomial of τ-degree a. This Ore polynomial ι is an isogeny $\phi \to \psi$ if and only if $\iota\phi_X = \psi_X\iota$. By identifying all the coefficients in the equality $\iota\phi_X = \psi_X\iota$, we obtain the system

$$\begin{aligned} \Delta'\iota_a^{q^2} - \Delta^{q^a}\iota_a &= 0, \\ \Delta'\iota_{a-1}^{q^2} - \Delta^{q^{a-1}}\iota_{a-1} &= \iota_a g^{q^a} - g'\iota_a^q, \\ \forall k \in [\![2, a]\!], \quad \Delta'\iota_{a-k}^{q^2} - \Delta^{q^{a-k}}\iota_{a-k} &= \iota_{a-k+1}g^{q^{a-k+1}} - g'\iota_{a-k+1}^q + \iota_{a-k+2}(\omega^{q^{a-k+2}} - \omega), \end{aligned} \tag{4.1}$$

and

$$\iota_0 g + \iota_1\omega^q = \omega\iota_1 + g'\iota_0^q. \tag{4.2}$$

All isogenies $\phi \to \psi$ with prescribed τ-degree a may be found by recursively solving System (4.1) for $\iota_a, \iota_{a-1}, \ldots, \iota_1, \iota_0$ and then by checking that the values found for ι_0, ι_1 satisfy Equation (4.2). Indeed, we notice that the i-th equality depends only on the coefficient $\iota_a, \iota_{a-1}, \ldots, \iota_{a-i+1}$, and that ι_{a-i+1} is the root of a polynomial of $L[X]$ with degree q^2. Therefore, given values for $\iota_a, \iota_{a-1}, \ldots, \iota_{a-i+2}$, there are only at most q^2 candidate values for ι_{a-i+1} in L. In fact, we shall see (Lemma 4.2 below) that there is either 0 or q candidate values for ι_{a-i+1}. Therefore, we can search for an isogeny by exploring a tree where each node branches to either 0 or q possibilities. We will also see in Lemma 4.1 that this depends on the trace over $\mathbb{F}_q$ of some quantity constructed with $\iota_a, \iota_{a-1}, \ldots, \iota_{a-i+2}$.

An exponential upper bound for the complexity is proved in [CGS20, §8], and it is *a priori* the current fastest known isogeny-finding algorithm. Up to our knowledge, there is no lower bound on the complexity: our aim in this section is to give some experimental and conjectural evidence that in our setting this algorithm is truly exponential in the degree in the isogeny, and that this is not only an upper bound. We start by a technical lemma, which is directly related to the additive form of Hilbert's Theorem 90:

Lemma 4.1. *Assume $[L : \mathbb{F}_q]$ is odd. For $\delta \in L$, the polynomial $X^{q^2} - X - \delta$ has q roots in L if $\mathrm{Trace}_{L/\mathbb{F}_q}(\delta) = 0$, otherwise it has no root in L.*

Proof. Since $[L : \mathbb{F}_q]$ is odd, τ^2 generates $\mathrm{Gal}(L/\mathbb{F}_q)$ and the lemma is a direct consequence of the additive form of Hilbert's Theorem 90, see e.g. [Lee18, Th. 2]. □

Lemma 4.2. *Assume $[L : \mathbb{F}_q]$ is odd, and let $i \in [\![2, a+1]\!]$ and let $\iota_a, \iota_{a-1}, \ldots, \iota_{a-i+2} \in L$ be values which satisfy the $i-1$ first equalities in (4.1). Then there are either 0 or q values for ι_{a-i+1} in L which satisfy the i-th equality in (4.1).*

Proof. In this proof, we use the shorthand $d \coloneqq [L : \mathbb{F}_q]$. The first equality in (4.1) gives $\Delta' = \Delta^{q^a}/\iota_a^{q^2-1}$. Let $i \in [\![2, a+1]\!]$. Set $\nu \coloneqq \Delta^{q^{a-i+1}}/\Delta' = \iota_a^{q^2-1}/\Delta^{q^{a-i+1}(q^{i-1}-1)}$. As $q-1$ divides $q^{i-1}-1$ and q^2-1, there exists $b \in L$ such that $\nu = b^{q-1}$.

We separate two cases, depending on whether q is odd or not. On one hand, assume that q is odd. Then, notice that $\gcd(q+1, q^d-1) = 2$, so that $\gcd((q+1)/2, q^d-1)/2) = 1$. Let $\mu \in \mathbb{F}_q^\times$ be such that μb is a square in $L^\times$ and write $b = c^2$. Since $(q+1)/2$, $(q^d-1)/2$ are coprime and $|(L^\times)^2| = (q^d-1)/2$, the map $x \mapsto x^{\frac{q+1}{2}}$ is a group automorphism of $(L^\times)^2$. Hence, there exists $\lambda \in (L^\times)^2$ such that $c = \lambda^{\frac{q+1}{2}}$, and we get $\nu = \lambda^{q^2-1}$. On the other hand, if q is a power of two, then $q+1$ and q^d-1 are coprime. Therefore, the map defined on $L^\times$ by $x \mapsto x^{q+1}$ is a group automorphism, and there exists $\lambda \in L^\times$ such that $b = \lambda^{q+1}$.

In both cases, we have constructed $\lambda \in L$ such that $\nu = \lambda^{q^2-1}$. The values of ι_{a-i+1} which satisfy the i-th equality in (4.1) are the roots of a univariate polynomial $\Delta' X^{q^2} - \Delta^{q^{a-i+1}} X - m$, where m is some element of L. Writing $X = \lambda Y$, we obtain

$$\begin{aligned}
\Delta' X^{q^2} - \Delta^{q^{a-i+1}} X - m &= \Delta' \lambda^{q^2} Y^{q^2} - \Delta^{q^{a-i+1}} \lambda X - m \\
&= \lambda \left(\nu \Delta' Y^{q^2} + \Delta^{q^{a-i+1}} X - m\lambda^{-1} \right) \\
&= \lambda \Delta^{q^{a-i+1}} \left(Y^{q^2} - Y - m\lambda^{-1} \Delta^{-q^{a-i+1}} \right).
\end{aligned}$$

By Lemma 4.1, this polynomial has either 0 or q roots in L, which concludes the proof. □

We ran this algorithm for several Drinfeld modules that are isogenous via the group action. Those experiments suggest that the research tree built by the algorithm is always full when there exists an isogeny, i.e. in Lemma 4.2 there are always q values ι_{a-i+1} in L which satisfy the i-th equality in (4.1). We formalize this observation in the following conjecture:

Conjecture 4.3. *Let $\phi, \psi \in \mathrm{Dr}_2(\mathbb{F}_q[X], L)$ be isogenous Drinfeld modules. The search tree obtained by solving (4.1) iteratively for $\iota_a, \iota_{a-1}, \ldots, \iota_0$ is full: each polynomial equation encountered during this iterative process has exactly q solutions in L.*

If Conjecture 4.3 holds true, then the number of nodes in the tree is exponential in a. Moreover, experiments suggest that only a few paths in the tree lead to isogenies. This number of isogenies is a multiple of $q-1$, because elements of $\mathbb{F}_q^\times$ are automorphism of Drinfeld modules. In practice, we observed that in most cases, there were actually exactly $q-1$ such paths. As suggested in [CGS20, Sec. 8], we cannot know *a priori* which path in the tree will give rise to an actual isogeny. Therefore, the algorithm essentially boils down to a path-searching algorithm, with asymptotic complexity $\Theta(q^a)$.

References

[BK92] S. Bae and J. K. Koo. On the singular Drinfeld modules of rank 2. *Mathematische Zeitschrift*, 210(1):267–275, 1992.

[BKV19] W. Beullens, T. Kleinjung, and F. Vercauteren. CSI-FiSh: Efficient isogeny based signatures through class group computations. In *Asiacrypt 2019*, pages 227–247. Springer, 2019.

[Car18] P. Caranay. *Computing Isogeny Volcanoes of Rank Two Drinfeld Modules*. PhD thesis, University of Calgary, 2018.

[CFA+05] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren. *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. CRC, 2005.

[CGS20] P. Caranay, M. Greenberg, and R. Scheidler. Computing modular polynomials and isogenies of rank two Drinfeld modules over finite fields. *Contemporary Mathematics*, 754:293–314, 2020.

[CLM+18] W. Castryck, T. Lange, C. Martindale, L. Panny, and J. Renes. CSIDH: An efficient post-quantum commutative group action. In *Asiacrypt 2018*, pages 395–427. Springer, 2018.

[Cou06] J.-M. Couveignes. Hard homogeneous spaces. Cryptology ePrint Archive, Report 2006/291, `https://ia.cr/2006/291`, 2006.

[CST14] W. Castryck, M. Streng, and D. Testa. Curves in characteristic 2 with non-trivial 2-torsion. *Advances in Mathematics of Communications (AMC)*, 8(4):479–495, 2014.

[DFKS18] L. De Feo, J. Kieffer, and B. Smith. Towards practical key exchange from ordinary isogeny graphs. In *Asiacrypt 2018*, pages 365–394. Springer, 2018.

[DH87] P. Deligne and D. Husemoller. Survey of Drinfel'd modules. *Contemporary mathematics*, 67:25–91, 1987.

[Dri74] V. G. Drinfel'd. Elliptic modules. *Mathematics of the USSR-Sbornik*, 23(4):561–592, 1974.

[DV06] J. Denef and F. Vercauteren. An extension of Kedlaya's algorithm to hyperelliptic curves in characteristic 2. *Journal of cryptology*, 19(1):1–25, 2006.

[Gek83] E.-U. Gekeler. Zur arithmetik von Drinfeld-moduln. *Mathematische Annalen*, 262(2):167–182, 1983.

[Gek91] E.-U. Gekeler. On finite Drinfeld modules. *Journal of algebra*, 1(141):187–203, 1991.

[Gos98] D. Goss. *Basic Structures of Function Field Arithmetic*. Springer, 1998.

[Hay91] D. R. Hayes. A brief introduction to Drinfeld modules. In *The Arithmetic of Function Fields: Proceedings of the Workshop at the Ohio State University, June 17-26, 1991*, pages 1–32. De Gruyter, 1991.

[JN19] A. Joux and A. K. Narayanan. Drinfeld modules may not be for isogeny based cryptography. Cryptology ePrint Archive, `https://ia.cr/2019/1329`, 2019.

[Ked01] K. S. Kedlaya. Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology. *Journal of the Ramanujan Mathematical Society*, 16:323–338, 2001.

[Kup05] G. Kuperberg. A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. *SIAM Journal on Computing*, 35(1):170–188, 2005.

[Lan87] S. Lang. *Elliptic functions*. Springer, 1987.

[Lan02] S. Lang. *Algebra*. Springer, 3rd edition, 2002.

[Lee18] S. Lee. Hilbert's theorem 90. `https://math.berkeley.edu/~seewoo5/h90.pdf`, 2018.

[Lor96] D. Lorenzini. *An Invitation to Arithmetic Geometry*. American Mathematical Society, 1996.

[MS19] Y. Musleh and É. Schost. Computing the characteristic polynomial of a finite rank two Drinfeld module. In *Proceedings of ISSAC 2019*, pages 307–314. ACM, 2019.

[Ros02] M. Rosen. *Number Theory in Function Fields*. Springer, 2002.

[RS06] A. Rostovtsev and A. Stolbunov. Public-key cryptosystem based on isogenies. Cryptology ePrint Archive, `https://ia.cr/2006/145`, 2006.

[Sil94] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves*. Springer, 1994.