Drinfeld modules are not for isogeny based cryptography*

Antoine Joux and Anand Kumar Narayanan

Sorbonne Université, Institut de Mathématiques de Jussieu–Paris Rive Gauche, CNRS, INRIA, Univ Paris Diderot, Campus Pierre et Marie Curie, F-75005 Paris, France.
antoine.joux@m4x.org,anand.narayanan@lip6.fr

Abstract. Elliptic curves play a prominent role in cryptography. For instance, the hardness of the elliptic curve discrete logarithm problem is a foundational assumption in public key cryptography. Drinfeld modules are positive characteristic function field analogues of elliptic curves. It is natural to ponder the existence/security of Drinfeld module analogues of elliptic curve cryptosystems. But the Drinfeld module discrete logarithm problem is easy even on a classical computer. Beyond discrete logarithms, elliptic curve isogeny based cryptosystems have have emerged as candidates for post-quantum cryptography, including supersingular isogeny Diffie-Hellman (SIDH) and commutative supersingular isogeny Diffie-Hellman (CSIDH) protocols. We formulate Drinfeld module analogues of these elliptic curve isogeny based cryptosystems and devise classical polynomial time algorithms to break these Drinfeld analogues catastrophically.

1 Introduction

Elliptic curve cryptosystems reliant on the hardness of the elliptic curve discrete logarithm problem (ECDLP) are cornerstones of public key cryptography. However Shor's algorithm makes ECDLP easy on a quantum computer [29]. As candidates for post-quantum cryptography, several cryptosystems reliant on the hardness of computing a large degree isogeny between two given elliptic curves have emerged.

The first such systems were proposed by Couveignes [7] and rediscovered by Rostovtsev-Stolbunov [27]. Their setting is a set of isogenous ordinary elliptic curves over a large finite field. Ideal class groups of certain orders in imaginary quadratic extensions act freely and transitively on this set. The underlying hard problem is identifying the class group element mapping one given curve to another. Charles, Lauter and Goren [4] constructed hash functions based on the hardness of computing isogenies. A novelty in their construction is the reliance on supersingular elliptic curves; renowned for their isogeny graphs being Ramanujan [25]. DeFeo, Jao and Plût devised a public key cryptosystem based on the hardness of computing an isogeny between two supersingular elliptic curves. Unlike the ordinary case, isogenies between supersingular elliptic curves do not necessarily commute. The Diffie-Hellman [10] formalism for key-exchange therefore does not apply. To overcome this non-commutativity obstruction and facilitate key exchange, De Feo, Jao and Plût resort to requiring that the entities involved publish the images of certain points under their secret isogenies. Their scheme is named supersingular isogeny Diffie-Hellman (SIDH) to reflect this. Recently, Castryck, Lange, Martindale, Panny and Renes [3] designed a Diffie-Hellman style key exchange based

* Supported by the European Unions H2020 Programme (grant agreement #ERC-669891).

on supersingular elliptic curves. They accomplish this by restricting to isogenies defined over the field of definition of the curves; which ensures the isogenies commute. Their scheme is named commutative supersingular isogeny Diffie-Hellman (CSIDH). The aforementioned class group action reappears in this context and the underlying hardness is now closely related to those of Couveignes and Rostovtsev-Stolbunov, coming full circle.

A distinction between SIDH and CSIDH/Couveignes-Rostovtsev-Stolbunov is that quantum sub-exponential algorithms are known to break the later. The reason being that their underlying hard problem can be phrased as a hidden shift problem amenable to Kuperberg's and Regev's algorithms [18,26,2,5]. There are no known quantum subexponential algorithms to break SIDH. Yet, the publication of images of points under the secret isogenies in SIDH is ominous. In CSIDH/Couveignes-Rostovtsev-Stolbunov, the public key is just an elliptic curve, no points are published. A thorough comparative study of these frameworks in the post-quantum setting is thus warranted.

Drinfeld introduced the modules bearing his name as analogues of elliptic curve complex multiplication theory [11,12]. To emphasize this connection, he called them elliptic modules and proved function field analogues of the Kronecker-Weber theorem, the main conjecture of Iwasawa theory and the Langlands conjecture for GL_2 (over a global field of positive characteristic). Drinfeld modules and their generalisations continue to play a crucial role in the arithmetic of function fields and in proving global Langlands conjecture over function fields for GL_n. We settle for a concrete simple notion of Drinfeld modules sufficient for our context.

It is natural to ponder if Drinfeld module arithmetic can be cast in place of elliptic curves in cryptography. Scanlon foresaw the folly and showed that the Drinfeld module versions of the elliptic curve discrete logarithm problem are easy, even on a classical computer [28]. Our paper is a tale of caution too. We meticulously formulate Drinfeld module analogues of the aforementioned elliptic curve isogeny schemes and catastrophically break them on a classical computer. En route to designing the cryptosystems, we devise certain algorithms that may be of independent interest in Drinfeld module arithmetic. For instance, we present algorithms for constructing supersingular Drinfeld modules over finite fields with prescribed order (Euler-Poincaré characteristic).

We focus primarily on Drinfeld module analogues of CSIDH and SIDH. In describing the cryptosystems, we restrict to non interactive key exchange protocols. It is straightforward to extend it to a public key encryption scheme etc. On the cryptanalysis front, the principle reason for vulnerability is that large degree Drinfeld module isogenies have a natural succinct representation as elements in a polynomial ring twisted by the Frobenius endomorphism. Contrast this with the elliptic curve scenario where large degree isogenies are not known to admit succinct representations, unless their factorization into a composition of small degree isogenies is known. Aside from the succinct representation, the algorithms for breaking Drinfeld analogues of CSIDH and SIDH are vastly different. The Drinfeld module SIDH scheme is broken by exploiting the published images of points under the secret isogenies. These images allow for the succinct representation of the secret isogenies to be interpolated. The Drinfeld module CSIDH system is broken by looking directly at the defining commutation relation of isogenies. The coefficients of the succinct representations of the secret isogenies are iteratively inferred from the commutation relation. The fact that the isogenies are over the defining field of the Drinfeld modules (and not over an extension) is critical to our Drinfeld CSIDH

breaking algorithm. In fact, this algorithm can be adapted in a straightforward manner to break Drinfeld module versions of Couveignes-Rostovtsev-Stolbunov cryptosystems.

The paper is organized as follows. In § 2, we introduce Drinfeld modules and build notation. Our exposition is largely self contained and targeted at a typical reader well versed with elliptic curve cryptography, but unfamiliar with Drinfeld modules. The following section § 3 is devoted to developing the main objects for our constructions; supersingular Drinfeld modules and isogenies connecting them. The Drinfeld module analogues of CSIDH and SIDH are devised in § 4 and broken in § 5.

2 Introduction to Drinfeld Modules

This section is a gentle introduction to Drinfeld modules with an eye towards computation. We constantly draw on analogies between number fields and function fields; in particular between integers and polynomials over finite fields and between elliptic curves and rank-2 Drinfeld modules. Alongside Drinfeld original paper [11], Gekeler's papers [14,15] serve as excellent quick references for the material in the current and following section.

2.1 Rank-2 Drinfeld modules

We begin by introducing rank-2 Drinfeld modules over rational function fields and over finite fields. They are respectively analogous to elliptic curves over the rational numbers and over finite fields. Let $\mathbb{F}_q$ denote the finite field with q elements and assume throughout that q is odd. Let $\mathbb{F}_q[x]$ denote the polynomial ring in the indeterminate x and let $\mathbb{F}_q(x)$ be its field of fractions. Let K be a field with a non zero ring homomorphism $\gamma : \mathbb{F}_q[x] \to K$. Necessarily, K contains $\mathbb{F}_q$ as a subfield. Let $\tau : K \longrightarrow K$ denote the q^{th} power Frobenius endomorphism. The ring of endomorphisms of the additive group scheme $\mathbb{G}_a$ over K can be identified with the skew polynomial ring $K\langle\tau\rangle$ where τ satisfies the commutation rule

$$\tau u = u^q \tau, \ \forall u \in K.$$

A rank-2 Drinfeld module $\phi\,/K$ over K is (the $\mathbb{F}_q[x]$-module structure on $\mathbb{G}_a$ given by) a ring homomorphism

$$\begin{aligned} \phi : \mathbb{F}_q[x] &\longrightarrow K\langle\tau\rangle \\ x &\longmapsto \gamma(x) + \mathfrak{g}_\phi(x)\tau + \Delta_\phi(x)\tau^2 \end{aligned}$$

for some $\mathfrak{g}_\phi(x) \in K$ and $\Delta_\phi(x) \in K^\times$. Such a ring homomorphism fixes $\mathbb{F}_q$ and is completely determined by the image of x. By design, a polynomial $\mathfrak{f}(x)$ maps to a polynomial in τ with constant term $\gamma(\mathfrak{f}(x))$,

$$\mathfrak{f}(x) \longmapsto \underbrace{\gamma(\mathfrak{f}(x)) + \sum_{i=1}^{2\deg(\mathfrak{f})} \mathfrak{f}_{\phi,i}\tau^i}_{Call\ \phi_\mathfrak{f}}$$

for some $\mathfrak{f}_{\phi,i} \in K$. It is convenient to use subscripts to denote images, that is, call $\phi_\mathfrak{f}$ the image of $\mathfrak{f}(x)$ under ϕ. Here on, we are primarily concerned with rank-2 Drinfeld modules and unless otherwise noted, a Drinfeld module will mean a rank-2 Drinfeld module. When explicitly describing a Drineld module, we will at times write $\phi = (\mathfrak{g}_\phi, \Delta_\phi)$. When the field of definition K is clear from context, we write ϕ instead of $\phi\,/K$.

Drinfeld modules over rational function fields: To obtain Drinfeld modules over the rational function field $\mathbb{F}_q(x)$, take K to be $\mathbb{F}_q(x)$ and set γ to be the inclusion $\gamma : \mathbb{F}_q[x] \hookrightarrow \mathbb{F}_q(x)$. A Drinfeld module $\phi\,/\mathbb{F}_q(x)$ over $\mathbb{F}_q(x)$ then takes the form

$$\begin{aligned}\phi : \mathbb{F}_q[x] &\longrightarrow \mathbb{F}_q(x)\langle\tau\rangle \\ x &\longmapsto x + \mathfrak{g}_\phi(x)\tau + \Delta_\phi(x)\tau^2\end{aligned}$$

for some $\mathfrak{g}_\phi(x) \in \mathbb{F}_q(x)$ and $\Delta_\phi(x) \in \mathbb{F}_q(x)^\times$. To better perceive the homomorphism, it is instructive to compute by hand the images of x^2, x^3 etc. employing the commutation rule in $\mathbb{F}_q(x)\langle\tau\rangle$.

Drinfeld modules over finite fields: For a monic irreducible $\mathfrak{p}(x) \in \mathbb{F}_q[x]$ of degree $\deg(\mathfrak{p}) > 0$, denote

$$\mathbb{F}_\mathfrak{p} := \mathbb{F}_q[x]/(\mathfrak{p}(x)) \cong \mathbb{F}_{q^{\deg(\mathfrak{p})}}.$$

Drinfeld modules defined over finite fields $\mathbb{F}_\mathfrak{p}$ will feature prominently in our constructions. To realize them, take $K = \mathbb{F}_\mathfrak{p}$ and set $\gamma : \mathbb{F}_\mathfrak{q}[x] \to \mathbb{F}_\mathfrak{p}$ to be the reduction modulo $\mathfrak{p}$ map. A Drinfeld module $\phi\,/\mathbb{F}_\mathfrak{p}$ over $\mathbb{F}_\mathfrak{p}$ takes the form

$$\begin{aligned}\phi : \mathbb{F}_q[x] &\longrightarrow \mathbb{F}_\mathfrak{p}\langle\tau\rangle \\ x &\longmapsto (x \mod \mathfrak{p}) + \mathfrak{g}_\phi\tau + \Delta_\phi\tau^2\end{aligned}$$

for some $\mathfrak{g}_\phi \in \mathbb{F}_\mathfrak{p}$ and $\Delta_\phi \in \mathbb{F}_\mathfrak{p}^\times$. Fix an algebraic closure $\overline{\mathbb{F}}_\mathfrak{p}$ of $\mathbb{F}_\mathfrak{p}$ and let $\mathbb{F}_{\mathfrak{p}^2}$ denote the unique quadratic extension of $\mathbb{F}_\mathfrak{p}$ in $\overline{\mathbb{F}}_\mathfrak{p}$. We will also frequently encounter Drinfeld modules over $\mathbb{F}_{\mathfrak{p}^2}$, defined by taking $K = \mathbb{F}_{\mathfrak{p}^2}$.

2.2 Endowing new $\mathbb{F}_q[x]$-module structure:

In the arithmetic of elliptic curves, abelian groups (that is, $\mathbb{Z}$-modules) are recurring objects, for instance as the group of rational points or the group of m torsion points for some number m. In Drinfeld module arithmetic, $\mathbb{F}_q[x]$-modules will take the role of the analogous recurring object.

Consider an $\mathbb{F}_q[x]$-algebra M (say defined over an algebraic closure of K). One way to make the $\mathbb{F}_q[x]$-algebra M into an $\mathbb{F}_q[x]$-module is to retain the addition and scalar multiplication but simply forget the multiplication. A Drinfeld module $\phi\,/K$ endows a new $\mathbb{F}_q[x]$-module structure to M by twisting the scalar multiplication. For $\mathfrak{f}(x) \in \mathbb{F}_q[x]$ and $\alpha \in M$, define the scalar multiplication $\mathfrak{f}(x) \circ \alpha := \phi_\mathfrak{f}(\alpha)$. Let $\phi(M)$ denote the new $\mathbb{F}_q[x]$ module structure thus endowed to M.

Of particular interest is the module $\phi(\mathbb{F}_\mathfrak{p})$ endowed by a Drinfeld module $\phi\,/\mathbb{F}_\mathfrak{p}$ on the $\mathbb{F}_q[x]$-algebra $\mathbb{F}_\mathfrak{p}$. This $\mathbb{F}_q[x]$-module $\phi(\mathbb{F}_\mathfrak{p})$ will play the role of the abelian group $E(\mathbb{F}_p)$ of $\mathbb{F}_p$-rational points of an elliptic curve $E/\mathbb{F}_p$ over a finite field with p elements. In this case, the twisted scalar multiplication is; for $\mathfrak{f}(x) \in \mathbb{F}_q[x]$ and $\alpha \in \mathbb{F}_\mathfrak{p}$,

$$\mathfrak{f}(x) \circ \alpha := \phi_\mathfrak{f}(\alpha) = (\mathfrak{f}(x) \mod \mathfrak{p})\ \alpha + \sum_{i=1}^{2\deg(\mathfrak{f})} \mathfrak{f}_{\phi,i}\alpha^{q^i}$$

where the arithmetic on the right is performed in $\mathbb{F}_\mathfrak{p}$. This new $\mathbb{F}_q[x]$-module structure is richer than merely forgetting the multiplication, as evident by the extra summation term on the right.

2.3 Morphisms of Drinfeld Module

Let ϕ/K and ψ/K be two Drinfeld modules over a field K as before. For a field extension L/K, an L-morphism $\iota : \phi/K \longrightarrow \psi/K$ defined over the extension L is an $\iota \in L\langle\tau\rangle$ such that

$$\iota\ \phi_{\mathfrak{f}} = \psi_{\mathfrak{f}}\ \iota, \quad \forall \mathfrak{f} \in \mathbb{F}_q[x].$$

Since $\mathbb{F}_q$ commutes with τ, it is sufficient to check $\iota\ \phi_x = \psi_x\ \iota$. Thus ι defines a morphism of group schemes over K that commutes with the $\mathbb{F}_q[x]$-action.

Isogenies: An L-isogeny is a non-zero L-morphism. An L-isogeny from ϕ/K to itself is an L-endomorphism. The L-endomorphism ring denoted by $End_L(\phi)$ consists of L-isogenies from ϕ/K to ϕ/K and the zero endomorphism.

$\mathbb{F}_{\mathfrak{p}}$-endomorphisms: For first examples of isogenies, we look to the endomorphism ring $End_{\mathbb{F}_{\mathfrak{p}}}(\phi)$ of a Drinfeld module $\phi/\mathbb{F}_{\mathfrak{p}}$. Pick a monic non zero $\mathfrak{b}(x) \in \mathbb{F}_q[x]$ and consider $\phi_{\mathfrak{b}} \in \mathbb{F}_{\mathfrak{p}}\langle\tau\rangle$. This yields the isogeny $\phi_{\mathfrak{b}} : \phi/\mathbb{F}_{\mathfrak{p}} \longrightarrow \phi/\mathbb{F}_{\mathfrak{p}}$ as evident from $\phi_{\mathfrak{b}}\phi_{\mathfrak{f}} = \phi_{\mathfrak{b}\mathfrak{f}} = \phi_{\mathfrak{f}\mathfrak{b}} = \phi_{\mathfrak{f}}\phi_{\mathfrak{b}}, \forall \mathfrak{f} \in \mathbb{F}_q[x]$. Hence we have the inclusion $\mathbb{F}_q[x] \hookrightarrow End_{\mathbb{F}_{\mathfrak{p}}}(\phi)$. But $End_{\mathbb{F}_{\mathfrak{p}}}(\phi)$ is strictly larger than $\mathbb{F}_q[x]$, for it contains the Frobenius element $\tau^{\deg(\mathfrak{p})}$. Since the defining coefficients $\mathfrak{g}_\phi$ and Δ_ϕ are in $\mathbb{F}_{\mathfrak{p}}$, $\phi_{\mathfrak{f}}$ commutes with the Frobenius element $\tau^{\deg(\mathfrak{p})}$ for every $\mathfrak{f}(x) \in \mathbb{F}_q[x]$. Hence we have the inclusion $\mathbb{F}_q[x][\tau^{\deg(\mathfrak{p})}] \hookrightarrow End_{\mathbb{F}_{\mathfrak{p}}}(\phi)$.

$\overline{\mathbb{F}}_{\mathfrak{p}}$-endomorphisms: For a Drinfeld module ϕ defined over a finite extension of $\mathbb{F}_{\mathfrak{p}}$, the endomorphism ring $End_{\overline{\mathbb{F}}_{\mathfrak{p}}}(\phi)$ over the algebraic closure $\overline{\mathbb{F}}_{\mathfrak{p}}$ is a free $\mathbb{F}_q[x]$-module of rank either 2 or 4. When the rank is 2, ϕ is called *ordinary* and $End_{\overline{\mathbb{F}}_{\mathfrak{p}}}(\phi)$ is an order in an imaginary quadratic extension of $\mathbb{F}_q(x)$. An imaginary quadratic extension is one where the place at infinity in $\mathbb{F}_q(x)$ is not split. When the rank is 4, ϕ is called *supersingular* and $End_{\overline{\mathbb{F}}_{\mathfrak{p}}}(\phi)$ is a maximal order in the unique quaternion algebra over $\mathbb{F}_q(x)$ ramifying precisely at $\mathfrak{p}$ and the place at infinity.

Isomorphisms and Automorphisms: The absolute j-invariant of a Drinfeld module $\phi = (\mathfrak{g}_\phi, \Delta_\phi)$ over a finite extension of $\mathbb{F}_{\mathfrak{p}}$ is defined as

$$j(\phi) := \mathfrak{g}_\phi^{q+1}/\Delta_\phi.$$

Drinfeld modules ϕ and ψ over a finite extension of $\mathbb{F}_{\mathfrak{p}}$ are $\overline{\mathbb{F}}_{\mathfrak{p}}$-isomorphic if and only if $j(\phi) = j(\psi)$. Drinfeld modules $\phi/\mathbb{F}_{\mathfrak{p}} = (\mathfrak{g}_\phi, \Delta_\phi)$ and $\psi/\mathbb{F}_{\mathfrak{p}} = (\mathfrak{g}_\psi, \Delta_\psi)$ are $\mathbb{F}_{\mathfrak{p}}$-isomorphic if and only if there exists a non zero $c \in \mathbb{F}_{\mathfrak{p}}$ such that $\mathfrak{g}_\psi = c^{q-1}\mathfrak{g}_\phi$ and $\Delta_\psi = c^{q^2-1}\Delta_\phi$. This condition is equivalent to

- $j(\phi) = j(\psi)$ and
- if $\mathfrak{g}_\psi \neq 0$ then $\mathfrak{g}_\phi/\mathfrak{g}_\psi \in \mathbb{F}_{\mathfrak{p}}^{q-1}$; else, $\Delta_\phi/\Delta_\psi \in \mathbb{F}_{\mathfrak{p}}^{q^2-1}$.

The number of Drinfeld modules $\phi/\mathbb{F}_{\mathfrak{p}} = (\mathfrak{g}_\phi, \Delta_\phi)$ over $\mathbb{F}_{\mathfrak{p}}$ is $q^{\deg(\mathfrak{p})}\left(q^{\deg(\mathfrak{p})} - 1\right)$ since $\mathfrak{g}_\phi \in \mathbb{F}_{\mathfrak{p}}$ and $\Delta_\phi \in \mathbb{F}_{\mathfrak{p}}^{\times}$. The number of $\mathbb{F}_{\mathfrak{p}}$-isomorphism classes is

$$\left(q^{\deg(\mathfrak{p})} - 1\right)(q-1) + \left|\mathbb{F}_{\mathfrak{p}}^{\times}/\mathbb{F}_{\mathfrak{p}}^{\times(q^2-1)}\right|$$

where $\left|\mathbb{F}_{\mathfrak{p}}^{\times}/\mathbb{F}_{\mathfrak{p}}^{\times(q^2-1)}\right|$ evaluates to q^2-1 if $\deg(\mathfrak{p})$ is odd and $q-1$ else. The count has a cleaner form when the isomorphism classes are inversely weighted with the size of the automorphism group $Aut_{\mathbb{F}_{\mathfrak{p}}}(\phi) \cong \mathbb{F}_{\mathfrak{p}}^{\times}$,

$$\sum_{\phi/\mathbb{F}_{\mathfrak{p}}} \frac{1}{|Aut_{\mathbb{F}_{\mathfrak{p}}}(\phi)|} = |\mathbb{F}_{\mathfrak{p}}| = q^{\deg \mathfrak{p}},$$

where the summation is over $\mathbb{F}_{\mathfrak{p}}$-isomorphism classes. This is analogous to the weighted count for elliptic curves $E/\mathbb{F}_p$ modulo a prime p over isomorphism classes

$$\sum_{E/\mathbb{F}_p} \frac{1}{|Aut_{\mathbb{F}_p}(E)|} = |\mathbb{F}_p| = p.$$

2.4 Characteristic Polynomial of Frobenius

Let ϕ be a Drinfeld module over a finite extension K of $\mathbb{F}_{\mathfrak{p}}$. From the structure of $End_{\mathbb{F}_{\mathfrak{p}}}(\phi)$, the Frobenius element $\tau^{\deg \mathfrak{p}}$ satisfies a polynomial equation over $\mathbb{F}_q[x]$. Denote its minimal polynomial by $M_\phi(X) \in \mathbb{F}_q[X]$. Gekeler [14] showed that the characteristic polynomial $P_\phi(X) \in \mathbb{F}_q[X]$ of the Frobenius element $\tau^{\deg \mathfrak{p}}$ (in the representations of $End_{\mathbb{F}_{\mathfrak{p}}}(\phi)$ at the ℓ-adic Tate modules c.f [13]) is of the form

$$P_\phi(X) = X^2 - Tr_\phi(x)X + \epsilon_\phi \mathfrak{p}(x)$$

where $\epsilon_\phi := (-1)^{\deg(\mathfrak{p})}/Norm_{K/\mathbb{F}_q}(\Delta_\phi) \in \mathbb{F}_q^{\times}$ is the sign of the norm of the Frobenius and $Tr_\phi(x) \in \mathbb{F}_q[x]$ is the trace of the Frobenius. Further, P_ϕ equals M_ϕ implying

$$P_\phi(\tau^{\deg \mathfrak{p}}) = \tau^{2\deg \mathfrak{p}} - Tr_\phi(x)\tau^{\deg \mathfrak{p}} + \epsilon_\phi \mathfrak{p}(x) = 0.$$

Isogenies and Characteristic Polynomials: Two Drinfeld modules $\phi/\mathbb{F}_{\mathfrak{p}}$ and $\psi/\mathbb{F}_{\mathfrak{p}}$ are $\mathbb{F}_{\mathfrak{p}}$-isogenous if there is an $\mathbb{F}_{\mathfrak{p}}$-isogeny $\iota : \phi/\mathbb{F}_{\mathfrak{p}} \longrightarrow \psi/\mathbb{F}_{\mathfrak{p}}$. Although not apparent, being $\mathbb{F}_{\mathfrak{p}}$-isogenous is an equivalence relation for there is a corresponding dual isogeny $\widehat{\iota} : \psi/\mathbb{F}_{\mathfrak{p}} \longrightarrow \phi/\mathbb{F}_{\mathfrak{p}}$. Two Drinfeld modules are $\mathbb{F}_{\mathfrak{p}}$-isogenous if and only if they have the same characteristic polynomial. This is analogous to the theorem of Tate that two elliptic curves over a finite field are isogenous if and only if they have the same characteristic polynomial.

Euler-Poincaré Characteristic: The group of $\mathbb{F}_p$-rational points on an elliptic curve $E/F_{\mathfrak{p}}$ has cardinality constrained by the Hasse bound. To discuss Drinfeld module analogues, we first require a cardinality measure for finite $\mathbb{F}_q[x]$-modules. Cardinality is an integer valued measure of the size of a finite abelian group (equivalently, a finite $\mathbb{Z}$-module). A convoluted definition is to assign as the cardinality of a cyclic group of prime order the corresponding prime: and for cardinality of finite abelian groups that sit in an exact sequence to be multiplicative. The Euler-Poincaré characteristic χ is an $\mathbb{F}_q[x]$-valued cardinality measure of a finite $\mathbb{F}_q[x]$ module defined completely analogously. For a finite $\mathbb{F}_q[x]$-module A, $\chi(A) \in \mathbb{F}_q[x]$ is the monic polynomial s.t.

- If $A \cong \mathbb{F}_q[x]/(\mathfrak{s}(x))$ for a monic irreducible $\mathfrak{p}(x)$, then $\chi(A) = \mathfrak{s}(x)$.
- If $0 \to A_1 \to A \to A_2 \to 0$ is exact, then $\chi(A) = \chi(A_1)\chi(A_2)$.

For the $\mathbb{F}_q[x]$-module $\phi(\mathbb{F}_{\mathfrak{p}})$, the Euler-Poincaré characteristic $\chi(\phi(\mathbb{F}_{\mathfrak{p}}))$ has a simple linear algebraic interpretation: the characteristic polynomial of the $\mathbb{F}_q$-linear map ϕ_x on $\mathbb{F}_{\mathfrak{p}}$. In particular, it is a degree $\deg \mathfrak{p}$ polynomial in $\mathbb{F}_q[x]$.

Riemann Hypothesis: For an elliptic curve $E/\mathbb{F}_p$, the p^{th} power frobenius element satisfies the characteristic polynomial

$$X^2 - Tr_E X + p$$

where $Tr_E \in \mathbb{Z}$ is the trace of the p^{th}-power Frobenius. The $\mathbb{F}_p$-rational points $E(\mathbb{F}_p)$ famously form a finite abelian group with cardinality $p+1$ up to an error determined by the Frobenius trace Tr_E. The Hasse bound, considered the Riemann hypothesis for elliptic curves over finite fields asserts

$$|Tr_E| \leq 2\sqrt{p} \Rightarrow |E(\mathbb{F}_p)| = p + 1 - \underbrace{Tr_E}_{-2\sqrt{p} \leq \ \leq 2\sqrt{p}}.$$

Gekeler [15] established the Drinfeld module analogue of the Hasse bound for $\phi\,/\mathbb{F}_{\mathfrak{p}}$;

$$\deg\left(Tr_\phi(x)\right) \leq \deg(\mathfrak{p})/2.$$

Consequently, the Euler-Poincaré characteristic of the $\mathbb{F}_q[x]$-module $\phi(\mathbb{F}_{\mathfrak{p}})$ is

$$\chi\left(\phi\left(\mathbb{F}_{\mathfrak{p}}\right)\right) = \epsilon_\phi \mathfrak{p}(x) + 1 - \underbrace{Tr_\phi(x)}_{\leq \deg(\mathfrak{p})/2}.$$

The analogy with the Hasse bound is striking. To describe the error in each case takes (roughly) at most half the number of bits as the estimate.

3 Supersingular Drinfeld Modules

Recall that a Drinfeld module $\phi\,/\mathbb{F}_{\mathfrak{p}}$ over $\mathbb{F}_{\mathfrak{p}}$ is *supersingular* if $End_{\overline{\mathbb{F}}_{\mathfrak{p}}}(\phi)$ is a maximal order in the unique quaternion algebra over $\mathbb{F}_q(x)$ ramifying precisely at $\mathfrak{p}$ and the place at infinity. We will be concerned with a more general notion of supersingularity. Namely, Drinfeld modules $\phi\,/L$ defined over a finite extension L of $\mathbb{F}_{\mathfrak{p}}$ such that $End_{\overline{\mathbb{F}}_{\mathfrak{p}}}(\phi)$ is not commutative. We call these supersingular Drinfeld module of characteristic $\mathfrak{p}$. There are only finitely many $\overline{\mathbb{F}}_{\mathfrak{p}}$-isomorphism classes of Drinfeld modules of characteristic $\mathfrak{p}$. In fact, every Drinfeld module of characteristic $\mathfrak{p}$ is in fact defined either over $\mathbb{F}_{\mathfrak{p}}$ or $\mathbb{F}_{\mathfrak{p}^2}$ (upto $\overline{\mathbb{F}}_{\mathfrak{p}}$-isomorphism) [14][Prop. 4.2]. Hence with the unique quadratic extension$\mathbb{F}_{\mathfrak{p}^2}$ of $\mathbb{F}_{\mathfrak{p}}$ as the field of definition, we can account for all the supersingular Drinfeld modules of relevance to our constructions.

Hasse Invariant: An alternate characterization of supersingularity is given by the Hasse invariant. The Hasse invariant $h_\phi \in \mathbb{F}_{\mathfrak{p}}$ of $\phi\,/\mathbb{F}_{\mathfrak{p}^2}$ is the coefficient of $\tau^{\deg(\mathfrak{p})}$ in the expansion

$$\phi_{\mathfrak{p}} = \sum_{i=0}^{2\deg(\mathfrak{p})} h_i \tau^i \in \mathbb{F}_{\mathfrak{p}^2}\langle\tau\rangle.$$

A Drinfeld module $\phi\,/\mathbb{F}_{\mathfrak{p}^2}$ is supersingular if and only if $h_\phi = 0$ [13]. In fact, for supersingular $\phi\,/\mathbb{F}_{\mathfrak{p}^2}$ [14][Prop. 4.1],

$$\phi_{\mathfrak{p}} = Norm_{\mathbb{F}_{\mathfrak{p}^2}/\mathbb{F}_q}(\Delta_\phi)\tau^{2\deg(\mathfrak{p})}. \tag{1}$$

Remark 1. The constant coefficient $Norm_{\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_q}(\Delta_\phi)$ is a notational inconvenience to our constructions. Thankfully, there is always an $\overline{\mathbb{F}}_{\mathfrak{p}}$-isomorphic Drinfeld module defined over $\mathbb{F}_{\mathfrak{p}^2}$ with $Norm_{\mathbb{F}_{\mathfrak{p}^2}/\mathbb{F}_q}(\Delta_\phi) = 1$ (see for instance the proof of Prop. 4.1 in [14]). Consequently, while working with $\mathbb{F}_{\mathfrak{p}^2}$ as the field of definition, without loss of generality, we may assume $\epsilon_\phi = 1$.

Trace of Frobenius: Yet another characterization of a supersingular Drinfeld module of characteristic $\mathfrak{p}$ is that the trace of the Frobenius $\tau^{\deg(\mathfrak{p})}$ vanishes.

3.1 Torsion Submodules

For a monic $\mathfrak{m}(x) \in \mathbb{F}_q[x]$ with $\deg(\mathfrak{m}) \geq 1$, the $\mathfrak{m}$-torsion points (that is, the kernel of the isogeny $\phi_{\mathfrak{m}}$) of a Drinfeld module ϕ (defined over $\mathbb{F}_{\mathfrak{p}}$ or $\mathbb{F}_{\mathfrak{p}^2}$)

$$\Lambda_\phi[\mathfrak{m}] := \left\{\alpha \in \overline{\mathbb{F}}_{\mathfrak{p}} \mid \phi_{\mathfrak{m}}(\alpha) = 0\right\}$$

form an $\mathbb{F}_q[x]$-module with the structure

$$\Lambda_\phi[\mathfrak{m}] \cong \mathbb{F}_q[x] \,/(\mathfrak{m}(x)) \oplus \mathbb{F}_q[x] \,/(\mathfrak{m}(x)) \,.$$

Lemma 1. *Let ϕ be a supersingular Drinfeld module defined over $\mathbb{F}_{\mathfrak{p}}$ or $\mathbb{F}_{\mathfrak{p}^2}$. If $\mathfrak{m}(x) \in \mathbb{F}_q[x]$ divides the Euler-Poincaré characteristic $\chi(\phi(\mathbb{F}_{\mathfrak{p}}))$, then $\Lambda_\phi[\mathfrak{m}] \subseteq \mathbb{F}_{\mathfrak{p}^2}$ and there exists $\lambda_1 \in \phi(\mathbb{F}_{\mathfrak{p}})$ and $\lambda_{-1} \in \phi(\mathbb{F}_{\mathfrak{p}^2})$ such that as $\mathbb{F}_q[x]$-modules*

$$\Lambda_\phi[\mathfrak{m}] = \langle\lambda_1\rangle \oplus \langle\lambda_{-1}\rangle.$$

Proof. Since ϕ is supersingular, the Frobenius $\tau^{\deg(\mathfrak{p})}$ has trace Tr_ϕ zero and its characteristic polynomial is

$$P_\phi(X) = X^2 + \epsilon_\phi \mathfrak{p}(x).$$

Since $\mathfrak{m}$ divides the Euler-Poincaré characteristic $\chi(\phi(\mathbb{F}_{\mathfrak{p}})) = P_\phi(1) = 1 + \epsilon_\phi \mathfrak{p}(x)$, the characteristic polynomial factors modulo $\mathfrak{m}$ as

$$\begin{aligned} P_\phi(X) \mod \mathfrak{m}(x) &= (X-1)(X - \epsilon_\phi \mathfrak{p}(x)) \mod \mathfrak{m}(x) \\ &= (X-1)(X+1) \mod \mathfrak{m}(x) \end{aligned}$$

Thus the Frobenius $\tau^{\deg(\mathfrak{p})}$ acting on $\Lambda_\phi[\mathfrak{m}]$ has a 1-eigenspace and a complement -1-eigenspace. Take a generator λ_1 for the 1-eigenspace. So $\tau^{\deg(\mathfrak{p})}\lambda_1 = \lambda_1$ and $\lambda_1 \in \phi(\mathbb{F}_{\mathfrak{p}})$. Likewise pick a generator λ_{-1} for the -1-eigenspace. So $\tau^{2\deg(\mathfrak{p})}\lambda_{-1} = \lambda_{-1}$ and $\lambda_{-1} \in \phi(\mathbb{F}_{\mathfrak{p}^2})$. □

We sketch an alternate proof using Hasse invariants that may be instructive. Since $\phi \,/\mathbb{F}_{\mathfrak{p}}$ is supersingular, the Frobenius element has trace Tr_ϕ zero and its characteristic polynomial is $P_\phi(X) = X^2 + \epsilon_\phi \mathfrak{p}(x)$. By remark 1, we assume $\epsilon_\phi = 1$ without loss of generality. Consequently, the Euler-Poincaré characteristic is $\chi(\phi(\mathbb{F}_{\mathfrak{p}})) = P_\phi(1) = 1 + \mathfrak{p}(x)$. For $\lambda \in \Lambda_\phi[\mathfrak{m}]$,

$$0 = \phi_{\chi(\phi(\mathbb{F}_{\mathfrak{p}}))}(\lambda) = \phi_{1+\mathfrak{p}}(\lambda) = (1 + \phi_{\mathfrak{p}})(\lambda) = (1 - \tau^{2\deg(\mathfrak{p})})(\lambda).$$

where the first equality follows since $\mathfrak{m}$ divides $\chi(\phi(\mathbb{F}_{\mathfrak{p}}))$ and the last equality is a consequence of equation 1. Thus λ is fixed by $\tau^{2\deg(\mathfrak{p})}$ and the lemma follows.

Computing ℓ-torsion: We first compute a generator λ_1 for the 1-eigenspace. One way is to pick $\beta \in \phi(\mathbb{F}_{\mathfrak{p}})$ at random and take λ_1 to be $\phi_{(1+\epsilon_\phi \mathfrak{p})/\ell}(\beta)$, after testing to ensure the later is non zero. Computing a generator λ_{-1} is similar. Take a random $\beta \in \phi(\mathbb{F}_{\mathfrak{p}^2})$ at random and take μ_{-1} to be $\phi_{(1+\epsilon_\phi \mathfrak{p})^2/\ell}(\beta)$, after testing to ensure the later is not in $\phi(\mathbb{F}_{\mathfrak{p}})$. By diagonalizing the basis $\{\lambda_1, \mu_{-1}\}$, we can extract λ_{-1}. The diagonalization is easy since Drinfeld module discrete logarithms are easy [28].

3.2 Explicit ℓ-power-Isogeny

Define the degree of an L-isogeny $\iota : \phi\,/L \to \psi\,/L$ (for a finite extension $L/\mathbb{F}_{\mathfrak{p}}$) as

$$\deg(\iota) := \chi(\phi(ker(\iota)),$$

closely following the notion of isogeny norm in Gekeler [14]. For example, the isogeny $\phi_{\mathfrak{f}} : \phi\,/\mathbb{F}_{\mathfrak{p}} \to \phi\,/\mathbb{F}_{\mathfrak{p}}$ for some monic $\mathfrak{f} \in \mathbb{F}_q[x]$ has degree $\deg(\phi_{\mathfrak{f}}) = \mathfrak{f}(x)^2$. An isogeny ι with degree $\deg(\iota) = \mathfrak{f} \in \mathbb{F}_q[x]$ will be called an $\mathfrak{f}$-isogeny. Let $\deg_\tau(\iota)$ denote the degree of an isogeny ι as a polynomial in τ. An $\mathfrak{f}$-isogeny ι thus has $\deg_\tau(\iota) = \deg(\mathfrak{f})$.

Let ϕ be a supersingular Drinfeld module of characteristic $\mathfrak{p}$, which we assume without loss of generality to be defined over $\mathbb{F}_{\mathfrak{p}^2}$. Let a monic irreducible $\ell(x) \in \mathbb{F}_q[x]$ divide the Euler-Poincaré characteristic $\chi(\phi(\mathbb{F}_{\mathfrak{p}}))$. We construct explicit ℓ-isogenies that are factors of the ℓ^2-isogeny ϕ_ℓ.

ℓ-isogenies: Recall from lemma 1 that the characteristic polynomial of the Frobenius $\tau^{\deg(\mathfrak{p})}$ factors modulo ℓ as

$$P_\phi(X) = (X-1)(X+1) \mod \ell(x)$$

and there exists $\lambda_1 \in \phi(\mathbb{F}_{\mathfrak{p}})$ and $\lambda_{-1} \in \phi(\mathbb{F}_{\mathfrak{p}^2})$ such that as $\mathbb{F}_q[x]$-modules

$$\Lambda_\phi[\ell] = \langle\lambda_1\rangle \oplus \langle\lambda_{-1}\rangle.$$

The (necessarily cyclic) $\mathbb{F}_q[x]$-submodules of $\Lambda_{\mathfrak{p}}[\ell]$ with Euler-Poincaré characteristic ℓ are of the form $\langle\lambda\rangle$ for $\lambda \in \Lambda_\phi[\ell]$. There are $q^{\deg(\ell)}+1$ such submodules, enumerated without repetition as $\langle\lambda_{-1}\rangle$ and $\{\langle\lambda_1+\phi_{\mathfrak{f}}(\lambda_{-1})\rangle\}$ (where $\mathfrak{f} \in \mathbb{F}_q[x]$ runs through a set of representatives of $\mathbb{F}_\ell$). In total, there are $q^{\deg(\ell)}+1$. For each such submodule Λ, there is a unique ℓ-isogeny

$$\iota_\Lambda : \phi\,/\mathbb{F}_{\mathfrak{p}^2} \longrightarrow \phi^\Lambda\,/\mathbb{F}_{\mathfrak{p}^2}$$

with kernel Λ. We next explicitly construct the isogeny $\iota_\Lambda \in \mathbb{F}_{\mathfrak{p}^2}\langle\tau\rangle$ that will also yield the coefficients of Drinfeld module $\phi^\Lambda\,/\mathbb{F}_{\mathfrak{p}^2}$ we implicitly defined. Our constructions only need the special case $\deg(\ell) = 1$, where the construction is particularly simple. Assume $\deg(\ell) = 1$ for the remainder of this subsection.

Consider $\Lambda = \langle\lambda\rangle$ for some $\lambda \in \Lambda_\phi[\ell]$. Seen as elements of $\mathbb{F}_{\mathfrak{p}^2}$, $\langle\lambda\rangle$ forms the one dimensional $\mathbb{F}_q$-space $\{c\lambda, c \in \mathbb{F}_q\}$. Thus there is a monic degree one (in τ) element in $\mathbb{F}_{\mathfrak{p}}[\tau]$ that kills $\langle\lambda\rangle$, namely $\tau - \lambda^{q-1}$, evidently independent of the chosen generator for $\langle\lambda\rangle$. The ring $\mathbb{F}_{\mathfrak{p}^2}\langle\tau\rangle$ has a right division algorithm [16][Prop. 1.6.2]. Thus there exists unique $u(\tau), v(\tau) \in \mathbb{F}_{\mathfrak{p}^2}\langle\tau\rangle$ (with $v(\tau)$ of τ-degree zero) such that $\phi_\ell = u(\tau)(\tau - \lambda^{q-1}) + v(\tau)$. Since $\phi_\ell(\lambda) = (\tau - \lambda^{q-1})(\lambda) = 0$, we infer $v(\tau) = 0$ and $\tau - \lambda^{q-1}$ right divides ϕ_ℓ. There thus exists a $a\tau + b \in \mathbb{F}_{\mathfrak{p}^2}\langle\tau\rangle$ such that

$$\phi_\ell = (a\tau+b)(\tau - \lambda^{q-1})$$

$$\Rightarrow (\tau - \lambda^{q-1})\phi_\ell = (\tau-\lambda^{q-1})(a\tau+b)(\tau-\lambda^{q-1}).$$

Define $\iota_\Lambda := \tau - \lambda^{q-1}$ and define $\phi^{\langle\lambda_1\rangle}\,/\mathbb{F}_{\mathfrak{p}}$ by setting

$$\phi^\Lambda_\ell := (\tau - \lambda^{q-1})(a\tau+b).$$

Since $\deg(\ell) = 1$, $\phi^{\langle\lambda_1\rangle}/\mathbb{F}_{\mathfrak{p}}$ is completely determined by the image ϕ_ℓ^Λ of ℓ. By construction,

$$\iota_\Lambda \ \phi_\ell = \phi_\ell^\Lambda \ \iota_\Lambda,$$

which along with ℓ being of degree 1 implies

$$\iota_\Lambda \ \phi_{\mathfrak{f}} = \phi_{\mathfrak{f}}^\Lambda \ \iota_\Lambda, \quad \forall \mathfrak{f} \in \mathbb{F}_q[x]$$

and we indeed obtain the isogeny

$$\iota_\Lambda : \phi/\mathbb{F}_{\mathfrak{p}^2} \longrightarrow \phi^\Lambda/\mathbb{F}_{\mathfrak{p}^2}.$$

$\mathbb{F}_{\mathfrak{p}}$-isogeny: For a supersingular Drinfeld module $\phi/\mathbb{F}_{\mathfrak{p}}$ and a degree one monic ℓ dividing $\chi(\phi(\mathbb{F}_{\mathfrak{p}}))$, define the operation

$$\ell \star \phi/\mathbb{F}_{\mathfrak{p}} := \phi^{\langle\lambda_1\rangle}/\mathbb{F}_{\mathfrak{p}}$$

through the $\mathbb{F}_{\mathfrak{p}}$-isogeny (with the 1-eigenspace $\langle\lambda_1\rangle$ as the kernel)

$$\iota_{\langle\lambda_1\rangle} : \phi/\mathbb{F}_{\mathfrak{p}} \longrightarrow \phi^{\langle\lambda_1\rangle}/\mathbb{F}_{\mathfrak{p}}.$$

Extend the operation to accommodate powers ℓ^a of ℓ recursively;

$$\ell^a \star \phi/\mathbb{F}_{\mathfrak{p}} := \ell \star (\ell^{a-1} \star \phi/\mathbb{F}_{\mathfrak{p}}).$$

This is well defined since being $\mathbb{F}_{\mathfrak{p}}$-isogenous, $\phi/\mathbb{F}_{\mathfrak{p}}$ and $\ell^{a-1} \star \phi/\mathbb{F}_{\mathfrak{p}}$ have the same characteristic polynomial, ensuring ℓ divides the Euler-Poincaré characteristic $\chi\left((\ell^{a-1} \star \phi/\mathbb{F}_{\mathfrak{p}})(\mathbb{F}_{\mathfrak{p}})\right)$. More generally, for a set L of monic degree one polynomials dividing $\chi(\phi(\mathbb{F}_{\mathfrak{p}}))$, L-smooth polynomials act on $\mathbb{F}_{\mathfrak{p}}$ through the $\star$ operator.

***ℓ*-power Isogeny:** For a supersingular Drinfeld module $\phi/\mathbb{F}_{\mathfrak{p}^2}$ and a degree one ℓ dividing $\chi(\phi(\mathbb{F}_{\mathfrak{p}}))$, an ℓ-power isogeny is obtained by composing a sequence of ℓ-isogenies. Since ℓ-isogenies do not necessarily commute, their ordering in the sequence matters. Conversely, every ℓ-power isogeny factors as a composition of ℓ-isogenies. An exception to the non-commutativity occurs (as we will see shortly) in the special case when $\phi/\mathbb{F}_{\mathfrak{p}}$ is defined over $\mathbb{F}_{\mathfrak{p}}$ and only $\mathbb{F}_{\mathfrak{p}}$-isogenies are considered.

The algorithmic details for the computation of ℓ-power isogenies and more generally smooth degree isogenies is discussed at the end of §4.2.

3.3 $\mathbb{F}_{\mathfrak{p}}$-restricted Isogeny graph:

Let $\phi/\mathbb{F}_{\mathfrak{p}}$ be a supersingular Drinfeld module. The $\mathbb{F}_{\mathfrak{p}}$-endomorphism ring $End_{\mathbb{F}_{\mathfrak{p}}}(\phi)$ is an order in the imaginary quadratic extension $\mathbb{F}_q(x)(\sqrt{D_\phi})$ where D_ϕ is the discriminant $-4\epsilon_\phi\mathfrak{p}$ of the characteristic polynomial $P_\phi(X) = X^2 + \epsilon_\phi\mathfrak{p}(x)$. In particular, $End_{\mathbb{F}_{\mathfrak{p}}}(\phi)$ is commutative. Drinfeld modules $\mathbb{F}_{\mathfrak{p}}$-isogenous to $\phi/\mathbb{F}_{\mathfrak{p}}$ are precisely those with the same characteristic polynomial. Let π be a root of $P_\phi(X)$. The number of $\mathbb{F}_{\mathfrak{p}}$-isomorphism classes of Drinfeld modules isogenous to $\phi/\mathbb{F}_{\mathfrak{p}}$ is related to the Gauss class number $h(\mathbb{F}_q[x][\pi])$ of $\mathbb{F}_q[x][\pi]$ [15][Prop. 6.8][30];

$$\sum_{\psi/\mathbb{F}_{\mathfrak{p}}} \frac{1}{|Aut_{\mathbb{F}_{\mathfrak{p}}}(\psi)|} = h(\mathbb{F}_q[x][\sqrt{D_\phi}]).$$

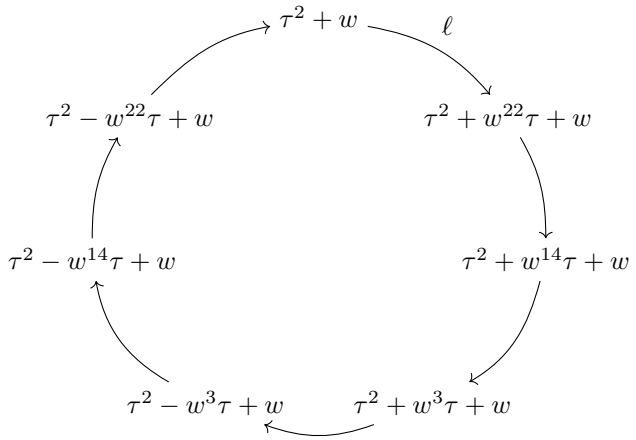
Counting without weighing by $1/|Aut_{\mathbb{F}_\mathfrak{p}}(\psi)|$, the formula has to distinguish the parity of the degree of $\mathfrak{p}$. The number of $\mathbb{F}_\mathfrak{p}$-isomorphism classes of Drinfeld modules isogenous to $\phi\,/\mathbb{F}_\mathfrak{p}$ is

$$\begin{cases} h(\mathbb{F}_q(x)(\sqrt{c\mathfrak{p}})) & \text{if } \deg(\mathfrak{p}) \text{ is even} \\ h(\mathbb{F}_q(x)(\sqrt{c\mathfrak{p}})) + h(\mathbb{F}_q(x)(\sqrt{\mathfrak{p}})) & \text{if } \deg(\mathfrak{p}) \text{ is odd} \end{cases}$$

where $c \in \mathbb{F}_q$ is a non square and $h()$ denotes the divisor class number of the enclosed field. Either way, from analytic class number formula (c.f. [15],[8][Lem.4.2]), the count is roughly $\sqrt{|\mathbb{F}_\mathfrak{p}|}$.

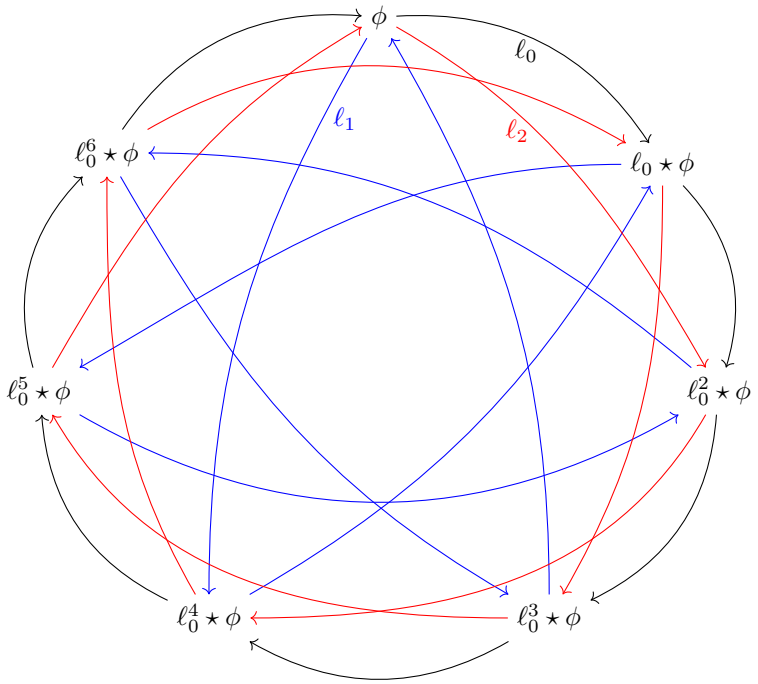
Let $\ell \in \mathbb{F}_q[x]$ be a monic degree one irreducible dividing the Euler-Poincaré characteristic $\chi(\phi(\mathbb{F}_\mathfrak{p}))$. Consider the graph $G_{\phi,\ell}$ with $\mathbb{F}_\mathfrak{p}$-isomorphism classes of Drinfeld modules $\mathbb{F}_\mathfrak{p}$-isogenous to $\phi\,/\mathbb{F}_\mathfrak{p}$ as vertices and $\mathbb{F}_\mathfrak{p}$-isogenies of degree ℓ as edges. Since D_ϕ is square-free, $G_{\phi,\ell}$ consists of a single connected component and is cyclic. We can traverse this cycle by consecutive powers of ℓ acting through the $\star$ operation.

Example 1. Take $q = 3$, $\mathfrak{p}(x) = x^3 - x + 1 \in \mathbb{F}_3[x]$ and $\ell(x) = x \in \mathbb{F}_3[x]$. Denote $x \mod \mathfrak{p}$ by w for ease of notation. Start with the supersingular Drinfeld module $\phi\,/\mathbb{F}_\mathfrak{p}$ with defining equation $\phi_x = \tau^2 + w$, duly noting that $\ell = x$ does indeed divide $\chi(\phi(\mathbb{F}_\mathfrak{p})) = x^3 - x$. Traverse the graph $G_{\phi,\ell}$ as illustrated below, in a clockwise cycle through the $\star$ action corresponding to $\ell = x$. A vertex corresponding to a Drinfeld module ψ is labelled by its defining image ψ_x.



Schreier Graphs: Now take a set L of $\ell(x) \in \mathbb{F}_q[x]$ that are monic degree one polynomials dividing the Euler-Poincaré characteristic $\chi(\phi(\mathbb{F}_\mathfrak{p}))$. Consider the graph $G_{\phi,L}$ with $\mathbb{F}_\mathfrak{p}$-isomorphism classes of Drinfeld modules $\mathbb{F}_\mathfrak{p}$-isogenous to $\phi\,/\mathbb{F}_\mathfrak{p}$ as vertices and $\mathbb{F}_\mathfrak{p}$-isogenies of degree ℓ for $\ell \in L$ as edges. That is, the set of edges in $G_{\phi,L}$ is the union of the set of edges of $G_{\phi,\ell}$ as ℓ runs through L. Since $End_{\mathbb{F}_\mathfrak{p}}(\phi)$ is commutative, the ℓ-isogenies corresponding to distinct ℓ commute. This structure is evident from the following representative example.

Example 2. Set $q = 3$, $\mathfrak{p}(x) = x^3 - x + 1 \in \mathbb{F}_3[x]$ and $L = \{x, x+1, x+2\} \subset \mathbb{F}_3[x]$. Starting with the supersingular Drinfeld module $\phi\,/\mathbb{F}_\mathfrak{p}$ with defining equation $\phi_x = \tau^2 + (x \mod \mathfrak{p})$, traverse the graph $G_{\phi,L}$ as illustrated below. The Drinfeld modules are arranged in a clockwise cycle through the $\star$ action corresponding to $\ell_0 = x$. The graph in black is exactly as in example 1 above. Blue edges correspond to the $\ell_1 = x + 1$ action and red edges to the $\ell_2 = x + 2$ action.



3.4 Full $\overline{\mathbb{F}}_{\mathfrak{p}}$-isogeny graphs:

For a degree one monic ℓ relative prime to $\mathfrak{p}$, the supersingular ℓ-isogeny graph, denoted by $G^{ss}_{\mathfrak{p},\ell}$, consists of $\overline{\mathbb{F}}_{\mathfrak{p}}$-isomorphism classes of supersingular Drinfeld modules over $\mathbb{F}_{\mathfrak{p}^2}$ as vertices. The absolute j-invariants of the Drinfeld modules thus make for convenient vertex indices. There is an edge between every pair of vertices connected by a ℓ degree $\mathbb{F}_{\mathfrak{p}^2}$-isogeny. Since being $\mathbb{F}_{\mathfrak{p}^2}$-isogenous is an equivalence relation, the edges are well defined and undirected. The degree of each vertex is the number of ℓ-isogenies starting from it; which is $q+1$ since ℓ is degree 1. The number of vertices is roughly $|\mathbb{F}_{\mathfrak{p}}| = q^{\deg(\mathfrak{p})}$. This estimate is obtained by relating the number of $\overline{\mathbb{F}}_{\mathfrak{p}}$-isomorphism classes of supersingular Drinfeld modules over $\mathbb{F}_{\mathfrak{p}^2}$ to the class number of the unique quaternion algebra over $\mathbb{F}_q(x)$ ramifying precisely at $\mathfrak{p}$ and the place at infinity [14][Thm. 4.3].

Recall that two Drinfeld modules over $\mathbb{F}_{\mathfrak{p}^2}$ are $\overline{\mathbb{F}}_{\mathfrak{p}}$-isogenous if and only if they have the same characteristic polynomial. Further, we can choose a representative $\phi^{\Lambda}/\mathbb{F}_{\mathfrak{p}^2}$ for each $\mathbb{F}_{\mathfrak{p}}$-isomorphism class of supersingular Drinfeld module of characteristic $\mathfrak{p}$ such that $\epsilon_{\phi,\mathfrak{p}} = 1$. Thus, for an irreducible ℓ dividing $1+\mathfrak{p}$, the supersingular ℓ-isogeny graph $G^{ss}_{\mathfrak{p},\ell}$ is a connected $\ell+1$ regular graph with roughly $q^{\deg(\mathfrak{p})}$ vertices. We will see shortly that these are the best possible expander graphs (in the spectral gap sense).

Ramanujan Graphs: Expander graphs are informally highly connected sparse graphs. There are different yet closely related notions of connectivity/expansion, ranging from vertex expansion, edge expansion to spectral expansion. Of particular interest to us will be families of connected d-regular graphs with an increasing number of vertices. For such graphs, the Laplacian has d as an eigenvalue and if in addition bipartite, has $-d$ as an eigenvalue. These

are deemed as trivial eigenvalues. The spectral condition for a d-regular graph to be an expander asks for a spectral gap, that is, for the non trivial eigenvalues λ of the Laplcian to be bounded $\lambda << d$ away from d. A lower bound of Alon and Bopanna shows that $|\lambda| \leq 2\sqrt{d-1}$ is asymptotically the best possible [1,23,19]. A Ramanujan graph is one meeting the bound $|\lambda| \leq 2\sqrt{d-1}$. Margulis and Lubotzky-Sarnak-Philips were the first to construct explicit infinite families of Ramanujan graphs as Cayley graphs of the projective special linear groups $PSL_2(\mathbb{F}_p)$ modulo primes p. Their constructions yield families for every prime plus one degree. The proof of the spectral bound relies on Deligne's proof of the Ramanujan-Peterson conjecture, hence the name Ramanujan graph. Morgenstern extended their construction to account for prime power plus one degrees by looking instead to Cayley graphs of the projective special linear groups $PSL_2(\mathbb{F}_{p^c})$ modulo prime powers p^c [21]. One remarkable feature in Morgenstern's construction is that it does not require constructing large prime numbers, but only large prime powers. It is a long standing open problem to find a deterministic algorithm to construct a large prime number, whereas constructing a large prime powers is trivial. Marcus, Spielman and Srivastava [20] constructed explicit infinite families of bipartite Ramanujan graphs for every degree greater than 2.

Supersingular Isogeny Ramanujan Graphs: Ramanujan graphs arising as isogeny graphs of supersingular elliptic curves are the setting of the De Feo-Jao-Plût post-quantum cryptosystem [17,9]. For prime numbers p, ℓ with ℓ dividing $1+p$, the supersingular elliptic curve isogeny graph consists of isomorphism classes (over the algebraic closure $\overline{\mathbb{F}}_p$) of supersingular elliptic curves over $\overline{\mathbb{F}}_p$ with degree ℓ isogenies as edges. Pizer showed that these graphs are $\ell+1$ regular Ramanujan graphs. Papikian proved the Drinfeld analogue [24][Thm 4.1](see also [22][Thm 2.1]): For monic irreducibles $\mathfrak{p}, \ell$ with ℓ dividing $1+\mathfrak{p}$, the supersingular ℓ-isogeny graph $G^{ss}_{\mathfrak{p},\ell}$ is a $q+1$-regular Ramanujan graph. These graphs will form the basis of our Drinfeld module analogue of SIDH.

4 Drinfeld module isogeny based Cryptosystems

In this section, we devise Drinfeld module analogues of CSIDH and SIDH protocols. We restrict our attention to the key exchange protocols. It is straightforward to extend our constructions to yield Drinfeld module isogeny based encryption, signature protocols etc. We refrain from optimizing the implementations for all these protocols will be broken in the subsequent section.

4.1 Drinfeld module analogue of CSIDH

Public Parameter Selection: The $\mathbb{F}_{\mathfrak{p}}$-restricted isogeny graphs $G_{\phi,L}$ will be the setting for the Drinfeld analogue of the CSIDH post quantum cryptosystem [3]. To set the stage, we first construct

- a monic irreducible polynomial $\mathfrak{p} \in \mathbb{F}_q[x]$ of degree $d > 1$,
- a set $L \subseteq \mathbb{F}_q[x]$ of monic degree one polynomials,
- a supersingular Drinfeld module $\phi \big/ \mathbb{F}_{\mathfrak{p}}$ such that $\forall \ell \in L$, ℓ divides the Euler-Poincaré characteristic $\chi(\phi(\mathbb{F}_{\mathfrak{p}}))$.

The resulting Schreier graph $G_{\phi,L}$ has about $q^{d/2}$ vertices, which is exponential in the degree d.

Our recipe to polynomial selection is to choose a set of monic degree one polynomials L, pick a small degree monic cofactor $\mathfrak{b} \in \mathbb{F}_q[x]$ at random and set $\mathfrak{p}(x)$ to $\mathfrak{b}(x)\prod_{\ell \in L}\ell(x) - 1$, if it is irreducible. It then suffices to choose a Drinfeld module $\phi/\mathbb{F}_{\mathfrak{p}}$ with Euler-Poincaré characteristic $\chi(\phi(\mathbb{F}_{\mathfrak{p}})) = 1 + \mathfrak{p}$. The later is accomplished by choosing a Drinfeld module with carefully chosen degenerate absolute j-invariant (either zero or $x^q - x$, depending on the parity of d).

For concreteness, choose a target small prime set size L and consider an odd target degree d. It is necessary that $d \geq |L|$. Take the difference $d - |L|$ as the degree of the random cofactor $\mathfrak{b}$. Heuristically, a polynomial of the form $1 + \mathfrak{b}\prod_{\ell \in L}\ell$ is likely to be irreducible with probability roughly $\Theta(1/d)$ (for large enough q). A sample space of size $q^{d-|L|} >> d$ should suffice to hit an irreducible. To this end, we choose $d - |L| >> \log_q(d)$. The heuristic argument can be made completely rigorous.

The reason we restricted ourselves to odd degree d is that for an odd degree irreducible $\mathfrak{p}$, a Drinfeld module with zero absolute j-invariant is supersingular. This is implicit in [13,6], but we prove it below for clarity.

Lemma 2. *The Drinfeld module $\phi/\mathbb{F}_{\mathfrak{p}}$ with defining equation $\phi_x := \tau^2 + (x \mod \mathfrak{p})$ is supersingular if and only if* $\deg(\mathfrak{p})$ *is odd.*

Proof. Recursively define a sequence $(r_{\phi,k})_{k\in\mathbb{N}}$ in $\mathbb{F}_{\mathfrak{p}}^{\mathbb{N}}$ as $r_{\phi,0} := 1$, $r_{\phi,1} := g_\phi$ and for $k > 1$,

$$r_{\phi,k} := g_\phi^{q^{k-1}} r_{\phi,k-1} - (x^{q^{k-1}} - x)\Delta_\phi^{q^{k-2}} r_{\phi,k-2}.$$

Gekeler [15, Eq 3.6, Prop 3.7] showed that $r_{\phi,k}$ is the value of the normalized Eisenstein series of weight $q^k - 1$ on ϕ and established Deligne's congruence for Drinfeld modules, which ascertains that the Hasse invariant

$$h_\phi = r_{\phi,\deg(\mathfrak{p})}.$$

Substituting $g_\phi = 0$ and $\Delta_\phi = 1$ in the recurrence, we get

$$h_\phi = r_{\phi,\deg(\mathfrak{p})} = \begin{cases} 0 & \text{if } \deg(\mathfrak{p}) \text{ is odd} \\ \prod_{i=1}^{\deg(\mathfrak{p})/2}\left(x^{q^{2i-1}} - x\right) & \text{if } \deg(\mathfrak{p}) \text{ is even} \end{cases}$$

Since no even degree irreducible polynomials divide $x^{q^m} - x$ for odd m, it follows that $h_\phi = 0$ if and only if $\deg(\mathfrak{p})$ is odd. □

In summary, for odd degree $\mathfrak{p}$, we may explicitly choose such a supersingular Drinfeld module $\phi/\mathbb{F}_{\mathfrak{p}}$ with Euler-Poincaré characteristic $\chi(\phi(\mathbb{F}_{\mathfrak{p}})) = 1 + \mathfrak{p}$ through the defining equation $\phi_x := \tau^2 + (x \mod \mathfrak{p})$.

Artin-Schreier Extensions: When q is an odd prime, we propose a particularly clean polynomial selection recipe using Artin-Schreier extensions. Take L to be the set of all monic degree one polynomials in $\mathbb{F}_q[x]$ and set

$$\mathfrak{p}(x) := 1 + \prod_{\ell \in L}\ell(x) = x^q - x + 1.$$

By Artin-Schreier theory, $\mathfrak{p}$ is irreducible. By construction, $\mathfrak{p}$ is of odd degree q. Hence, the Drinfeld module $\phi\,/\mathbb{F}_{\mathfrak{p}}$ with defining equation $\phi_x := \tau^2 + (x \mod \mathfrak{p})$ is supersingular with with Euler-Poincaré characteristic $\chi(\phi(\mathbb{F}_{\mathfrak{p}})) = 1 + \mathfrak{p}$. The size of the graph $G_{\phi,L}$ in this case is roughly $q^{q/2}$.

Key Generation: As public parameters, we have an odd degree d irreducible $\mathfrak{p}$, a set L of monic degree one polynomials and a supersingular Drinfeld module $\phi\,/\mathbb{F}_{\mathfrak{p}}$ such that $\forall \ell \in L$, ℓ divides the Euler-Poincaré characteristic $\chi(\phi(\mathbb{F}_{\mathfrak{p}}))$.

Alice chooses a string of integers $(a_\ell, \ell \in L)$ drawn at random from an interval $[-m, m]^{|L|}$ and sets $\mathfrak{s}_a := \prod_{\ell \in L} \ell^{a_\ell}$ as her private key. She publishes the (absolute j-invariant of the) Drinfeld module

$$\phi^a\,/\mathbb{F}_{\mathfrak{p}} := \mathfrak{s}_a \star \phi\,/\mathbb{F}_{\mathfrak{p}}$$

as her public key. Likewise, Bob chooses a string of integers $(b_\ell, \ell \in L)$ drawn at random from an interval $[-m, m]^{|L|}$ and sets $\mathfrak{s}_b := \prod_{\ell \in L} \ell^{b_\ell}$ as his private key. He publishes the (absolute j-invariant of the) Drinfeld module $\phi^a\,/\mathbb{F}_{\mathfrak{p}} := \mathfrak{s}_b \star \phi\,/\mathbb{F}_{\mathfrak{p}}$ as his public key.

Key Exchange: On receiving Bob's public key $\mathfrak{s}_b \star \phi\,/\mathbb{F}_{\mathfrak{p}}$, Alice uses her secret key $\mathfrak{s}_a$ to compute $\mathfrak{s}_a \star (\mathfrak{s}_b \star \phi\,/\mathbb{F}_{\mathfrak{p}})$. Likewise, On receiving Alice's public key $\mathfrak{s}_a \star \phi\,/\mathbb{F}_{\mathfrak{p}}$, Bob uses his secret key $\mathfrak{s}_b$ to compute $\mathfrak{s}_b \star (\mathfrak{s}_a \star \phi\,/\mathbb{F}_{\mathfrak{p}})$. They both share as the secret, the absolute j-invariant of the Drinfeld module

$$\mathfrak{s}_a \star (\mathfrak{s}_b \star \phi\,/\mathbb{F}_{\mathfrak{p}}) = \mathfrak{s}_b \star (\mathfrak{s}_a \star \phi\,/\mathbb{F}_{\mathfrak{p}}) = (\mathfrak{s}_a\mathfrak{s}_b) \star \phi\,/\mathbb{F}_{\mathfrak{p}}\,.$$

4.2 Drinfeld module analogue of SIDH

We propose a Drinfeld module analogue of the non-interactive key exchange protocol of DeFeo-Jao-Plut [17,9]. To set the stage, we first construct

- a monic irreducible polynomial $\mathfrak{p} \in \mathbb{F}_q[x]$ of degree $d > 1$,
- a set $L \subseteq \mathbb{F}_q[x]$ of monic degree one polynomials and two L-smooth products $\mathfrak{c}_A := \prod_{\ell \in L} \ell^{a_\ell}$ and $\mathfrak{c}_B := \prod_{\ell \in L} \ell^{b_\ell}$ with disjoint support,
- a starting supersingular Drinfeld module $\phi\,/\mathbb{F}_{\mathfrak{p}^2}$ such that $\mathfrak{c}_A\mathfrak{c}_B$ divides the Euler-Poincaré characteristic $\chi(\phi(\mathbb{F}_{\mathfrak{p}^2}))$,
- two bases $\Lambda_\phi[\mathfrak{c}_A] = \langle \lambda_1^A \rangle \oplus \langle \lambda_{-1}^A \rangle$ and $\Lambda_\phi[\mathfrak{c}_B] = \langle \lambda_1^B \rangle \oplus \langle \lambda_{-1}^B \rangle$ respectively for the $\mathfrak{c}_A$ and $\mathfrak{c}_B$-torsion.

The resulting full $\overline{\mathbb{F}}_{\mathfrak{p}}$-isogeny graphs $G^{ss}_{\mathfrak{p},\ell}$, $\ell \in L$, each with the same set of roughly $q^{\deg(\mathfrak{p})}$ vertices will be the setting for our cryptosystem.

If one desires strict analogy with the SIDH, we may take $L = \{\ell_A, \ell_B\}$ to consists of two irreducible, say for instance $\ell_A = x$ and $\ell_B = x + 1$. Then set $\mathfrak{c}_A = \ell_A^r, \mathfrak{c}_B = \ell_B^r$ and select a $\mathfrak{p}$ such that $\mathfrak{p} = \ell_A^r \ell_B^r \mathfrak{f} \pm 1$ for some small degree cofactor $\mathfrak{f}$ and set the starting Drinfeld module to be $\phi_x := \tau^2 + (x \mod \mathfrak{p})$. Such a parameter selection can be accomplished through the procedure outlined in § 4.1.

There is much greater freedom in selecting $\mathfrak{c}_A$ and $\mathfrak{c}_B$ in our Drinfeld setting compared to the elliptic curves. One natural choice is set L to be the set of all monic polynomials and take

$\mathfrak{c}_A = x^{\frac{q-1}{2}} - 1$ and $\mathfrak{c}_B = x^{\frac{q+1}{2}} + x$. The relation between the Drinfeld module analogues of the CSIDH and SIDH are much more apparent in this case. The formula for parameter selection are particularly nice when q is an odd prime. Then by Artin-Schreier theory $\mathfrak{p}(x) = x^q - x + 1$ is irreducible and by lemma 2, the starting supersingular Drinfeld module may be chosen as $\phi_x = \tau^2 + (x \mod \mathfrak{p})$.

Key Generation: As her secret key, Alice chooses two uniformly random elements $\mathfrak{m}_A, \mathfrak{n}_A \in \mathbb{F}_q[x]$ of degree at most $\deg(\mathfrak{c}_A)$ (after testing to ensure no ℓ dividing $\mathfrak{c}_A$ divides both $\mathfrak{m}_A, \mathfrak{n}_A$). She then constructs the unique isogeny

$$\iota_A : \phi \,/\mathbb{F}_{\mathfrak{p}^2} \longrightarrow \phi^A \,/\mathbb{F}_{\mathfrak{p}^2}$$

with kernel

$$ker(\iota_A) = \langle \phi_{\mathfrak{m}_A}(\lambda_1^A) + \phi_{\mathfrak{n}_A}(\lambda_{-1}^A) \rangle.$$

She sends Bob the Drinfeld module $\phi^A \,/\mathbb{F}_{\mathfrak{p}^2}$ arrived at. Further, she also sends Bob the images $\iota_A(\lambda_1^B), \iota_A(\lambda_{-1}^B)$ of Bob's basis under her isogeny. Likewise, as his secret key, Bob chooses two uniformly random elements $\mathfrak{m}_B, \mathfrak{n}_B \in \mathbb{F}_q[x]$ of degree at most $\deg(\mathfrak{c}_B)$ (after testing to ensure no ℓ dividing $\mathfrak{c}_B$ divides both $\mathfrak{m}_B, \mathfrak{n}_B$). He then constructs the unique isogeny

$$\iota_B : \phi \,/\mathbb{F}_{\mathfrak{p}^2} \longrightarrow \phi^B \,/\mathbb{F}_{\mathfrak{p}^2}$$

with kernel

$$ker(\iota_B) = \langle \phi_{\mathfrak{m}_B}(\lambda_1^B) + \phi_{\mathfrak{n}_B}(\lambda_{-1}^B) \rangle.$$

He sends Alice the Drinfeld module $\phi^B \,/\mathbb{F}_{\mathfrak{p}^2}$ arrived at along with the images $\iota_B(\lambda_1^A), \iota_B(\lambda_{-1}^A)$ of Alice's basis under his isogeny.

Key Exchange: On receiving $\phi^B \,/\mathbb{F}_{\mathfrak{p}^2}, \iota_B(\lambda_1^A), \iota_B(\lambda_{-1}^A)$ from Bob, Alice constructs the unique isogeny

$$\widehat{\iota}_A : \phi^B \,/\mathbb{F}_{\mathfrak{p}^2} \longrightarrow \phi^{A \circ B} \,/\mathbb{F}_{\mathfrak{p}^2}$$

with kernel

$$ker(\widehat{\iota}_A) = \langle \phi^B_{\mathfrak{m}_A} \iota_B(\lambda_1^A) + \phi^B_{\mathfrak{n}_A} \iota_B(\lambda_{-1}^A) \rangle.$$

She is able to construct the kernel and consequently the isogeny from her secret $\mathfrak{m}_A, \mathfrak{n}_A$ and the information received from Bob. Likewise, using the information $\phi^A \,/\mathbb{F}_{\mathfrak{p}^2}, \iota_A(\lambda_1^B), \iota_A(\lambda_{-1}^B)$ from Alice, Bob constructs the unique isogeny

$$\widehat{\iota}_B : \phi^A \,/\mathbb{F}_{\mathfrak{p}^2} \longrightarrow \phi^{B \circ A} \,/\mathbb{F}_{\mathfrak{p}^2}$$

with kernel

$$ker(\widehat{\iota}_B) = \langle \phi^A_{\mathfrak{m}_B} \iota_A(\lambda_1^B) + \phi^A_{\mathfrak{n}_B} \iota_A(\lambda_{-1}^B) \rangle.$$

Shared Secret: Ultimately, Alice arrives at $\phi^{A \circ B} \,/\mathbb{F}_{\mathfrak{p}^2}$ and Bob arrives at $\phi^{B \circ A} \,/\mathbb{F}_{\mathfrak{p}^2}$. We next argue that $\phi^{A \circ B} \,/\mathbb{F}_{\mathfrak{p}^2}$ and $\phi^{B \circ A} \,/\mathbb{F}_{\mathfrak{p}^2}$ are $\overline{\mathbb{F}}_{\mathfrak{p}}$-isomorphic. Hence, their absolute j-invariant is a shared secret.

The kernel of the isogeny $\widehat{\iota}_A \circ \iota_B : \phi \,/\mathbb{F}_{\mathfrak{p}^2} \longrightarrow \phi^{A\circ B} \,/\mathbb{F}_{\mathfrak{p}^2}$ contains the kernel of ι_B, namely $\phi_{\mathfrak{m}_B}(\lambda_1^B) + \phi_{\mathfrak{n}_B}(\lambda_{-1}^B)$. To determine $ker(\widehat{\iota}_A \circ \iota_B)$ in its entirety, we first employ the defining commutation property of isogenies to rephrase $ker(\widehat{\iota}_A)$ as

$$ker(\widehat{\iota}_A) = \langle \phi^B_{\mathfrak{m}_A} \iota_B(\lambda_1^A) + \phi^B_{\mathfrak{n}_A} \iota_B(\lambda_{-1}^A) \rangle = \langle \iota_B \phi_{\mathfrak{m}_A}(\lambda_1^A) + \iota_B \phi_{\mathfrak{n}_A}(\lambda_{-1}^A) \rangle.$$

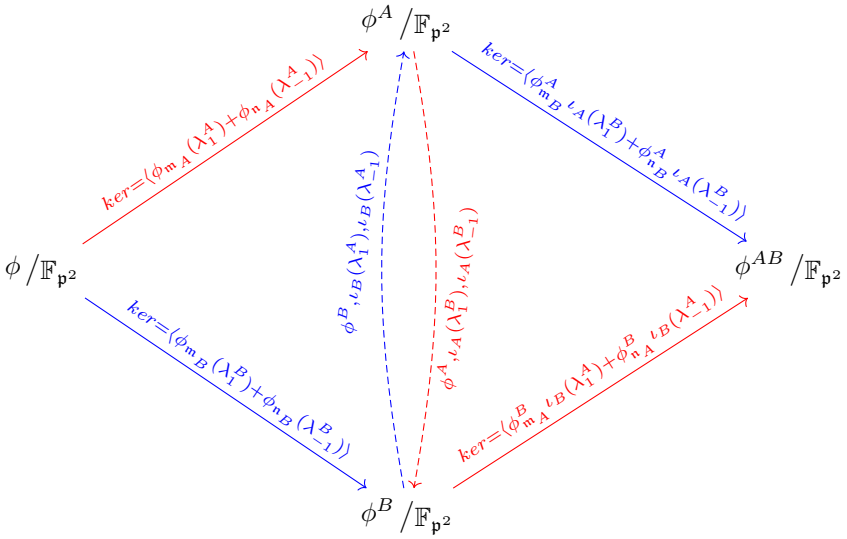
It is now apparent that the image of $\langle \phi_{\mathfrak{m}_A}(\lambda_1^A) + \phi_{\mathfrak{n}_A}(\lambda_{-1}^A) \rangle$ under ι_B is killed by $\widehat{\iota}_A$. By construction and degree considerations, we can conclude that

$$ker(\widehat{\iota}_A \circ \iota_B) = \langle \langle \phi_{\mathfrak{m}_A}(\lambda_1^A) + \phi_{\mathfrak{n}_A}(\lambda_{-1}^A) \rangle, \phi_{\mathfrak{m}_B}(\lambda_1^B) + \phi_{\mathfrak{n}_B}(\lambda_{-1}^B) \rangle.$$

By symmetry,

$$ker(\widehat{\iota}_B \circ \iota_A) = \langle \langle \phi_{\mathfrak{m}_A}(\lambda_1^A) + \phi_{\mathfrak{n}_A}(\lambda_{-1}^A) \rangle, \phi_{\mathfrak{m}_B}(\lambda_1^B) + \phi_{\mathfrak{n}_B}(\lambda_{-1}^B) \rangle.$$

Hence $\phi^{A\circ B} \,/\mathbb{F}_{\mathfrak{p}^2}$ and $\phi^{B\circ A} \,/\mathbb{F}_{\mathfrak{p}^2}$ are $\overline{\mathbb{F}}_{\mathfrak{p}}$-isomorphic and we may denote them as $\phi^{AB} \,/\mathbb{F}_{\mathfrak{p}^2}$ in the following augmented commutative diagram summarizing the key exchange. The solid lines represent isogenies (and computation) labelled with their kernels and dotted lines denote communication. Red lines correspond to computation or communication done by Alice and blue lines to Bob.



Computation of Isogenies: For ease of notation, denote the generator of Alice's secret as $\mu_A := \phi_{\mathfrak{m}_A}(\lambda_1^A) + \phi_{\mathfrak{n}_A}(\lambda_{-1}^A)$. During the key generation phase, Alice is faced with computing the unique isogeny

$$\iota_A : \phi \,/\mathbb{F}_{\mathfrak{p}^2} \longrightarrow \phi^A \,/\mathbb{F}_{\mathfrak{p}^2}$$

with kernel $\langle \mu_A \rangle$. This is accomplished through composing a sequence of isogenies

$$\phi \xrightarrow{\iota_0} \phi^1 \xrightarrow{\iota_1} \dots \qquad \phi^i \xrightarrow{\iota_i} \phi^{i+1} \xrightarrow{\iota_{i+1}} \dots \qquad \phi^{a-2} \xrightarrow{\iota_{a-1}} \phi^{a-1}$$

$$\mu_A \longmapsto \mu_1 \longmapsto \dots \qquad \mu_i \longmapsto \mu_{i+1} \longmapsto \dots \qquad \mu_{a-2} \longmapsto \mu_{a-1}.$$

The first isogeny ι_0 is built by choosing some prime ℓ_0 dividing $\mathfrak{c}_A$ and taking ι to have kernel $\phi_{\mathfrak{c}_A/\ell_0}(\mu_A)$. Then set $\mathfrak{c}_{A,1} := \mathfrak{c}_A/\ell_0$ and $\mu_1 = \iota_(\mu_A)$. At the i^{th}-iteration, pick a prime ℓ_i dividing $\mathfrak{c}_{A,i}$ and take ι_i to be the unique ℓ_i-isogeny with kernel $\langle \phi^i_{\mathfrak{c}_{A,i}/\ell_i}(\mu_i)\rangle$. At the end of the iteration, if $a := \deg(\mathfrak{c}_A)$ is the number of prime ℓ dividing $\mathfrak{c}_A$ counted with multiplicity, ϕ^{a-1} is the Drinfeld module $\phi^A/\mathbb{F}_{\mathfrak{p}^2}$ that we seek, up to $\overline{\mathbb{F}}_{\mathfrak{p}}$-isomorphism.

During key exchange, on receiving $\phi^B/\mathbb{F}_{\mathfrak{p}^2}, \iota_B(\lambda_1^A), \iota_B(\lambda_{-1}^A)$ from Bob, Alice has to compute the isogeny

$$\iota_{\langle \iota_B(\mu_A)\rangle} : \phi^B/\mathbb{F}_{\mathfrak{p}^2} \longrightarrow \phi^{AB}/\mathbb{F}_{\mathfrak{p}^2}$$

with kernel $\langle \iota_B(\mu_A)\rangle$. Using her secret $\mathfrak{m}_A, \mathfrak{n}_A$, Alice first computes

$$\iota_B(\mu_A) = \iota_B(\phi_{\mathfrak{m}_A}\lambda_1^A) + \iota_B(\phi_{\mathfrak{n}_A}\lambda_{-1}^A) = \phi^B_{\mathfrak{m}_A}\iota_B(\lambda_1^A) + \phi^B_{\mathfrak{n}_A}\iota_B(\lambda_{-1}^A).$$

Then she composes the following of isogeny sequence with $b := \deg(\mathfrak{c}_B)$

$$\phi^B \xrightarrow{\xi_0} \phi^{B,1} \xrightarrow{\xi_1} \dots \qquad \phi^{B,i} \xrightarrow{\xi_i} \phi^{B,i+1} \xrightarrow{\xi_{i+1}} \dots \qquad \xrightarrow{\xi_{b-1}} \phi^{B,b-1}$$

$$\iota_B(\mu_A) \longmapsto \nu_1 \longmapsto \dots \qquad \nu_i \longmapsto \nu_{i+1} \longmapsto \dots \qquad \longmapsto \nu_{b-1}.$$

The procedure is virtually identical to her previous computation. The first isogeny ξ_0 is built by choosing some prime ℓ_0 dividing $\mathfrak{c}_B$ and taking ξ_0 to have kernel $\phi_{\mathfrak{c}_B/\ell_0}(\iota_B(\mu_A))$; and so on until arriving at $\phi^{B,b-1} \cong \phi^{AB}$.

5 Cryptanalysis of Drinfeld isogeny based Cryptosystems

5.1 Cryptanalysis of the Drinfeld analogue of SIDH

Keep the notation as in § 4.2. We begin the cryptanalysis by first describing the underlying hardness assumptions, targeting Alice's secrets/computation.

Drinfeld supersingular Isogeny Problem: The Drinfeld analogue of the computational supersingular isogeny problem is given $\phi^A/\mathbb{F}_{\mathfrak{p}^2}, \iota_A(\lambda_1^B), \iota_A(\lambda_{-1}^B)$ to compute Alice's secret submodule $\langle \mu_A\rangle$. The decision version is to tell if there is indeed an $\mathfrak{c}_A$-isogeny from ϕ to $\phi^A/\mathbb{F}_{\mathfrak{p}^2}$.

Drinfeld supersingular Isogeny Diffie-Hellman: The computational Diffie-Hellmann problem asks to compute $\phi^{AB}/\mathbb{F}_{\mathfrak{p}^2}$ given $\phi^A/\mathbb{F}_{\mathfrak{p}^2}, \phi^B/\mathbb{F}_{\mathfrak{p}^2}, \iota_A(\lambda_1^B), \iota_A(\lambda_{-1}^B), \iota_B(\lambda_1^A), \iota_B(\lambda_{-1}^A)$ and the public parameters. It is at least as easy as the aforementioned computational Drinfeld supersingular isogeny problem; Alice's secret allows one to compute $\iota_A : \phi^B \longrightarrow \phi^{AB}$ as Alice would do.

Without loss of generality, assume Bob's isogeny degree $\deg(\mathfrak{c}_B)$ is at least as big as Alice's isogeny degree $\deg(\mathfrak{c}_A)$. We show that Bob can reconstruct Alice's secret key $\mathfrak{m}_A, \mathfrak{n}_A$ from Alice's communication $\phi^A/\mathbb{F}_{\mathfrak{p}^2}, \iota_A(\lambda_1^B), \iota_A(\lambda_{-1}^B)$ sent during the key exchange.

Succinct Representation of Large Degree Isogenies: We first show that Bob can find a succinct representation of Alice's isogeny ι_A and compute images under it. This completely breaks the system by solving the computational Drinfeld supersingular isogeny problem. The succinct representation springs right out of the definition. Recall that ι_A is of the form

$$\iota_A = \sum_{i=0}^{a} \alpha_i \tau^i \in \mathbb{F}_{\mathfrak{p}^2}\langle\tau\rangle$$

where $a = \deg(\mathfrak{c}_A)$. In particular, $a \leq \deg(\mathfrak{p})$ since $\deg(\mathfrak{c}_A) \leq \deg(\mathfrak{p})$. The coefficients α_i are in $\mathbb{F}_{\mathfrak{p}^2}$ and not a higher degree extension because ϕ is defined over $\mathbb{F}_{\mathfrak{p}^2}$ and so is the torsion $\Lambda_\phi[\mathfrak{c}_A]$. In summary, the size of the representation of ι_A as $\sum_{i=0}^{a} \alpha_i \tau^i$ is polynomial in the security parameter. Contrast this with the analogous case for elliptic curves, where it is not clear how to represent large degree isogenies succinctly, unless their factorization into a composition of small degree isogenies is known.

Isogeny Interpolation: The $\mathfrak{c}_B$-torsion module $\Lambda_\phi[\mathfrak{c}_B]$ seen as an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{\mathfrak{p}^2}$ has dimension $b = \deg(\mathfrak{c}_B)$. By assumption $b \geq a$. Since Alice's and Bob's exponents $\mathfrak{c}_A$ and $\mathfrak{c}_B$ are coprime, the images Alice sent generate the full $\mathfrak{c}_B$-torsion group as

$$\Lambda_{\phi^A}[\mathfrak{c}_B] = \langle \iota_A(\lambda_1^B)\rangle \oplus \langle \iota_A(\lambda_{-1}^B)\rangle.$$

Let $(\ell_i, 0 \leq i \leq b)$, be a sequence of (not necessarily distinct) monic degree one irreducibles dividing L such that $\prod_i \ell_i = \mathfrak{c}_B$. Compute the sequence of isogenies corresponding to action of the chosen sequence of primes under ϕ^A and consider the images of $\iota_A(\lambda_1^B), \iota_A(\lambda_{-1}^B)$ sent by Alice;

$$\begin{array}{llll}
\phi^A \xrightarrow{\phi^A_{\ell_0}} \phi^A \xrightarrow{\phi^A_{\ell_1}} \dots & \phi^A \xrightarrow{\phi^A_{\ell_i}} \dots & \xrightarrow{\phi^A_{\ell_{b-1}}} \phi^A \\
\iota_A(\lambda_1^B) \longmapsto \phi^A_{\ell_0}\iota_A(\lambda_1^B) \longmapsto \dots & \phi^A_{\ell_0\ell_1\dots\ell_i}\iota_A(\lambda_1^B) \longmapsto \dots & \longmapsto 0 \\
\iota_A(\lambda_{-1}^B) \longmapsto \phi^A_{\ell_0}\iota_A(\lambda_{-1}^B) \longmapsto \dots & \phi^A_{\ell_0\ell_1\dots\ell_i}\iota_A(\lambda_{-1}^B) \longmapsto \dots & \longmapsto 0.
\end{array}$$

Rephrasing the images by the commutation relations of isogenies, we get

$$\begin{array}{llll}
\phi^A \xrightarrow{\phi^A_{\ell_0}} \phi^A \xrightarrow{\phi^A_{\ell_1}} \dots & \phi^A \xrightarrow{\phi^A_{\ell_i}} \dots & \xrightarrow{\phi^A_{\ell_{b-1}}} \phi^A \\
\iota_A(\lambda_1^B) \longmapsto \iota_A\phi_{\ell_0}(\lambda_1^B) \longmapsto \dots & \iota_A\phi_{\ell_0\ell_1\dots\ell_i}(\lambda_1^B) \longmapsto \dots & \longmapsto 0 \\
\iota_A(\lambda_{-1}^B) \longmapsto \iota_A\phi_{\ell_0}(\lambda_{-1}^B) \longmapsto \dots & \iota_A\phi_{\ell_0\ell_1\dots\ell_i}(\lambda_{-1}^B) \longmapsto \dots & \longmapsto 0.
\end{array}$$

The images of ι_A at $2b$ elements in $\phi(\mathbb{F}_{\mathfrak{p}^2})$ constitutes an $\mathbb{F}_{\mathfrak{p}^2}$-linear system;

$$\iota_A(\delta) = \sum_{i=0}^{a} \alpha_i \delta^{q^i} = 0, \quad \delta \in E,$$

$$E := \left\{\iota_A\left(\phi_{\ell_0\ell_1\ldots\ell_i}(\lambda_1^B)\right), 0 \le i < b\right\} \bigcup \left\{\iota_A\left(\phi_{\ell_0\ell_1\ldots\ell_i}(\lambda_{-1}^B)\right), 0 \le i < b\right\} \subseteq \Lambda_\phi[\mathfrak{c}_B]$$

with the coefficients α_i as variables. By construction, since $\deg(\mathfrak{c}_B) \ge \deg(\mathfrak{c}_A)$, the linear system determines ι_A. By computing a basis for the roots of $\sum_i \alpha_i\tau^i$, we find Alice's secret. Since Alice's secret is revealed, it is easy to solve the computational Drinfeld supersingular isogeny Diffie-Hellman problem by following Alice's key exchange procedure.

Isogeny Factorization: There may be applications where an explicit path in the isogeny graph from $\phi/\mathbb{F}_{\mathfrak{p}^2}$ to $\phi^A/\mathbb{F}_{\mathfrak{p}^2}$ is sought. To this end, we look for some $\tau - \beta \in \mathbb{F}_{\mathfrak{p}^2}\langle\tau\rangle$ right dividing $\sum_i \alpha_i\tau^i$ resulting in a factorization $\iota_A = \widehat{\iota_A}(\tau - \beta)$. If such a $\tau - \beta$ happens to be an ℓ-isogeny from some $\psi/\mathbb{F}_{\mathfrak{p}^2}$ to $\phi^A/\mathbb{F}_{\mathfrak{p}^2}$, our problem reduces to finding an isogeny path from $\phi/\mathbb{F}_{\mathfrak{p}^2}$ to $\phi^A/\mathbb{F}_{\mathfrak{p}^2}$ given $\widehat{\iota_A}$. Since the number $q+1$ of ℓ-isogenies arriving at $\phi^A/\mathbb{F}_{\mathfrak{p}^2}$ is small, we can exhaustively search for such a factorization $\iota_A = \widehat{\iota_A}(\tau - \beta)$ using the right division algorithm in $\mathbb{F}_{\mathfrak{p}^2}\langle\tau\rangle$ [16][chap.1.6]

5.2 Cryptanalysis of the Drinfeld analogue of CSIDH

Keep the notation as in § 5.2. We begin the cryptanalysis by first mentioning the underlying problems, targeting Alice's secrets/computation. Given Alice's public key $\mathfrak{s}_a \star \phi/\mathbb{F}_{\mathfrak{p}}$, compute her secret key $\mathfrak{s}_a$. The computational Diffie-Hellman version is to compute $\mathfrak{s}_{ab} \star \phi/\mathbb{F}_{\mathfrak{p}}$ given $\mathfrak{s}_a \star \phi/\mathbb{F}_{\mathfrak{p}}$ and $\mathfrak{s}_b \star \phi/\mathbb{F}_{\mathfrak{p}}$.

Testing existence of isogenies of prescribed τ-degree: We first devise a procedure to decide (and recover) if there is an L-smooth degree $\mathbb{F}_{\mathfrak{p}}$-isogeny $\iota := \sum_{i=0}^{a} \alpha_i\tau^i \in \mathbb{F}_{\mathfrak{p}}\langle\tau\rangle$ of a prescribed τ-degree a from $\phi/\mathbb{F}_{\mathfrak{p}}$ to $\psi/\mathbb{F}_{\mathfrak{p}}$. To this end, we look to the commuting relation $\iota\,\phi_x = \psi_x\,\iota$. For the ϕ, ψ arising in this context, we may assume $\Delta_\phi = \Delta_\psi = 1$. Denote $w := x \mod \mathfrak{p}$. Recall that $d = \deg(\mathfrak{p})$ is odd. We have

$$\left(\sum_{i=0}^{a} \alpha_i\tau^i\right)(\tau^2 + \mathfrak{g}_\phi\tau + w) = (\tau^2 + \mathfrak{g}_\psi\tau + w)\left(\sum_{i=0}^{a} \alpha_i\tau^i\right).$$

We will determine α_i iteratively starting with α_a. Since $\mathbb{F}_q$ commutes with τ, if there is an isogeny of the form we seek with $\alpha_i = \beta_i + \gamma_i$ for some $\gamma_i \in \mathbb{F}_q$, then there is one with $\alpha_i = \beta_i$. Therefore, at each stage it suffices to keep track of one solution for each α_i.

Comparing leading coefficients, we get $\alpha_a^{q^2} - \alpha_a = 0$. A further constraint $\alpha_a^{q^d} - \alpha_a = 0$ appears since the coefficients are in $\mathbb{F}_{\mathfrak{p}}$. The τ-degree constraint implies $\alpha_a \ne 0$. Since d is odd, we conclude $\alpha_a \in \mathbb{F}_q \setminus \{0\}$ as the set of solutions satisfying these constraints. Without loss of generality, we may set $\alpha_a = 1$. Comparing coefficients of τ^{i+2},

$$\alpha_i^{q^2} - \alpha_i = \mathfrak{g}_\psi\alpha_{i+1}^q - \mathfrak{g}_\phi^{q^i}\alpha_{i+1} + (x^{q^i} - x)\alpha_{i+2}.$$

As an induction hypothesis, assume solution spaces for $\alpha_{i+1}, \alpha_{i+2}$ are already computed as $\alpha_{i+1} = \beta_{i+1} + \mathbb{F}_q$ and $\alpha_{i+2} = \beta_{i+2} + \mathbb{F}_q$ for some $\beta_{i+1}, \beta_{i+2} \in \mathbb{F}_{\mathfrak{p}}$.

$$X^{q^2} - X = \mathfrak{g}_\psi\beta_{i+1}^q - \mathfrak{g}_\phi^{q^i}\beta_{i+1} + (x^{q^i} - x)\beta_{i+2}$$

has a root $\beta_i \in \mathbb{F}_{\mathfrak{p}}$ if and only if the right hand side has trace (from $\mathbb{F}_{\mathfrak{p}}$ to $\mathbb{F}_q$) zero. Such a solution can be found since root finding over finite fields is in randomized polynomial time. If

$\beta_i \in \mathbb{F}_{\mathfrak{p}}$ is a solution then so are $\beta_i + \mathbb{F}_{q^2}$. Since we look for solutions in $\mathbb{F}_{\mathfrak{p}}$, we take $\alpha_i = \beta_i + \mathbb{F}_q$ as our solution space. If the iterative procedure runs to completion, we have computed the isogeny we seek, else we declare failure.

Recovery of the secret: Let $\iota : \phi \,/\mathbb{F}_{\mathfrak{p}} \longrightarrow \mathfrak{s}_a \star \phi \,/\mathbb{F}_{\mathfrak{p}}$ be an isogeny of smallest τ-degree, found using the aforementioned procedure. For ℓ dividing L with $\mathbb{F}_{\mathfrak{p}}$-isogeny $\xi^{\ell} : \ell \star \psi \,/\mathbb{F}_{\mathfrak{p}} = \mathfrak{s}_a \star \phi \,/\mathbb{F}_{\mathfrak{p}}$, we can test using the right division algorithm in $\mathbb{F}_{\mathfrak{p}^2}$ [16] if ξ_x^{ℓ} right divides ι. If so, we obtain a factorization $\iota = \widehat{\iota}\, \xi_x^{\ell}$. This reduces the problem of factoring ι into a composition of L-smooth $\mathbb{F}_{\mathfrak{p}}$-isogenies to that of factoring $\widehat{\iota}$. Such a factorization of ι reveals the secret $\mathfrak{s}_a$.

References

1. Alon, N.: Eigenvalues and expanders. Combinatorica **6**, 83–96 (1983)
2. Biasse, J.F., Jao, D., Sankar, A.: A quantum algorithm for computing isogenies between supersingular elliptic curves. INDOCRYPT, Lecture Notes in Computer Science, **8885**, 428–442 (2014)
3. Castryck, W., Lange, T., Martindale, C., Panny, L., Renes, J.: Csidh: An efficient post-quantum commutative group action. ASIACRYPT : Advances in Cryptology pp. 395–427 (2018)
4. Charles, D.X., Lauter, K.E., Goren, E.Z.: Cryptographic hash functions from expander graphs. Journal of Cryptology **22(1)**, 93113 (2009)
5. Childs, A.M., Jao, D., Soukharev, V.: Constructing elliptic curve isogenies in quantum subexponential time. J. Mathematical Cryptology **8(1)**, 1–29 (2014)
6. Cornelissen, G.: Delignes congruence and supersingular reduction of drinfeld modules. Archiv der Mathematik **72(5)**, 346353 (1999)
7. Couveignes, J.M.: Hard homogeneous spaces. IACR Cryptology ePrint Archive **291** (2006), `https://ia.cr/2006/291`
8. David, C.: Average distribution of supersingular drinfeld modules. Journal of Number Theory **56(2)**, 366–380 (1996)
9. DeFeo, L., Jao, D., Plut, J.: Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. Journal of Mathematical Cryptology **8(3)**, 209247 (2014)
10. Diffie, W., Hellman, M.E.: New directions in cryptography. IEEE Trans. Information Theory **22(6)**, 644654 (1976)
11. Drinfeld, V.: Elliptic modules i. Mathematics of the USSR-Sbornik **23(4)**, 561–592 (1974)
12. Drinfeld, V.: Elliptic modules ii. Mathematics of the USSR-Sbornik **31(2)**, 159–170 (1977)
13. Gekeler, E.U.: On the coefficients of drinfeld modular forms. Inventiones mathematicae **93**, 667–700 (1988)
14. Gekeler, E.U.: On finite drinfeld modules. Journal of Algebra **141**, 187–203 (1991)
15. Gekeler, E.U.: Frobenius distributions of drinfeld modules over finite fields. Transactions of the American Mathematical Society **360**, 1695–1721 (2008)
16. Goss, D.: Basic Structures of Function Field Arithmetic. Springer
17. Jao, D., DeFeo, L.: Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. PQCrypto 2011: Post-Quantum Cryptography pp. 19–34 (2011)
18. Kuperberg, G.: A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. SIAM J. Comput. **35(1)**, 170188 (2005)
19. Lubotzky, A., Phillips, R., Sarnak, P.: Ramanujan graphs. Combinatorica **8**, 261–277 (1988)
20. Marcus, A., Spielman, D., Srivastava, N.: Interlacing families i: Bipartite ramanujan graphs of all degrees. IEEE 54th Annual Symposium. Foundations of Computer Science (FOCS) (2013)
21. Morgenstern, M.: Existence and explicit constructions of q+1 regular ramanujan graphs for every prime power q. Journal of Combinatorial Theory, Series B. **62**, 44–62 (1994)
22. Morgenstern, M.: Natural bounded concentrators. Combinatorica **15(1)**, 111–122 (1995)
23. Nilli, A.: On the second eigenvalue of a graph. Discrete Math. **1991**, 207–210 (91(2)

24. Papikian, M.: Graph laplacians, component groups and drinfeld modular curves. Munster Journal of Mathematics **9**, 221–251 (2016)
25. Pizer, A.K.: Ramanujan graphs and hecke operators. Bulletin of the American Mathematical Society **23(1)**, 127–137 (1990)
26. Regev, O.: A subexponential time algorithm for the dihedral hidden subgroup problem with polynomial space (2004), `https://arxiv.org/abs/quant-ph/0406151.`
27. Rostovtsev, A., Stolbunov, A.: Public-key cryptosystem based on isogenies. IACR Cryptology ePrint Archive **145** (2006), `https://ia.cr/2006/145`
28. Scanlon, T.: Public key cryptosystems based on Drinfeld modules are insecure. Journal of Cryptology **14**, 225–230 (2001)
29. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput. **26(5)**, 14841509 (1997)
30. Yu, J.: Isogenies of drinfeld modules over finite fields. Journal of Number Theory **54(1)**, 161–171 (1995)