DRINFELD MODULES MAY NOT BE FOR ISOGENY BASED CRYPTOGRAPHY

ANTOINE JOUX AND ANAND KUMAR NARAYANAN

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. Couveignes calls it the "hard homogenous space" problem, a twist on the Diffie-Hellman problem [10]. 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, isogenous supersingular elliptic curves do not admit a free transitive action by an abelian group. To overcome this 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 on supersingular elliptic curves. They accomplish this by restricting

This work has been supported by the European Union's H2020 Programme under grant agreement number ERC-669891.

to isogenies defined over the field of definition of the curves; which ensures a commutative endomorphism ring. 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 homogenous space problem can be phrased as a hidden shift problem amenable to Kuperberg's and Regev's algorithms [22, 26, 1, 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 worrying [14]. In CSIDH/Couveignes-Rostovtsev-Stolbunov, the public key is just an elliptic curve, no points are published.

Drinfeld introduced the modules bearing his name as analogues of elliptic curve complex multiplication theory [12, 13]. 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. For instance, we present algorithms for constructing supersingular Drinfeld modules with a prescribed rational torsion over finite fields; relying on Gekeler's Drinfeld analogue of Deligne's congruence.

We focus 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. After posting a preprint, we were informed of an algorithm for computing ordinary Drinfeld module isogeny volcanoes in the PhD thesis of Caranay [2][Alg 8.5.4, Thm 8.5.8] similar to our Drinfeld CSIDH cryptanalysis. While both algorithms rely on the polynomial system ([2][eqns. 8.39]) resulting from the commutation relation of the isogenies, ours is iterative.

Organization: In § 2, we introduce Drinfeld modules and build notation. The following section § 3 is devoted to developing the main objects for our constructions; supersingular Drinfeld modules and isogenies connecting them. Unless otherwise noted, statements/claims made in the first three sections can be found in standard references such as [16, 18] (see also [2]). The Drinfeld module analogues of CSIDH and SIDH are devised in § 4 and broken in § 5.

2. Drinfeld Modules Preliminaries

2.1. **Rank-2 Drinfeld modules.** Let $\mathbb{F}_q$ denote the finite field with q elements. Let $\mathbb{F}_q[x]$ denote the polynomial ring in one indeterminate x and $\mathbb{F}_q(x)$ 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

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

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

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

for some $\mathfrak{f}_{\phi,i} \in K$. It is convenient to use subscripts to denote images and denote by $\phi_\mathfrak{f}$ the image of $\mathfrak{f}$ under ϕ. Here on, unless otherwise noted, a Drinfeld module will mean a rank-2 Drinfeld module. When the field of definition K is clear from context, we write ϕ instead of $\phi\,/K$. To explicitly describe ϕ, we write $\phi = (\mathfrak{g}_\phi, \Delta_\phi)$.

Drinfeld modules over rational function fields: Take K to be $\mathbb{F}_q(x)$ and set γ to the inclusion $\gamma : \mathbb{F}_q[x] \hookrightarrow \mathbb{F}_q(x)$ to obtain Drinfeld modules $\phi\,/\mathbb{F}_q(x)$ over $\mathbb{F}_q(x)$ of the form $\phi : \mathbb{F}_q[x] \longrightarrow \mathbb{F}_q(x)\langle\tau\rangle$ mapping $x \longmapsto x + \mathfrak{g}_\phi(x)\tau + \Delta_\phi(x)\tau^2$ for some $\mathfrak{g}_\phi(x) \in \mathbb{F}_q(x)$ and $\Delta_\phi(x) \in \mathbb{F}_q(x)^\times$.

Drinfeld modules over finite fields: For a monic irreducible $\mathfrak{p} \in \mathbb{F}_q[x]$ of degree $\deg(\mathfrak{p}) > 0$, denote $\mathbb{F}_\mathfrak{p} := \mathbb{F}_q[x]/(\mathfrak{p}(x)) \cong \mathbb{F}_{q^{\deg(\mathfrak{p})}}$. 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 to yield Drinfeld modules $\phi\,/\mathbb{F}_\mathfrak{p}$ over $\mathbb{F}_\mathfrak{p}$ of the form $\phi : \mathbb{F}_q[x] \longrightarrow \mathbb{F}_\mathfrak{p}\langle\tau\rangle$ mapping $x \longmapsto (x \mod \mathfrak{p}) + \mathfrak{g}_\phi\tau + \Delta_\phi\tau^2$ 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 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 elliptic curve arithmetic, 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 $\mathfrak{f} \in \mathbb{F}_q[x]$ and $\alpha \in M$, define the scalar multiplication $\mathfrak{f} \circ \alpha := \phi_\mathfrak{f}(\alpha)$. Let $\phi(M)$ denote the new $\mathbb{F}_q[x]$ module structure thus endowed to M.

Example 2.1. The module $\phi(\mathbb{F}_\mathfrak{p})$ endowed by a Drinfeld module $\phi\,/\mathbb{F}_\mathfrak{p}$ on the $\mathbb{F}_q[x]$-algebra $\mathbb{F}_\mathfrak{p}$ plays 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. Here, the twisted scalar multiplication is; for $\mathfrak{f} \in \mathbb{F}_q[x]$ and $\alpha \in \mathbb{F}_\mathfrak{p}$, $\mathfrak{f} \circ \alpha := \phi_\mathfrak{f}(\alpha) = (\mathfrak{f} \mod \mathfrak{p})\ \alpha + \sum_{i=1}^{2\deg(\mathfrak{f})} \mathfrak{f}_{\phi,i}\alpha^{q^i}$ 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 from the extra summation on the right.

Euler-Poincaré Characteristic: 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 such that

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

The likeness to the cardinality of a $\mathbb{Z}$-module is apparent; the cardinality of a cyclic group of prime order is the corresponding prime: and the cardinality of finite abelian groups that sit in an exact sequence is multiplicative.

2.3. **Morphisms of Drinfeld Modules.** Let $\phi\,/K$ and $\psi\,/K$ be two Drinfeld modules over a field K. An L-morphism $\iota : \phi\,/K \longrightarrow \psi\,/K$ defined over a field extension L/K 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 $\iota\ \phi_x = \psi_x\ \iota$. A morphism ι defines a morphism of group schemes over K commuting with $\mathbb{F}_q[x]$-action.

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

Example 2.2. 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 $\mathfrak{b} \in \mathbb{F}_q[x]$ 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 $\tau^{\deg(\mathfrak{p})}$, implying the inclusion $\mathbb{F}_q[x][\tau^{\deg(\mathfrak{p})}] \hookrightarrow End_{\mathbb{F}_\mathfrak{p}}(\phi)$.

For a Drinfeld module ϕ 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.

2.4. **Characteristic Polynomial of Frobenius.** Let ϕ be a Drinfeld module over a finite extension K of $\mathbb{F}_\mathfrak{p}$. 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 [16] showed that the characteristic polynomial $P_\phi(X) \in \mathbb{F}_q[x, X]$ 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 [15]) is of the form

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

where $\epsilon_\phi := (-1)^{[K:\mathbb{F}_\mathfrak{p}]\deg(\mathfrak{p})}/Norm_{K/\mathbb{F}_q}(\Delta_\phi) \in \mathbb{F}_q^\times$ 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 $P_\phi(\tau^{\deg \mathfrak{p}}) = \tau^{2\deg \mathfrak{p}} - Tr_\phi \tau^{\deg \mathfrak{p}} + \epsilon_\phi \mathfrak{p} = 0$. Two Drinfeld modules $\phi\,/\mathbb{F}_\mathfrak{p}, \psi\,/\mathbb{F}_\mathfrak{p}$ over K are K-isogenous if there is a K-isogeny $\iota : \phi\,/\mathbb{F}_\mathfrak{p} \longrightarrow \psi\,/\mathbb{F}_\mathfrak{p}$. Although not apparent, being K-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 K-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. The absolute j-invariant of a Drinfeld module ϕ over K is defined as $j(\phi) := \mathfrak{g}_\phi^{q+1}/\Delta_\phi$. Drinfeld modules ϕ and ψ over K are $\overline{\mathbb{F}}_\mathfrak{p}$-isomorphic if and only if $j(\phi) = j(\psi)$.

3. Supersingular Drinfeld Modules

Recall that a Drinfeld module ϕ over a finite extension of $\mathbb{F}_\mathfrak{p}$ 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 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 $\mathbb{F}_{\mathfrak{p}^2}$ (up to $\overline{\mathbb{F}}_\mathfrak{p}$-isomorphism) [16][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: The Hasse invariant $h_\phi \in \mathbb{F}_{\mathfrak{p}^2}$ of $\phi\,/\mathbb{F}_{\mathfrak{p}^2}$ is the coefficient of $\tau^{\deg(\mathfrak{p})}$ in the expansion $\phi_\mathfrak{p} = \sum_{i=0}^{2\deg(\mathfrak{p})} h_i \tau^i \in \mathbb{F}_{\mathfrak{p}^2}\langle\tau\rangle$. It provides an alternate characterization of supersingularity; $\phi\,/\mathbb{F}_{\mathfrak{p}^2}$ is supersingular if and only if $h_\phi = 0$ [15]. In fact, for supersingular $\phi\,/\mathbb{F}_{\mathfrak{p}^2}$ [16][Prop. 4.1], $\phi_\mathfrak{p} = Norm_{\mathbb{F}_{\mathfrak{p}^2}/\mathbb{F}_q}(\Delta_\phi)\tau^{2\deg(\mathfrak{p})}$.

3.1. **Torsion Submodules.** For a monic $\mathfrak{m} \in \mathbb{F}_q[x]$ 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 $\Lambda_\phi[\mathfrak{m}] \cong \mathbb{F}_q[x]/(\mathfrak{m}) \oplus \mathbb{F}_q[x]/(\mathfrak{m})$.

Lemma 3.1. *Let $\phi/\mathbb{F}_{\mathfrak{p}^2}$ be supersingular. 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 $\lambda_1 \in \phi(\mathbb{F}_{\mathfrak{p}})$, $\lambda_{-1} \in \phi(\mathbb{F}_{\mathfrak{p}^2})$ such that $\Lambda_\phi[\mathfrak{m}] = \langle\lambda_1\rangle \oplus \langle\lambda_{-1}\rangle$ as $\mathbb{F}_q[x]$-modules.*

Proof. Since ϕ is supersingular, the Frobenius $\tau^{\deg(\mathfrak{p})}$ has trace Tr_ϕ zero and characteristic polynomial $P_\phi(X) = X^2 + \epsilon_\phi\mathfrak{p}$. Since $\mathfrak{m}$ divides the Euler-Poincaré characteristic $\chi(\phi(\mathbb{F}_{\mathfrak{p}})) = P_\phi(1) = 1 + \epsilon_\phi\mathfrak{p}$, $P_\phi(X)$ factors modulo $\mathfrak{m}$ as

$$P_\phi(X) \mod \mathfrak{m} = X^2 + \epsilon\mathfrak{p} \mod \mathfrak{m} = X^2 - 1 \mod \mathfrak{m} = (X-1)(X+1) \mod \mathfrak{m}.$$

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

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 $\{\lambda_1, \mu_{-1}\}$ (by Drinfeld module discrete logarithms [28]), we can extract λ_{-1}.

3.2. **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 Gekeler's isogeny norm [16]. For example, the isogeny $\phi_{\mathfrak{f}} : \phi/\mathbb{F}_{\mathfrak{p}} \to \phi/\mathbb{F}_{\mathfrak{p}}$ for a monic $\mathfrak{f} \in \mathbb{F}_q[x]$ has $\deg(\phi_{\mathfrak{f}}) = \mathfrak{f}^2$. An isogeny ι with $\deg(\iota) = \mathfrak{f} \in \mathbb{F}_q[x]$ 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-isogeny: Recall from lemma 3.1 that the characteristic polynomial of the Frobenius $\tau^{\deg(\mathfrak{p})}$ factors modulo ℓ as $P_\phi(X) = (X-1)(X+1) \mod \ell$ 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 [18][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^Λ_ℓ of ℓ. By construction, $\iota_\Lambda\ \phi_\ell = \phi^\Lambda_\ell\ \iota_\Lambda$, which along with ℓ being of degree 1 implies $\iota_\Lambda\ \phi_{\mathfrak{f}} = \phi^\Lambda_{\mathfrak{f}}\ \iota_\Lambda, \quad \forall \mathfrak{f} \in \mathbb{F}_q[x]$ 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 $\chi\left((\ell^{a-1}\star\phi/\mathbb{F}_{\mathfrak{p}})(\mathbb{F}_{\mathfrak{p}})\right)$. Moreover, 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-isogenies and more generally ℓ-power and smooth degree isogenies is discussed at the end of §4.2.

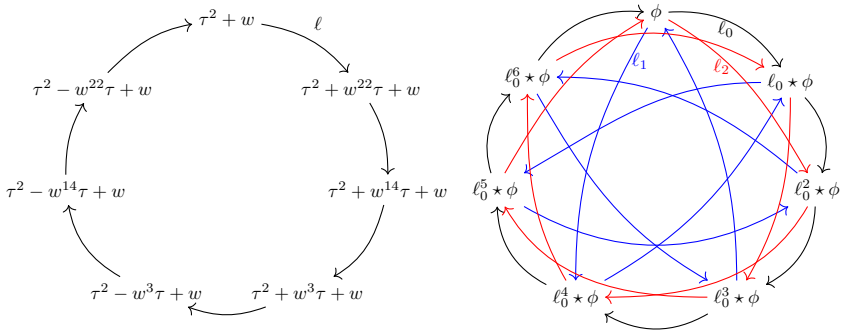
3.3. **$\mathbb{F}_{\mathfrak{p}}$-restricted Isogeny graph:** Let $\phi/\mathbb{F}_{\mathfrak{p}}$ be a supersingular Drinfeld module. The $\mathbb{F}_{\mathfrak{p}}$-endomorphism ring $End_{\mathbb{F}_{\mathfrak{p}}}(\phi)$ is an order in the imaginary quadratic extension $\mathbb{F}_q(x)(\sqrt{D_\phi})$ 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 $\mathbb{F}_q[x][\pi]$ [17][Prop. 6.8][31]; $\sum_{\psi/\mathbb{F}_{\mathfrak{p}}} \frac{1}{|Aut_{\mathbb{F}_{\mathfrak{p}}}(\psi)|} = h(\mathbb{F}_q[x][\sqrt{D_\phi}])$. 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. [17],[8][Lem.4.2]), the count is roughly $\sqrt{|\mathbb{F}_{\mathfrak{p}}|}$ [2]. 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 squarefree, $G_{\phi,\ell}$ 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 3.2. 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 (left), 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 3.3. 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 above (right). 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 3.2 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 [16][Thm. 4.3]. Two characteristic $\mathfrak{p}$ Drinfeld modules over $\mathbb{F}_{\mathfrak{p}^2}$ are $\mathbb{F}_{\mathfrak{p}^2}$-isogenous (c.f. [16][Thm 3.5, Prop. 4.1]) and

the supersingular ℓ-isogeny graph $G^{ss}_{\mathfrak{p},\ell}$ is a connected $q^{\deg(\ell)}+1$ regular graph with roughly $q^{\deg(\mathfrak{p})}$ vertices.

Supersingular Isogeny Ramanujan Diagrams: Isogeny graphs of supersingular elliptic curves are the setting of the De Feo-Jao-Plût post-quantum cryptosystem [19, 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 [23][Thm 2.1]), supersingular Drinfeld modules yield Ramanujan diagrams. Our supersingular ℓ-isogeny graph $G^{ss}_{\mathfrak{p},\ell}$ is the finite part of such a Ramanujan diagram and has optimal spectral expansion [24][Thm. 4.8].

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 schemes etc. We refrain from optimizing the implementations, for all these protocols will be broken in the subsequent section. The cryptosystems can be built over an arbitrary sequence of finite fields $\mathbb{F}_{q^d}$ of increasing cardinality. The security parameter in the CSIDH and SIDH analogues are respectively $\log(q^{d/2})$ and $\log(q^d)$. The protocols and the algorithms breaking them, all run in time polynomial in $\log q$ and d. The prospect of cryptosystems over Drinfeld modules of rank higher than two remains to be explicated. Yet, our cryptanalytic algorithms strongly suggest that the very mechanism that enables key exchange (for larger ranks) will likely make it vulnerable to our cryptanalysis.

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 build the Schreier graph $G_{\phi,L}$ with about $q^{d/2}$ vertices, 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 $\chi(\phi(\mathbb{F}_{\mathfrak{p}}))$.

Our recipe to is to choose an $\epsilon \in \mathbb{F}_q^{\times}$, 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 $\mathfrak{p}$ to $\mathfrak{b}(\prod_{\ell\in L}\ell)+1/\epsilon$, if it is irreducible. A random degree d polynomial is irreducible with probability roughly $\Theta(1/d)$ (for large enough q). Assuming (heuristically) polynomials of the form $\mathfrak{b}(\prod_{\ell\in L}\ell)+1/\epsilon$ is pseudorandom, co-factor degree $d-|L| >> \log_q(d)$ should suffice to hit an irreducible. We then call the complex multiplication method from [11][§ 3] to choose a Drinfeld module $\phi\big/\mathbb{F}_{\mathfrak{p}}$ with Euler-Poincaré characteristic $\chi(\phi(\mathbb{F}_{\mathfrak{p}})) = 1+\epsilon\mathfrak{p}$. The strategy in [11] is to pick $c \in \mathbb{F}_q$ at random, construct a Drinfeld module over $\mathbb{F}_q(x)$ with complex multiplication by $\mathbb{F}_q(x)(\sqrt{x-c})$. With probability roughly half, the reduction is supersingular at $\mathfrak{p}$. For odd $\deg(p)$, we propose a clean alternative to [11][§ 3]. Set $\epsilon = -1$ and choose the Drinfeld module with zero absolute j-invariant; as detailed in the following lemma (implicit in [15, 6]).

Lemma 4.1. *For odd* $\deg(\mathfrak{p})$*, the Drinfeld module* $\phi\,/\mathbb{F}_{\mathfrak{p}}$ *with* $\phi_x := \tau^2 + (x \mod \mathfrak{p})$ *is supersingular with Euler-Poincaré characteristic* $\chi(\phi(\mathbb{F}_{\mathfrak{p}})) = 1 - \mathfrak{p}$.

Proof. For a $\phi = (\mathfrak{g}_\phi, \Delta_\phi)$, 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 [17, 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 $h_\phi = r_{\phi,\deg(\mathfrak{p})} \mod \mathfrak{p}$. Consider the odd degree case. Substituting $g_\phi = 0$ and $\Delta_\phi = 1$ in the recurrence, we see $r_{\phi,\deg(\mathfrak{p})} = \prod_{i=1}^{\deg(\mathfrak{p})/2} \left(x^{q^{2i-1}} - x\right)$ if $\deg(\mathfrak{p})$ is even and zero otherwise. Since no even degree irreducible polynomials divide $x^{q^m} - x$ for odd m, the Hasse invariant $h_\phi (= r_{\phi,\deg(\mathfrak{p})} \mod \mathfrak{p})$ is 0 if and only if $\deg(\mathfrak{p})$ is odd. □

Remark 4.2. For an odd prime q, we propose a particularly clean polynomial selection recipe using Artin-Schreier extensions for $d = q$. 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 $\chi(\phi(\mathbb{F}_{\mathfrak{p}})) = 1 - \mathfrak{p}$.

Key Generation/Exchange: As public parameters, we have a 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 $\chi(\phi(\mathbb{F}_{\mathfrak{p}}))$. 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. 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 share 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 [19, 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 first three requirements are met by the construction in § 4.1 and the last by the algorithms in § 3.2. The resulting full $\overline{\mathbb{F}}_{\mathfrak{p}}$-isogeny graphs $G_{\mathfrak{p},\ell}^{ss}$, $\ell \in L$, 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 irreducibles, 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 $\mathfrak{f}$. There is 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 $q = d$ is an odd prime. Then by Artin-Schreier theory $\mathfrak{p}(x) = x^q - x + 1$ is irreducible and by lemma 4.1, the starting supersingular Drinfeld module may be chosen as $\phi_x = \tau^2 + (x \mod \mathfrak{p})$.

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

On receiving $\phi^B \,/\mathbb{F}_{\mathfrak{p}^2}, \iota_B(\lambda_1^A), \iota_B(\lambda_{-1}^A)$ from Bob, Alice constructs the 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 isogeny $\widehat{\iota}_B : \phi^A \,/\mathbb{F}_{\mathfrak{p}^2} \longrightarrow \phi^{B \circ A} \,/\mathbb{F}_{\mathfrak{p}^2}$ with kernel $\langle \phi^A_{\mathfrak{m}_B} \iota_A(\lambda_1^B) + \phi^A_{\mathfrak{n}_B} \iota_A(\lambda_{-1}^B) \rangle$.

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

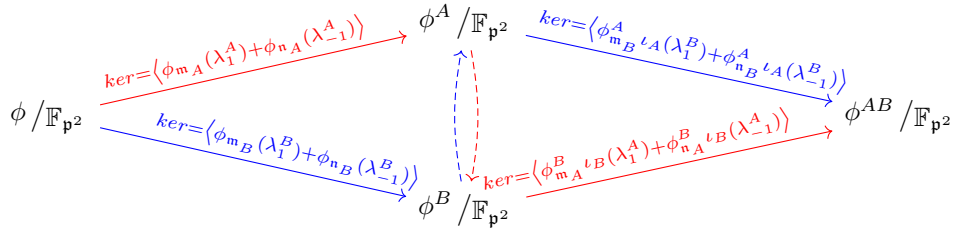
$$ker(\widehat{\iota}_A) = \langle \phi^B_{\mathfrak{m}_A} \iota_B(\lambda_1^A) + \phi^B_{\mathfrak{n}_A} \iota_B(\lambda_{-1}^A) \rangle = \langle \iota_B \phi_{\mathfrak{m}_A}(\lambda_1^A) + \iota_B \phi_{\mathfrak{n}_A}(\lambda_{-1}^A) \rangle.$$

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,

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

where the second equality follows by symmetry. 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 Alice's computation/communication and blue lines to Bob's.



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

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

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

The first isogeny ι_0 is built by choosing some prime ℓ_0 dividing $\mathfrak{c}_A$ and taking ι_0 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 isogeny sequence with $b := \deg(\mathfrak{c}_B)$

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

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

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. 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 $\phi^A/\mathbb{F}_{\mathfrak{p}^2}$. 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 $\phi^A \big/ \mathbb{F}_{\mathfrak{p}^2}, \iota_A(\lambda_1^B), \iota_A(\lambda_{-1}^B)$ 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 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;

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

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

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

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

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

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

with the coefficients α_i as variables. By construction, since $\deg(\mathfrak{c}_B) \geq \deg(\mathfrak{c}_A)$, 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 seeking an explicit path in the isogeny graph from $\phi/\mathbb{F}_{\mathfrak{p}^2}$ to $\phi^A/\mathbb{F}_{\mathfrak{p}^2}$. 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 path finding 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 $\mathbb{F}_{\mathfrak{p}^2}\langle\tau\rangle$ [18][chap.1.6]

5.2. **Cryptanalysis of the Drinfeld analogue of CSIDH.** Keeping the notation as in § 5.2, we show how to recover Alice's secret key $\mathfrak{s}_a$ given her public key $\mathfrak{s}_a \star \phi/\mathbb{F}_{\mathfrak{p}}$. Consequently, the computational Diffie-Hellman version of computing $\mathfrak{s}_{ab}\star\phi/\mathbb{F}_{\mathfrak{p}}$ given $\mathfrak{s}_a\star\phi/\mathbb{F}_{\mathfrak{p}}$ and $\mathfrak{s}_b\star\phi/\mathbb{F}_{\mathfrak{p}}$ is also solved.

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 $\iota\ \phi_x = \psi_x\ \iota$. Assume $d = \deg(\mathfrak{p})$ is odd, the even case is similar (c.f. [2][Alg. 8.5.4]). For the ϕ, ψ arising in this context, we may assume $\Delta_\phi = \Delta_\psi = 1$. Denote $w := x \mod \mathfrak{p}$. 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 $\alpha_a \neq 0$. Since d is odd, $\alpha_a \in \mathbb{F}_q \setminus \{0\}$ is the set of solutions satisfying these constraints and we may set $\alpha_a = 1$ without loss of generality. 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. 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 $\mathbb{F}_{\mathfrak{p}}$ and d is odd, we take $\alpha_i = \beta_i + \mathbb{F}_q$ as our solution space. Each root finding step takes expected time nearly linear in dq^2: using the von zur Gathen-Shoup iterated Frobenius algorithm [30] to raise to high q-powers modulo $\mathfrak{p}$ and Kaltofen-Shoup [20] for root finding in high degree extensions (implemented using the Kedlaya-Umans [21] modular composition). For q far bigger than d, to ensure runtime polynomial in $d\log q$, (on the left) compute $X^{q^2} - X \mod \mathfrak{p}(X)$ by repeated squaring/iterated Frobenius, lift to $\mathbb{F}_q[X]$, then deploy root finding. If the iterative procedure terminates, we have the sought isogeny. Else, declare non existence.

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 $\mathbb{F}_{\mathfrak{p}^2}$ [18] 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] J-F Biasse, D. Jao, and A. Sankar. A quantum algorithm for computing isogenies between supersingular elliptic curves. *INDOCRYPT, LNCS*, 8885:428–442, 2014.

[2] Perlas Caranay. Computing isogeny volcanoes of rank two drinfeld modules. *PhD Thesis, University of Alberta, Calgary*, 2018.

[3] W. Castryck, T. Lange, C. Martindale, L. Panny, and J. Renes. Csidh: An efficient post-quantum commutative group action. *ASIACRYPT*, pages 395–427, 2018.

[4] D. X. Charles, K. E. Lauter, and E. Z. Goren. Cryptographic hash functions from expander graphs. *Journal of Cryptology*, 22(1):93113, 2009.

[5] A. M. Childs, D. Jao, and V. Soukharev. Constructing elliptic curve isogenies in quantum subexponential time. *J. Mathematical Cryptology*, 8(1):1–29, 2014.

[6] G. Cornelissen. Delignes congruence and supersingular reduction of drinfeld modules. *Archiv der Mathematik*, 72(5):346353, 1999.

[7] J-M Couveignes. Hard homogeneous spaces. *IACR Cryptology ePrint Archive*, 291, 2006.

[8] C. David. Average distribution of supersingular drinfeld modules. *Journal of Number Theory*, 56(2):366–380, 1996.

[9] L. DeFeo, D. Jao, and J. Plut. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *Journal of Mathematical Cryptology*, 8(3):209247, 2014.

[10] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Trans. Information Theory*, 22(6):644654, 1976.

[11] J. Doliskani, A.K.Narayanan, and É. Schost. Drinfeld modules with complex multiplication, hasse invariants and factoring polynomials over finite fields. *preprint*, 2017.

[12] V.I. Drinfeld. Elliptic modules i. *Mathematics of the USSR-Sbornik*, 23(4):561–592, 1974.

[13] V.I. Drinfeld. Elliptic modules ii. *Mathematics of the USSR-Sbornik*, 31(2):159–170, 1977.

[14] S.D. Galbraith, C. Petit, B. Shani, and Y.B. Ti. On the security of supersingular isogeny cryptosystems. *ASIACRYPT*, pages 63–91, 2016.

[15] E.-U. Gekeler. On the coefficients of drinfeld modular forms. *Inventiones mathematicae*, 93:667–700, 1988.

[16] E.-U. Gekeler. On finite drinfeld modules. *Journal of Algebra*, 141:187–203, 1991.

[17] E.-U. Gekeler. Frobenius distributions of drinfeld modules over finite fields. *Transactions of the American Mathematical Society*, 360:1695–1721, 2008.

[18] D. Goss. *Basic Structures of Function Field Arithmetic*. Springer.

[19] D. Jao and L. DeFeo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *PQCrypto 2011: Post-Quantum Cryptography*, pages 19–34, 2011.

[20] E. Kaltofen and V. Shoup. Fast polynomial factorization over high algebraic extensions of finite fields. *Internat. Symp. Symbolic Algebraic Comput. (ISSAC'97)*, pages 184–188, 1997.

[21] K. Kedlaya and C. Umans. Fast modular composition in any characteristic. *IEEE Symposium on Foundations of Computer Science (FOCS)*, 49:146–165, 2008.

[22] G. Kuperberg. A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. *SIAM J. Comput.*, 35(1):170188, 2005.

[23] M. Morgenstern. Natural bounded concentrators. *Combinatorica*, 15(1):111–122, 1995.

[24] M. Papikian. Graph laplacians, component groups and drinfeld modular curves. *Munster Journal of Mathematics*, 9:221–251, 2016.

[25] A. K. Pizer. Ramanujan graphs and hecke operators. *Bulletin of the American Mathematical Society*, 23(1):127–137, 1990.

[26] O. Regev. A subexponential time algorithm for the dihedral hidden subgroup problem with polynomial space. 2004.

[27] A. Rostovtsev and A. Stolbunov. Public-key cryptosystem based on isogenies. *IACR Cryptology ePrint Archive*, 145, 2006.

[28] T. Scanlon. Public key cryptosystems based on Drinfeld modules are insecure. *Journal of Cryptology*, 14:225–230, 2001.
[29] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):14841509, 1997.
[30] J. von zur Gathen and V. Shoup. Computing frobenius maps and factoring polynomials. *Comput. Complexity*, 2:187–224, 1992.
[31] J.K. Yu. Isogenies of drinfeld modules over finite fields. *Journal of Number Theory*, 54(1):161–171, 1995.

CISPA Helmholtz Center for Information Security Stuhlsatzenhaus 5, Saarland Informatics Campus 66123 Saarbrücken, Germany.
E-mail address: Antoine.Joux@m4x.org

Sorbonne Université, Institut de Mathématiques de Jussieu–Paris Rive Gauche, CNRS, INRIA, Univ Paris Diderot, Campus Pierre et Marie Curie, F-75005 Paris, France.
E-mail address: anand.narayanan@lip6.fr