FROM ORIENTATIONS TO ℓ-ADIC PERIOD VECTORS

LEONARDO COLÒ

Abstract. We propose a bridge between oriented supersingular elliptic curves and the arithmetic topology of modular curves. To an $\mathcal{O}$-oriented supersingular curve, we attach a class in the relative homology group $H(X_0(N), C, \mathbb{Z})$, i.e. modular symbols, compatible with the Hecke action. We then compute vectors of ℓ-adic periods by pairing with weight-2 cusp forms via Coleman integration. This yields an explicit, computable map from short combinatorial homology representatives to truncated vectors in $(\mathbb{Z}/\ell^m\mathbb{Z})^d$. Motivated by this encoding, we formulate the Modular Symbol Inversion (MSI) problem –recovering a short homology representative from its truncated ℓ-adic period data– and discuss its arithmetic structure, its relation to path problems on isogeny graphs and Bruhat–Tits trees, and potential applications to cryptographic constructions.

1. Introduction

Isogeny-based cryptography has emerged as one of the most promising families of post-quantum public-key primitives, with schemes based on supersingular elliptic curves, quaternion algebras, and class group actions. Constructions such as CSIDH [8], OSIDH [12], SQISign [21], and their variants exploit the rich arithmetic, geometry and combinatorial structure of supersingular isogeny graphs to obtain compact keys and protocols with conjectured post-quantum security.

In parallel, arithmetic geometers have long used modular symbols and ℓ-adic integration to study modular forms, modular curves, and the arithmetic of elliptic curves. The modular-symbol formalism packages the homology on the modular curve $X_0(N)$ in a combinatorial way, while overconvergent modular symbols and harmonic cocycles on the Bruhat–Tits tree provide effective algorithms for computing ℓ-adic periods and ℓ-adic L-values without explicit projective models of the curves.

The central idea of this work is to use modular symbols and ℓ-adic integrals as an interface between oriented supersingular elliptic curves and discrete ℓ-adic data. Concretely, we propose to attach to an orientation

$$\iota : \mathcal{O} \hookrightarrow \mathrm{End}(E)$$

a homology class

$$\gamma(\iota) \in H_1\big(X_0(N), \{\text{cusps}\}; \mathbb{Z}\big)$$

via a class-group action on homology, and then to evaluate $\gamma(\iota)$ against weight-2 cusp forms by Coleman integration to obtain a truncated ℓ-adic period vector

$$\Pi_m(\gamma(\iota)) \in (\mathbb{Z}/\ell^m)^d.$$

This yields the algebraic–analytic pipeline

(1)
$$\iota \longmapsto [\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O}) \xrightarrow{\rho} \gamma([\mathfrak{a}]) \in H_1(X_0(N), C; \mathbb{Z}) \xrightarrow{\Pi_m} \Pi_m(\gamma([\mathfrak{a}])) \in (\mathbb{Z}/\ell^m\mathbb{Z})^d,$$

where C denotes the cusp set and ρ is a homological representation of the ideal class group $\mathrm{Pic}(\mathcal{O})$.

From a cryptographic perspective, this suggests a new family of hard problems and primitives, distinct from but morally related to the supersingular isogeny path problem and to lattice-based SIS/LWE. We highlight the following informal hardness assumption:

Modular Symbol Inversion (MSI). *Given a truncated ℓ-adic period vector $y \in (\mathbb{Z}/\ell^m\mathbb{Z})^d$ known to be of the form $y = \Pi_m(\gamma^\star)$ for some "short" homology class $\gamma^\star$ (with bounded path complexity), find any homology class γ of comparable complexity such that $\Pi_m(\gamma) = y$.*

The MSI problem is encoded in the last part of (1); the supersingular/orientation and ideal-class layers simply provide one way to sample short homology classes in a structured arithmetic way. This new assumption is supported by the exponential combinatorial complexity of homology paths and the absence of known subexponential attacks.

2. Supersingular elliptic curves and orientations

In this section we recall basic facts about supersingular elliptic curves, orders in imaginary quadratic fields, and orientations. We emphasize the parametrization of oriented supersingular curves by ideal classes in an order $\mathcal{O}$, which underlies OSIDH [12] and related constructions.

2.1. Elliptic curves and isogenies.

We refer to [57] for a complete treatment. Throughout this work we fix a field k of positive characteristic p. When $p > 3$, an elliptic curve E over k is defined by a Weierstraß model

$$E : y^2 = x^3 + Ax + B, \qquad A, B \in k,$$

with non-vanishing discriminant $\Delta = -16(4A^3 + 27B^2) \neq 0$. The set of k-rational points

$$E(k) = \{(x, y) \in k^2 : y^2 = x^3 + Ax + B\} \cup \{O_E\}$$

forms an abelian group under the usual chord–tangent law, with O_E as the neutral element.

The j-invariant of an elliptic curve E in the above model is

$$j(E) = 1728 \cdot \frac{4A^3}{4A^3 + 27B^2},$$

and two elliptic curves over $\overline{k}$ are isomorphic if and only if they have the same j-invariant.

A separable isogeny between two elliptic curves defined over k is a non-constant morphism of curves $\varphi : E_1 \longrightarrow E_2$ that is also a group homomorphism sending O_{E_1} to O_{E_2}. Its degree $\deg(\varphi)$ is its degree as a rational map. Isogenies compose, and

every non-constant isogeny of degree $n > 1$ factors into a composition of isogenies of prime degree whose product equals n.

When φ has degree coprime to p, it is uniquely determined by its kernel $\ker(\varphi) \subset E_1(\overline{k})$. Conversely, every finite subgroup $G \subseteq E_1(\overline{k})$ of order coprime to p defines a separable isogeny $\varphi_G : E_1 \to E_1/G$, and φ_G can be computed efficiently using Vélu's formulas [63].

Supersingular elliptic curves and their endomorphisms. An elliptic curve E/k is supersingular if it has no nontrivial p-torsion over $\overline{\mathbb{F}}_p$, i.e., $E(\overline{\mathbb{F}}_p)[p] = 0$. More analytically, supersingular curves are characterized by the fact that their Newton polygon is a line segment of slope $1/2$, see [52].

A fundamental theorem of Deuring [22] states that if E is supersingular over $\overline{\mathbb{F}}_p$, then the $\mathbb{Q}$-algebra

$$\mathrm{End}^0(E) := \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$$

is the quaternion algebra $\mathfrak{A}_{p,\infty}$ ramified precisely at p and ∞. Moreover, $\mathrm{End}(E)$ is a maximal order R inside $\mathfrak{A}_{p,\infty}$.

2.2. **Orders and orientations.** We define the notion of orientation on supersingular elliptic curves following [12]. Let K be an imaginary quadratic field, and let $\mathcal{O}_K$ be its ring of integers. An *order* in K is a subring $\mathcal{O} \subseteq \mathcal{O}_K$ of finite index such that $\mathcal{O}$ is a free $\mathbb{Z}$-module of rank 2. Every order has the form

$$\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$$

for some integer $f \geq 1$, called the conductor. We will write $\mathcal{O} = \mathcal{O}_f$ when we wish to emphasize the conductor.

Definition 1. A K-orientation on a supersingular elliptic curve E/k is a homomorphism $\iota : K \to \mathrm{End}^0(E)$. Let $\mathcal{O} \subset \mathcal{O}_K$ be an order in K. If $\iota(\mathcal{O}) \subseteq \mathrm{End}(E)$, then ι is said to be an $\mathcal{O}$-orientation. We say that the orientation is primitive if

$$\iota(\mathcal{O}) = \iota(K) \cap \mathrm{End}(E),$$

i.e. if $\mathcal{O}$ is the largest quadratic order mapping inside $\mathrm{End}(E)$ via ι.

We will always assume optimal orientations, and we will work up to oriented isomorphism; two oriented supersingular elliptic curves (E, ι) and (E', ι') are isomorphic if there exists an isomorphism $\phi : E \to E'$ such that

$$\phi \circ \iota(a) = \iota'(a) \circ \phi \quad \text{for all } a \in \mathcal{O}$$

A result of Onuki shows that there exists an embedding $K \hookrightarrow \mathrm{End}^0(E)$ if and only if p is either inert or ramified in K, [49]. In this case there is a unique order $\mathcal{O} \subseteq \mathcal{O}_K$ such that $\iota(\mathcal{O}) = \iota(K) \cap \mathrm{End}(E)$; hence optimal orientations arise naturally from the arithmetic of p in K.

The endomorphism ring $\mathrm{End}(E)$ carries a canonical character

$$\rho : \mathrm{End}(E) \longrightarrow \overline{\mathbb{F}}_p,$$

defined by the action of endomorphisms on the one-dimensional space of invariant differentials: for all $\alpha \in \mathrm{End}(E)$,

$$\alpha^* \omega_E = \rho(\alpha)\, \omega_E.$$

Composing any $\mathcal{O}$-orientation ι with the reduction map $\mathrm{End}(E) \to \overline{\mathbb{F}}_p$ yields a p-*orientation* on $\mathcal{O}$. If p ramifies in K, then ρ takes values in $\mathbb{F}_p$ and is self-conjugate; if p is inert, ρ and its conjugate $\bar{\rho}$ give two distinct p-orientations, related by Frobenius, see [13].

We denote by $\mathrm{SS}_{\mathcal{O}}(p)$ the set of supersingular elliptic curves equipped with an optimal $\mathcal{O}$-orientation, up to oriented isomorphism, and by $\mathrm{SS}_{\mathcal{O}}(\rho)$ the subset determined by the p-orientation induced by ρ. When p is inert in $\mathcal{O}$, we obtain two disjoint subsets $\mathrm{SS}_{\mathcal{O}}(\rho)$ and $\mathrm{SS}_{\mathcal{O}}(\bar{\rho})$ exchanged by Frobenius. When p is ramified, these coincide.

2.3. **Ideal classes and oriented supersingular curves.** Let $\mathcal{O}$ be an order in K, and let $\mathrm{Pic}(\mathcal{O})$ denote its proper ideal class group: the group of invertible proper $\mathcal{O}$-ideals modulo principal ideals. For background on ideal classes in non-maximal orders we refer to [14, 22, 41].

Let $E \in \mathrm{SS}_{\mathcal{O}}(p)$ be a $\mathcal{O}$-oriented curve with $\mathrm{End}(E) \cong R \subset \mathfrak{A}_{p,\infty}$ and let $\mathfrak{a} \subset \mathcal{O}$ be a proper invertible $\mathcal{O}$-ideal. Using the embedding ι_0, define the left R-ideal

$$I_{\mathfrak{a}} \;:=\; R \cdot \iota_0(\mathfrak{a}) \;\subseteq\; R. \tag{2}$$

Equivalently, $I_{\mathfrak{a}} = \{\, x \in R \mid x \cdot \iota_0(\mathcal{O}) \subseteq \iota_0(\mathfrak{a}) \,\}$. The ideal $I_{\mathfrak{a}}$ is locally principal at every finite prime $\ell \neq p$ and its reduced norm generates the same ideal of $\mathbb{Z}$ as the quadratic norm of $\mathfrak{a}$, i.e. $\mathrm{nrd}(I_{\mathfrak{a}}) \sim N(\mathfrak{a})$, [41].

The associated finite subgroup of E_0 is defined by

$$E_0[I_{\mathfrak{a}}] := \bigcap_{x \in I_{\mathfrak{a}}} \ker(x),$$

and has order $N(\mathfrak{a})$. The quotient yields an isogeny

$$\phi_{\mathfrak{a}} : E_0 \longrightarrow E_{\mathfrak{a}} := E_0/E_0[I_{\mathfrak{a}}]. \tag{3}$$

Since each element of $I_{\mathfrak{a}}$ commutes with $\iota_0(\mathcal{O})$, the isogeny $\phi_{\mathfrak{a}}$ preserves $\mathcal{O}$-orientation. Let $\widehat{\phi_{\mathfrak{a}}}$ denote the dual isogeny of $\phi_{\mathfrak{a}}$,

$$\iota_{\mathfrak{a}}(\alpha) \;:=\; \frac{1}{\deg \phi_{\mathfrak{a}}}\, \phi_{\mathfrak{a}} \circ \iota_0(\alpha) \circ \widehat{\phi_{\mathfrak{a}}} \qquad (\alpha \in \mathcal{O}). \tag{4}$$

is an optimal embedding $\mathcal{O} \hookrightarrow \mathrm{End}(E_{\mathfrak{a}})$, [22, 41].

We call the pair $(E_{\mathfrak{a}}, \iota_{\mathfrak{a}})$ the oriented isogeny transform of (E_0, ι_0) by $\mathfrak{a}$.

Theorem 2. The set $\mathrm{SS}^{pr}_{\mathcal{O}}(\rho)$ of optimally $\mathcal{O}$-oriented supersingular elliptic curves with p-orientation ρ is a torsor for $\mathrm{Pic}(\mathcal{O})$.

Thus, isomorphism classes of supersingular elliptic curves with a fixed optimal orientation are parameterized by $\mathrm{Pic}(\mathcal{O})$.

2.4. **Oriented isogenies and the Bruhat–Tits tree.** The action of $\mathrm{Pic}(\mathcal{O})$ on optimally $\mathcal{O}$-oriented supersingular elliptic curves admits an interpretation in terms of ℓ–adic geometry, through the Bruhat–Tits tree associated with $\mathrm{PGL}_2(\mathbb{Q}_\ell)$. This viewpoint will later serve as a bridge between orientations and modular symbols. For more information on Bruhat–Tits tree one can check [2] and [7].

The Bruhat–Tits tree. Let $\mathcal{T}_\ell$ denote the infinite $(\ell+1)$-regular [55] Bruhat–Tits tree of $\mathrm{PGL}_2(\mathbb{Q}_\ell)$. Its vertices correspond to homothety classes of $\mathbb{Z}_\ell$-lattices in $\mathbb{Q}_\ell^2$, or equivalently, to isomorphism classes of maximal orders in the quaternion algebra $\mathrm{Mat}_2(\mathbb{Q}_\ell)$. Two vertices are connected by an edge precisely when the corresponding lattices differ by index ℓ, or equivalently, when there exists an isogeny of degree ℓ between the corresponding supersingular elliptic curves.

Let $\Gamma := R^\times$, where $R \cong \mathrm{End}(E_0)$ is a fixed maximal order. Then Γ acts on $\mathcal{T}_\ell$ without inversion, and the quotient $\Gamma\backslash\mathcal{T}_\ell$ is a finite graph, canonically identified with the ℓ-isogeny graph of supersingular elliptic curves, where each vertex is a curve E and edges correspond to ℓ-isogenies, [2, §4.3].

Remark. Passing from $\mathcal{T}_\ell$ to the quotient $\Gamma\backslash\mathcal{T}_\ell$ identifies vertices and edges that differ by the Γ-action, thereby folding the infinite, cycle-free tree into a finite graph in which cycles may appear.

Oriented vertices. Fix an optimal embedding $\iota_0 : \mathcal{O} \hookrightarrow R \cong \mathrm{End}(E_0)$. For any $\mathcal{O}$-oriented supersingular elliptic curve (E, ι), the image $\iota(\mathcal{O})$ determines a copy of $\mathcal{O}$ inside the endomorphism ring of E. This additional structure restricts which vertices and edges in $\Gamma\backslash\mathcal{T}_\ell$ are permissible.

Definition 3. The *oriented supersingular isogeny graph* is the subgraph of $\Gamma\backslash\mathcal{T}_\ell$ consisting of vertices $\{(E, \iota)\}$ and edges corresponding to horizontal ℓ-isogenies respecting the $\mathcal{O}$-orientation.

Ideal classes as oriented paths. Let $\mathfrak{a}$ be a proper invertible $\mathcal{O}$-ideal, and let $(E_\mathfrak{a}, \iota_\mathfrak{a})$ be the oriented curve associated to $\mathfrak{a}$ as in Section 2.2. Let $I_\mathfrak{a} \subset R$ be the left ideal from (2). Then:

Proposition 1. The ideal $I_\mathfrak{a}$ determines a unique geodesic path in $\Gamma\backslash\mathcal{T}_\ell$ starting at (E_0, ι_0) and ending at $(E_\mathfrak{a}, \iota_\mathfrak{a})$. The length of the path is equal to the ℓ–adic valuation of the ideal norm:

$$\mathrm{length}(\mathfrak{a}) = v_\ell(N(\mathfrak{a})),$$

where $N(\mathfrak{a})$ denotes the positive integer norm of $\mathfrak{a}$.

Proof. Reduction of $I_\mathfrak{a}$ at ℓ- yields a $\mathbb{Z}_\ell$-lattice in $\mathbb{Q}_\ell^2$ whose homothety class corresponds to a vertex of $\mathcal{T}_\ell$. Multiplication by a local generator of $\mathfrak{a}$ at ℓ- induces a sequence of index-ℓ- sub-lattices, hence edges. Since invertible $\mathcal{O}$-ideals are locally principal at ℓ, the path is well-defined, and its length is $v_\ell(N(\mathfrak{a}))$, matching the valuation of $I_\mathfrak{a}$. The endpoint corresponds to the order $\mathrm{End}(E_\mathfrak{a})$, giving the orientation $\iota_\mathfrak{a}$ by (4). □

Corollary 1. Each ideal class $[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O})$ corresponds to the homotopy class of oriented paths in $\Gamma\backslash\mathcal{T}_\ell$ starting at (E_0, ι_0).

2.5. **Horizontal and vertical isogenies; volcano picture.** Thus far we have fixed an order $\mathcal{O} = \mathcal{O}_f \subset K$ and studied the action of its class group on $\mathcal{O}$-oriented supersingular elliptic curves. In practice, one may vary the conductor f, and obtain a richer picture by considering orientations by the family of orders

$$\mathcal{O}_f = \mathbb{Z} + f\mathcal{O}_K, \qquad f \geq 1.$$

An oriented curve (E, ι) then implicitly carries the information of the order $\iota(\mathcal{O}_f) = \iota(K) \cap \mathrm{End}(E)$, and isogenies between such curves do not necessarily preserve f.

Horizontal versus vertical isogenies. Let (E, ι) be an optimally $\mathcal{O}_f$-oriented supersingular elliptic curve, and let $\phi : E \to E'$ be an isogeny of prime degree $\ell \neq p$. We endow E' with the induced K-action

$$\iota'(\alpha) \ := \ \frac{1}{\ell}\, \phi \circ \iota(\alpha) \circ \widehat{\phi} \qquad (\alpha \in K),$$

so that ι' is a ring homomorphism $K \to \mathrm{End}^0(E')$. We then define the induced oriented order on E'

$$\mathcal{O}' := \ \iota'(K) \cap \mathrm{End}(E') \ \subseteq \ \iota'(K).$$

Definition 4. We say that ϕ is *horizontal* if $\mathcal{O}' = \iota'(\mathcal{O}_f)$ equivalently, if $\iota'|_{\mathcal{O}_f}$ is again an *optimal* embedding $\mathcal{O}_f \hookrightarrow \mathrm{End}(E')$. In this case the conductor is preserved. We call ϕ *vertical* if $\mathcal{O}' \neq \iota'(\mathcal{O}_f)$. Equivalently, the induced order on E' is a different quadratic order $\mathcal{O}' = \mathcal{O}_{f'} \subset K$ with $f' \neq f$. In this case the conductor changes.

Horizontal ℓ-isogenies are precisely those compatible with the given $\mathcal{O}_f$-action; when $\ell \nmid f$ they are parametrized by proper invertible $\mathcal{O}_f$-ideals of norm ℓ. Vertical ℓ-isogenies occur exactly when the kernel has local constraints at primes dividing the conductor (in particular at $\ell \mid f$), and they move between different conductors.

Volcano structure. When ℓ is a prime dividing the conductor f, the ℓ-primary part of $\mathrm{End}(E)$ may change under an ℓ-isogeny. More precisely, if $\ell \mid f$ and ϕ is an ℓ-isogeny, then:

$$\mathrm{End}(E') \cap \iota(K) \ \in \ \{\mathcal{O}_f, \mathcal{O}_{f/\ell}, \mathcal{O}_{\ell f}\}.$$

Hence the vertices corresponding to oriented curves with endomorphism ring $\mathcal{O}_f$ form a "horizontal layer," while ℓ-isogenies may climb upward toward smaller conductor (larger order) or descend toward larger conductor. This has the typical shape of an isogeny *volcano*, familiar from ordinary elliptic curves, [41, 60].

3. Modular symbols and relative homology

We now recall modular symbols, the relative homology of $X_0(N)$, and the action of Hecke operators. We fix a positive integer $N \geq 1$ throughout this section. Standard references include [23, 40, 56, 59].

3.1. Modular curves and modular forms.

Congruence subgroups. Let $\mathbb{H} := \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ be the upper half-plane. The group $\mathrm{GL}_2^+(\mathbb{R})$ acts on $\mathbb{H}$ by fractional linear transformations

$$\gamma \cdot z = \frac{az + b}{cz + d} \qquad \text{for} \qquad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

and this restricts to an action of $\mathrm{SL}_2(\mathbb{Z})$. We denote $\Gamma(N)$ the kernel of the reduction map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ and we call it the principal congruence subgroup of

level N. A *congruence subgroup* is any subgroup of $\mathrm{SL}_2(\mathbb{Z})$ that contains $\Gamma(N)$ for some N. In particular, we will work with

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \ : \ c \equiv 0 \pmod{N} \right\}.$$

The set of cusps of $\Gamma_0(N)$ is naturally identified with $\Gamma_0(N)\backslash\mathbb{P}^1(\mathbb{Q})$, where $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$. See [23, §1.2] or [59, §1.3].

The modular curve $X_0(N)$ and its cusps. The quotient

$$Y_0(N) := \Gamma_0(N)\backslash\mathbb{H}.$$

defines a non-compact Riemann surface or, equivalently, a smooth complex analytic manifold, which admits a canonical compactification by adjoining finitely many cusps:

$$X_0(N) = Y_0(N) \sqcup C, \qquad C \simeq \Gamma_0(N)\backslash\mathbb{P}^1(\mathbb{Q}).$$

The compact Riemann surface $X_0(N)$ has a canonical model over $\mathbb{Q}$ [47, §7] and is the coarse moduli space parametrizing elliptic curves equipped with a cyclic subgroup of order N or, equivalently, a $\Gamma_0(N)$-level structure, [24]. We write $g = g(X_0(N))$ for its genus, $C = \{c_1, \ldots, c_c\}$ for the set of cusps and $c = \#C$ for their number.

Modular forms and cusp forms of weight 2. A holomorphic function $f : \mathbb{H} \to \mathbb{C}$ is a weight-2 modular form for $\Gamma_0(N)$ if

$$f(\gamma z)\,(cz + d)^{-2} = f(z) \qquad \text{for all } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N),$$

and if it is holomorphic at every cusp, in the sense of having a Fourier expansion with no negative powers at each cusp. The space of such forms is denoted $M_2(\Gamma_0(N))$.

A modular form $f \in M_2(\Gamma_0(N))$ is a *cusp form* if its Fourier expansion at each cusp has vanishing constant term; the subspace of cusp forms is denoted $S_2(\Gamma_0(N))$. For $f \in M_2(\Gamma_0(N))$ the differential

$$\omega_f := f(z)\,dz$$

is $\Gamma_0(N)$-invariant on $\mathbb{H}$, hence giving a meromorphic differential on $X_0(N)$ with possible poles only at cusps. There is a canonical identification

$$S_2(\Gamma_0(N)) \ \cong \ H^0\big(X_0(N), \Omega^1_{X_0(N)}\big), \qquad f \longmapsto \omega_f,$$

and therefore $\dim_{\mathbb{C}} S_2(\Gamma_0(N)) = g(X_0(N))$, [64, Ch. 3].

Hecke operators on modular forms. The Hecke operators arise from natural algebraic correspondences on $X_0(N)$. For $n \geq 1$, the *Hecke correspondence* T_n is induced by the finite correspondence on $Y_0(N)$ that sends a point (E, C) (with $C \subset E$ cyclic of order N) to the formal sum on divisors

$$(E/C',\ (C + C')/C')$$

as C' ranges over cyclic subgroups of E of order n and $C \cap C' = \{O\}$, and extends to a correspondence on $X_0(N)$, see [17, §1.3] and [23, §5.3]. Analytically, this correspondence is represented by a double coset operator

$$\Gamma_0(N)\,\alpha\,\Gamma_0(N), \qquad \alpha \in M_2(\mathbb{Z}),\ \det(\alpha) = n,$$

acting on modular forms; see [23, §5.1].

When $(n, N) = 1$, the operator T_n on weight-2 modular forms admits the usual explicit formula [37, §6.2]

$$T_n(f)(z) \;=\; n \sum_{\substack{ad=n \\ 0 \le b < d}} d^{-2}\, f\left(\frac{az+b}{d}\right),$$

and the operators $\{T_n\}_{n\geq 1}$ commute and preserve $S_2(\Gamma_0(N))$. They are normal with respect to the Petersson inner product [23, §5.5], so one can choose an orthonormal basis of simultaneous eigenforms.

When $\ell \mid N$, the operator U_ℓ is the double-coset operator $\Gamma_0(N)\left(\begin{smallmatrix} 1 & 0 \\ 0 & \ell \end{smallmatrix}\right)\Gamma_0(N)$. On weight-2 forms $f(q) = \sum_{n\geq 1} a_n q^n$ it satisfies

$$U_\ell(f)(q) = \sum_{n\geq 1} a_{\ell n}\, q^n,$$

3.2. **Relative homology and Manin symbols.** Let $C \subset X_0(N)$ denote the set of cusps on $X_0(N)$. The absolute homology $H_1(X_0(N); \mathbb{Z})$ group is generated by homology classes of singular 1-cycles on the Riemann surface $X_0(N)$, and more generally encodes 1-dimensional topological features of $X_0(N)$. The *relative homology* group $H_1(X_0(N), C; \mathbb{Z})$ enlarges this by allowing 1-chains whose boundary lies in C; in other words, we consider paths on $X_0(N)$ whose endpoints are permitted to be cusps, and we identify two such paths if their difference is homologous to a sum of closed loops together with paths contained entirely in the cusps, [59, 3.2].

The group H has a very concrete description in terms of modular symbols, see [34, §2] and [59, §3.3]. Let $\widetilde{\mathbb{M}}_2(\Gamma_0(N))$ be the free abelian group on formal *modular symbols* $\{r \to s\}$ with $r, s \in \mathbb{P}^1(\mathbb{Q})$, modulo the relations

$$\{r \to s\} + \{s \to t\} + \{t \to r\} = 0 \qquad \text{for all } r, s, t \in \mathbb{P}^1(\mathbb{Q}),$$
$$\{r \to r\} = 0 \qquad \text{for all } r \in \mathbb{P}^1(\mathbb{Q}).$$

The group $\Gamma_0(N)$ acts on $\mathbb{P}^1(\mathbb{Q})$ by linear fractional transformations, and hence on $\widetilde{\mathbb{M}}_2(\Gamma_0(N))$ by

$$\gamma \cdot \{r \to s\} := \{\gamma r \to \gamma s\}.$$

Manin observed that relative homology $H_1(X_0(N), C; \mathbb{Z})$ can be realized as the $\Gamma_0(N)$-coinvariants of $\widetilde{\mathbb{M}}_2(\Gamma_0(N))$, [45].

Proposition 2. There is a natural isomorphism of abelian groups

$$H_1(X_0(N), C; \mathbb{Z}) \cong \mathbb{M}_2(\Gamma_0(N)) := \Gamma_0(N)\backslash\widetilde{\mathbb{M}}_2(\Gamma_0(N))$$

where $\mathbb{M}_2(\Gamma_0(N))$ denotes the quotient module by the $\Gamma_0(N)$-action.

Elements of $H_1(X_0(N), C; \mathbb{Z})$ are thus represented by finite $\mathbb{Z}$-linear combinations of symbols $\{r \to s\}$ modulo the above relations and the $\Gamma_0(N)$-action.

Rank formula. The rank of the relative homology H can be expressed in terms of the genus and the number of cusps.

Proposition 3. Let $g = g(X_0(N))$ be the genus of $X_0(N)$ and let $c = \#C$ be the number of cusps. Then

$$\mathrm{rk}_{\mathbb{Z}}\, H_1(X_0(N), C; \mathbb{Z}) = 2g + (c-1).$$

Proof. Consider the long exact sequence in homology associated to the pair $(X_0(N), C)$:

$$\cdots \to H_1(X_0(N);\mathbb{Z}) \to H_1(X_0(N), C;\mathbb{Z}) \to H_0(C;\mathbb{Z}) \to H_0(X_0(N);\mathbb{Z}) \to 0.$$

We have $H_0(X_0(N);\mathbb{Z}) \cong \mathbb{Z}$ and $H_0(C;\mathbb{Z}) \cong \mathbb{Z}^c$. The map $H_0(C;\mathbb{Z}) \to H_0(X_0(N);\mathbb{Z})$ is the augmentation map $\mathbb{Z}^c \to \mathbb{Z}$ sending $(n_1, \ldots, n_c) \mapsto \sum_i n_i$, whose kernel has rank $c-1$. Since $X_0(N)$ is connected, the boundary map $H_1(X_0(N), C;\mathbb{Z}) \to H_0(C;\mathbb{Z})$ is surjective onto this kernel, and we obtain a short exact sequence

$$0 \to H_1(X_0(N);\mathbb{Z}) \to H_1(X_0(N), C;\mathbb{Z}) \to \ker(\mathbb{Z}^c \to \mathbb{Z}) \to 0.$$

The result follows from the fact that $H_1(X_0(N);\mathbb{Z})$ is free of rank $2g$, and $\ker(\mathbb{Z}^c \to \mathbb{Z})$ is free of rank $c-1$. □

Hecke action on modular symbols. The Hecke algebra $\mathbb{T}$ of level $\Gamma_0(N)$ is generated by the usual Hecke operators T_ℓ for primes $\ell \nmid N$ and U_ℓ for $\ell \mid N$. These operators act on cusp forms of weight 2 and level $\Gamma_0(N)$, but also on the homology H via correspondences on $X_0(N)$, see [15, §2.4]. More precisely, for each $m \geq 1$ the Hecke operator is induced by the Hecke correspondence $X_0(N) \xleftarrow{\pi_1} X_0(N, m) \xrightarrow{\pi_2} X_0(N)$, and its action on relative homology is the push–pull map $T_m = (\pi_2)_* \circ \pi_1^*$.

This Hecke action provides a mechanism by which the class group action on supersingular curves can be transferred to an action on homology, as we explain in the next section.

4. Class-group representations on modular-symbol homology

In this section we explain how the ideal class group $\mathrm{Pic}(\mathcal{O})$ gives rise to a Hecke-equivariant action on a suitable submodule of the relative homology $H_1(X_0(pN), C;\mathbb{Z})$, and how this allows us to associate a homology class to an oriented supersingular elliptic curve. We present three different approaches and prove that they agree in $H_1(X_0(pN), C;\mathbb{Z})$.

Throughout this section we fix an imaginary quadratic field K and an order $\mathcal{O} \subset K$ of discriminant $\mathrm{disc}(\mathcal{O}) = \Delta$; we also fix a prime p and a supersingular elliptic curve $E_0/\overline{\mathbb{F}}_p$ with a primitive orientation $\iota_0 : \mathcal{O} \hookrightarrow \mathrm{End}(E_0)$.

4.1. **Construction 1: Brandt module.** Let us fix an imaginary quadratic order $\mathcal{O} \subset K$ and a primitively $\mathcal{O}$-oriented supersingular curve (E_0, ι_0). Also fix a level N coprime to p. A cyclic subgroup $C \subset E_0[N]$ defines an Eichler order $R_N \subseteq \mathfrak{A}_{p,\infty}$ of level N, and (E_0, C) corresponds to a distinguished left ideal class I_0 in $\mathcal{C}\ell(\mathcal{R}_N)$. Each invertible $\mathcal{O}$-ideal $\mathfrak{a}$ defines a new oriented curve $(E_\mathfrak{a}, \iota_\mathfrak{a})$ and a new left ideal class $I_\mathfrak{a}$.

The set of left R_N-ideal classes is finite, and the associated *Brandt module*

$$\mathbb{B} := \mathbb{Z}[\mathcal{C}\ell(\mathcal{O}_B)]$$

is a free abelian group with basis indexed by these ideal classes. For each prime $\ell \nmid \mathrm{disc}(\mathfrak{A}_{p,\infty})\, N$, the Hecke operator T_ℓ acts on $\mathbb{B}$ via the classical Brandt matrices, encoding ℓ-neighbor relations between ideal classes; see [50] and [43, §3.2].

At the level of the Brandt module, the ideal action can be encoded by a $\mathbb{Z}$-linear operator

$$T_{\mathfrak{a}} : \mathbb{B} \longrightarrow \mathbb{B}.$$

The Jacquet–Langlands correspondence relates the Hecke module $\mathbb{B} \otimes \mathbb{Q}$ to a space of weight-2 cusp forms on $\mathrm{GL}_2(\mathbb{Q})$. More precisely, since $\mathfrak{A}_{p,\infty}$ has discriminant p and R_N has level N, then $\mathbb{B} \otimes \mathbb{Q}$ is Hecke-isomorphic to the subspace of $S_2(\Gamma_0(pN))$ consisting of forms that are new at p, see [46, §4/5] and [25].

On the other hand, by the Eichler–Shimura isomorphism, the space of weight-2 cusp forms on $\Gamma_0(pN)$ embeds Hecke-equivariantly into the singular homology of the modular curve $X_0(pN)$, see [16] for more details. Passing to relative homology with respect to the cusps yields a Hecke-stable lattice

$$H' \subseteq H_1(X_0(pN), C; \mathbb{Z})$$

Under these correspondences, each operator $T_{\mathfrak{a}}$ induces an automorphism $T'_{\mathfrak{a}}$ of H'. Passing to ideal classes, we obtain a homomorphism

$$\rho : \mathrm{Pic}(\mathcal{O}) \to \mathrm{Aut}_{\mathbb{Z}}(H'), \qquad [\mathfrak{a}] \mapsto T'_{\mathfrak{a}}.$$

We do not claim that ρ is faithful in general; its kernel depends on $(K, \mathcal{O}, N)$ and the chosen component. However, ρ is nontrivial, and in generic situations its kernel is expected to be small.

Definition 5. Let H' and ρ as above. Fix a nonzero base class $\gamma_0 \in H'$. For an ideal class $[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O})$, we define the associated homology class

$$\gamma^{(1)}([\mathfrak{a}]) := \rho([\mathfrak{a}])(\gamma_0) \in H'.$$

If (E, ι) is an $\mathcal{O}$-oriented supersingular elliptic curve lying in the $\mathrm{Pic}(\mathcal{O})$-orbit of a fixed base curve (E_0, ι_0), we choose an ideal class $[\mathfrak{a}]$ such that $(E, \iota) \simeq [\mathfrak{a}] \star (E_0, \iota_0)$ and set

$$\gamma^{(1)}(E, \iota) := \gamma^{(1)}([\mathfrak{a}]).$$

The homology class $\gamma^{(1)}(E, \iota)$ depends on the choice of $[\mathfrak{a}]$ only up to the stabilizer of γ_0 under the representation ρ.

Definition 6. The stabilizer of γ_0 is the subgroup

$$\mathrm{Stab}(\gamma_0) := \{[\mathfrak{c}] \in \mathrm{Pic}(\mathcal{O}) : \rho([\mathfrak{c}])(\gamma_0) = \gamma_0\}.$$

If $(E, \iota) \simeq [\mathfrak{a}] \star (E_0, \iota_0) \simeq [\mathfrak{b}] \star (E_0, \iota_0)$, then $[\mathfrak{b}]^{-1}[\mathfrak{a}]$ lies in the stabilizer of (E_0, ι_0) on the supersingular side, which is known to be finite, see [22] and [41, § 5.2]. Provided this finite subgroup maps into $\mathrm{Stab}(\gamma_0)$, the assignment $(E, \iota) \mapsto \gamma(E, \iota)$ is well defined up to the finite ambiguity $\mathrm{Stab}(\gamma_0)$.

Remark. From a cryptographic perspective, exact injectivity of the map $(E, \iota) \mapsto \gamma(E, \iota)$ is neither expected nor required. The map is used to sample homology classes from a structured but exponentially large subset of H', and any bounded non-injectivity arising from finite stabilizers does not weaken the hardness assumptions underlying the inversion problems considered in Section 6.

The role of quaternion algebras and the Jacquet–Langlands correspondence in this section is mostly conceptual: it provides a representation-theoretic justification for

the existence and structure of the action we use. All constructions needed later for cryptographic purposes (in particular, the computation of homology classes and ℓ-adic integrals) are carried out directly on the modular curve $X_0(N)$, without recourse to quaternionic algorithms.

4.2. **Construction 2: Heegner points and geometric geodesic cycles.** We now describe a geometric construction of a relative homology class on the modular curve $X_0(pN)$ associated to an ideal class in $\mathrm{Pic}(\mathcal{O})$, using complex multiplication and geodesic paths on the analytic modular curve. This construction is classical and goes back to the theory of Heegner points.

Over the complex numbers, the modular curve $X_0(pN)$ admits the analytic uniformization $X_0(pN)(\mathbb{C}) \cong \Gamma_0(pN)\backslash\mathbb{H}^*$ where $\mathbb{H}^* = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$.

Assume that $(pN, \Delta) = 1$ The theory of complex multiplication associates to each proper invertible $\mathcal{O}$-ideal $\mathfrak{a}$ a CM elliptic curve $E_\mathfrak{a}/\mathbb{C}$ together with a cyclic subgroup $C_\mathfrak{a} \subset E_\mathfrak{a}$ of order pN, yielding a point

$$x_\mathfrak{a} \;:=\; (E_\mathfrak{a}, C_\mathfrak{a}) \;\in\; X_0(pN)(\mathbb{C}).$$

The resulting set of CM points of discriminant Δ on $X_0(pN)$ is nonempty and is canonically parametrized by $\mathrm{Pic}(\mathcal{O})$, with the natural Galois and Hecke actions corresponding to the ideal class action, [16, Ch. 3].

Fix a base CM point $x_0 = x_\mathcal{O}$ corresponding to the trivial class, and fix a base cusp $c_\infty \in C$, e.g. the class of ∞. For $[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O})$ choose any continuous path

$$\eta_\mathfrak{a} : [0,1] \to X_0(pN)(\mathbb{C}) \qquad \text{with} \qquad \eta_\mathfrak{a}(0) = x_0,\ \eta_\mathfrak{a}(1) = x_\mathfrak{a}.$$

Then $\eta_\mathfrak{a}$ defines a class in the relative homology group $H_1(X_0(pN), \{x_0, x_\mathfrak{a}\}; \mathbb{Z})$. Its boundary is

$$\partial[\eta_\mathfrak{a}] = [x_\mathfrak{a}] - [x_0] \in H_0(\{x_0, x_\mathfrak{a}\}; \mathbb{Z}).$$

Choose a base cusp $c_\infty \in C$ and for each CM point x choose a path δ_x from x to c_∞. We can define a relative 1-cycle in the pair $(X_0(pN), C)$ by

$$\widetilde{\gamma}^{(2)}([\mathfrak{a}]) \;:=\; \eta_\mathfrak{a} + \delta_{x_\mathfrak{a}} - \delta_{x_0}.$$

and this yields a class

$$\gamma^{(2)}([\mathfrak{a}]) \;:=\; [\widetilde{\gamma}^{(2)}([\mathfrak{a}])] \;\in\; H_1(X_0(pN), C; \mathbb{Z}).$$

Independence of choices. Changing $\eta_\mathfrak{a}$ with fixed endpoints changes $\eta_\mathfrak{a}$ by an absolute 1-cycle, hence changes $\gamma^{(2)}([\mathfrak{a}])$ by an element of $H_1(X_0(pN); \mathbb{Z})$. In the same way, changing δ_x for a fixed x changes δ_x by an absolute 1-cycle as well.

Modular-symbol description. Via the Manin-symbol presentation of $H_1(X_0(pN), C; \mathbb{Z})$ (see §3.2), the class $\gamma^{(2)}([\mathfrak{a}])$ may be represented by an explicit $\mathbb{Z}$-linear combination of Manin symbols once one chooses matrices sending ∞ to the cusps and sending a fixed CM parameter τ_0 to a parameter $\tau_\mathfrak{a}$ for $x_\mathfrak{a}$.

4.3. **Construction 3: Bruhat–Tits graph and harmonic cocycles.** A third, more ℓ-adic, viewpoint comes from the Cerednik–Drinfeld uniformization [18,26] and the theory of harmonic cocycles on Bruhat–Tits trees. Throughout this subsection, ℓ denotes a prime dividing pN such that the relevant modular or Shimura curve admits Cerednik–Drinfeld uniformization at ℓ.

Over $\mathbb{Q}_\ell$, the curve admits a rigid-analytic uniformization as a quotient of the Drinfeld upper half-plane $\mathcal{H}_\ell$ by a discrete subgroup $\Gamma \subset \mathrm{PGL}_2(\mathbb{Q}_\ell)$, [16, § 5.3]:

$$X^{\mathrm{an}} \simeq \Gamma\backslash\mathcal{H}_\ell.$$

The skeleton of $\mathcal{H}_\ell$ is the Bruhat–Tits tree $\mathcal{T}_\ell$ of $\mathrm{PGL}_2(\mathbb{Q}_\ell)$, and the skeleton of the quotient X^{an} is the finite graph

$$\Gamma\backslash\mathcal{T}_\ell.$$

A more precise statement can be found in [2, § 3], [30, § 2] and [61].

Let $H_1(\Gamma\backslash\mathcal{T}_\ell;\mathbb{Z})$ denote the first homology of the quotient graph. Harmonic cocycles on $\mathcal{T}_\ell$ with respect to Γ form a Hecke module naturally isomorphic to spaces of weight-2 modular cusp forms. Moreover, there is a canonical Hecke-equivariant map

$$H_1(\Gamma\backslash\mathcal{T}_\ell;\mathbb{Z}) \longrightarrow H_1(X, C;\mathbb{Z}),$$

where X denotes the corresponding algebraic curve and C its set of cusps, or boundary components in the Shimura case. This map is induced by the specialization of analytic paths to algebraic cycles and is compatible with the Eichler–Shimura isomorphism and with ℓ-adic integration, see [29, Ch. 4].

Fix a base oriented object, e.g. a primitively oriented supersingular curve, and let v_0 denote the corresponding vertex of the quotient graph $\Gamma\backslash\mathcal{T}_\ell$. The action of the ideal class group $\mathrm{Pic}(\mathcal{O})$ on oriented supersingular curves induces, via the local embedding $\mathcal{O}\otimes\mathbb{Z}_\ell \hookrightarrow M_2(\mathbb{Q}_\ell)$, an action by correspondences on vertices of $\Gamma\backslash\mathcal{T}_\ell$; this is discussed explicitly in the context of oriented curves and Bruhat–Tits trees in [2] and [30, § 4].

For an ideal class $[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O})$, choose a representative path in the quotient graph from v_0 to a vertex $v_\mathfrak{a}$ corresponding to the oriented curve $(E_\mathfrak{a}, \iota_\mathfrak{a})$. By fixing once and for all a spanning tree of $\Gamma\backslash\mathcal{T}_\ell$, we may close this path to obtain a cycle $c_\mathfrak{a} \in H_1(\Gamma\backslash\mathcal{T}_\ell;\mathbb{Z})$.

We then define

$$\gamma^{(3)}([\mathfrak{a}]) := \mathrm{sp}(c_\mathfrak{a}) \in H_1(X, C;\mathbb{Z}),$$

where sp denotes the specialization map from graph homology to algebraic relative homology.

Remark. Different choices of representatives, spanning trees, or base edges modify $c_\mathfrak{a}$ by boundaries or by cycles homologous to zero in the graph. Under the specialization map, these changes correspond to absolute cycles in $H_1(X;\mathbb{Z})$, which vanish in relative homology.

4.4. **Equivalence of the three constructions.** These three constructions agree in $H_1(X_0(pN), C;\mathbb{Z})\otimes\mathbb{Q}$, and hence in the integral lattice H' up to finite index.

Proposition 4. There exists a $\mathbb{Q}$-subspace

$$H'_{\mathbb{Q}} \subseteq H_1(X_0(pN), C; \mathbb{Q}),$$

stable under the Hecke algebra away from pN, such that for every $[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O})$ the three constructions

$$\gamma^{(1)}([\mathfrak{a}]), \quad \gamma^{(2)}([\mathfrak{a}]), \quad \gamma^{(3)}([\mathfrak{a}])$$

define the same element of $H'_{\mathbb{Q}}$.

Proof. On the cuspidal $\mathbb{T}^{(pN)}$-module $H'_{\mathbb{Q}}$ the Eichler–Shimura pairing with $S_2(\Gamma_0(pN))$ is non-degenerate, so it suffices to show that $\gamma^{(i)}([\mathfrak{a}])$ have the same periods against every newform occurring in $H'_{\mathbb{Q}}$. But (1) and (2) define the same $\mathbb{T}^{(pN)}$-equivariant CM/Heegner class in the newform quotient via Jacquet-Langlands and Eichler–Shimura, and (3) has the same pairings by ℓ-adic uniformization and the identification of harmonic cocycles/graph cycles with modular symbols; hence $\gamma^{(1)}([\mathfrak{a}]) = \gamma^{(2)}([\mathfrak{a}]) = \gamma^{(3)}([\mathfrak{a}])$ in $H'_{\mathbb{Q}}$.

□

5. ℓ-adic period vectors and Coleman Integrals

We now pass from homology classes on $X_0(N)$ to ℓ-adic vectors via Coleman abelian integration.

5.1. **Weight-2 cusp forms and the period pairing.** Let $S_2(\Gamma_0(N))$ denote the space of weight-2 cusp forms of level $\Gamma_0(N)$ with coefficients in $\mathbb{C}$ or in a ℓ-adic field $\mathbb{Q}_\ell$. We restrict attention to the Hecke-stable subspace corresponding to the homology submodule $H' \subseteq H_1(X_0(N), C; \mathbb{Z})$; concretely, this amounts to working in the span of one or more Hecke eigenforms $f_1, \ldots, f_d \in S_2(\Gamma_0(N))$ corresponding to the newform attached to our Brandt module.

Let $f \in S_2(\Gamma_0(N))$ be a holomorphic cusp form. Classically, the *period pairing* between f and a homology class $\gamma \in H_1(X_0(N), C; \mathbb{Z})$ is defined by the complex integral

$$\langle f, \gamma \rangle \ := \ \int_\gamma f(z)\, dz,$$

where γ is represented by a singular 1-chain on the Riemann surface $X_0(N)(\mathbb{C}) \cong \Gamma_0(N)\backslash\mathbb{H}^*$ and $f(z)\,dz$ a holomorphic differential. This pairing is $\mathbb{C}$-bilinear and, by the Eichler–Shimura isomorphism, induces a perfect pairing between the cuspidal part of $H_1(X_0(N); \mathbb{Z}) \otimes \mathbb{C}$ and $S_2(\Gamma_0(N)) \oplus \overline{S_2(\Gamma_0(N))}$, [59, § 8].

A ℓ-adic analogue of this period pairing was developed by Coleman in his foundational work on ℓ–adic integration on curves [11]. For a smooth curve with good reduction over a ℓ-adic field, Coleman defined a canonical theory of path-independent ℓ-adic line integrals of differentials, now known as *Coleman integrals*.

Over the last two decades, a series of works by Balakrishnan, Kedlaya, and Tuitman developed practical algorithms for numerically computing these integrals on curves, including methods based on explicit ℓ-adic cohomology and Frobenius lifts; see [4, 5, 62]. More recently, Chen, Kedlaya, and Lau [10] introduced an efficient approach specialized to modular curves, computing Coleman integrals directly from

modular forms data together with the ℓ-adic analytic uniformization. A key feature of the Chen–Kedlaya–Lau approach is that it does not require an explicit algebraic model of the modular curve $X_0(N)$: instead, it works directly with q-expansions of modular forms and the rigid-analytic uniformization, making it particularly well suited for large levels and cryptographic applications

In this framework, for a weight-2 cusp form f of finite slope at ℓ and a relative homology class $\gamma \in H_1(X_0(N), C; \mathbb{Z})$, one obtains a well-defined ℓ-adic period

$$\langle f, \gamma \rangle_\ell \in \mathbb{Q}_\ell,$$

This pairing is $\mathbb{Q}_\ell$-linear in both arguments and compatible with Hecke operators,.

5.2. **The period vector.** Let $f_1, \dots, f_d$ be a fixed collection of weight-2 cusp forms corresponding to the homology submodule H'. For $\gamma \in H'$, we define the ℓ-adic period vector

$$\Pi(\gamma) := \big(\langle f_1, \gamma \rangle_\ell \dots, \langle f_d, \gamma \rangle_\ell\big) \in \mathbb{Q}_\ell^d.$$

For applications, we fix a precision parameter $m \geq 1$ and reduce modulo ℓ^m.

Definition 7. Let p be a prime not dividing N. For $m \geq 1$ and $\gamma \in H'$, the *truncated ℓ-adic period vector* of γ is

$$\Pi_m(\gamma) := \big(\langle f_1, \gamma \rangle_\ell, \dots, \langle f_d, \gamma \rangle_\ell\big) \bmod \ell^m \in (\mathbb{Z}/\ell^m\mathbb{Z})^d.$$

The map $\Pi_m : H' \to (\mathbb{Z}/\ell^m\mathbb{Z})^d$ is $\mathbb{Z}$-linear, and its image is contained in a subgroup whose size depends on d, ℓ, and m. If the f_i's are chosen to be linearly independent, and the integrals are sufficiently non-degenerate modulo ℓ^m, then one expects Π_m to have full rank d as a homomorphism of $\mathbb{Z}_\ell$-modules restricted to $H' \otimes \mathbb{Z}_p$.

The output space has size ℓ^{md}, and in the following framework we will require ℓ^{md} to be large compared to the number of candidate homology classes in order to avoid excessive collisions.

5.3. **A practical work-flow.** In practice, we pass from an $\mathcal{O}$-oriented supersingular elliptic curve to a numerical ℓ-adic period vector by combining Construction 2 with the Coleman-integration algorithm of Chen–Kedlaya–Lau [10, § 3].

Throughout, we fix a prime p and work with supersingular curves over $\overline{\mathbb{F}}_p$ primitively oriented by an imaginary quadratic order $\mathcal{O}$ of discriminant Δ. We also fix a level N with $(N, p) = 1$, and a prime $\ell \nmid Np$ used for ℓ-adic analysis and integration.

Oriented curves: Primitively $\mathcal{O}$-oriented supersingular elliptic curves in characteristic p are classified by ideal classes of $\mathcal{O}$, or equivalently by classes of primitive positive definite binary quadratic forms of discriminant $\Delta = \mathrm{disc}(\mathcal{O})$. To a quadratic form $Q = [a, b, c]$ one associates the CM point [58]

$$\tau = \frac{-b + \sqrt{\Delta}}{2a} \in \mathbb{H},$$

and hence a point on $X_0(N)(\mathbb{C})$ via its j-invariant $j(\tau) \in \overline{\mathbb{Q}}$.

In practice, one computes $j(\tau)$ either numerically via the analytic j-function, and then obtain an algebraic approximation, or algebraically as a root of the Hilbert class polynomial $H_D(X) \in \mathbb{Z}[X]$.

Ideal action. The action of $[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O})$ sends the CM point τ associated to (E, ι) to the CM point $\tau_{\mathfrak{a}}$ associated to $(E_{\mathfrak{a}}, \iota_{\mathfrak{a}})$, yielding $j(E_{\mathfrak{a}}) = j(\tau_{\mathfrak{a}})$ with $\tau_{\mathfrak{a}}$ determined by the corresponding quadratic form.

Level structure. To obtain a point on the modular curve $X_0(N)$, we must additionally choose a cyclic subgroup $C \subset E$ of order N. The resulting data (E, C) defines a point $P = (E, C) \in X_0(N)(\mathbb{C})$ and the ideal action transports (E, C) to corresponding level structures on $E_{\mathfrak{a}}$, producing a point $Q := P_{\mathfrak{a}} = (E_{\mathfrak{a}}, C_{\mathfrak{a}}) \in X_0(N)(\mathbb{C})$.

Hecke neighborhoods via modular polynomial. We have two points $P, Q \in X_0(N)$ represented analytically by points on $\mathbb{H}$ modulo $\Gamma_0(N)$. The Hecke correspondence T_ℓ on $X_0(N)$ sends a point P to the collection of points corresponding to cyclic ℓ-isogenies out of the associated elliptic curve. We note them as $\{j(P_i)\}_i$ and $\{j(Q_i)\}_i$

Local coordinate and residue discs. Fix the base point P and define the local parameter $t := j - j(P)$. For a neighbor P_i with j-invariant $j(P_i)$, we have $t(P_i) = j(P_i) - j(P) \in L$.

Differentials and their t-expansions. Let ω be a holomorphic differential on $X_0(N)$. Locally at P, the differential can be expressed as a power series in t:

$$\omega = \left(\sum_{n \geq 0} a_n t^n \right) dt, \qquad a_n \in L.$$

Tiny Coleman integrals. Given the local expression of ω as above, a Coleman primitive is obtained by formal integration:

$$F_\omega(t) := \int \omega = \sum_{n \geq 0} \frac{a_n}{n+1}\, t^{n+1}.$$

For any point P_i in the same residue disc, the tiny integral from P to P_i is computed by evaluating

$$\int_P^{P_i} \omega \;=\; F_\omega\big(t(P_i)\big) \;=\; \sum_{n \geq 0} \frac{a_n}{n+1} \big(j(P_i) - j(P)\big)^{n+1}.$$

Coleman integrals of holomorphic differentials on $X_0(N)$ compute the same linear functionals on $H_1(X_0(N), C; \mathbb{Z})$ as classical modular-symbol integrals.

Hecke symmetrization and eigenvalue normalization. Form Hecke-symmetrized combinations and apply the normalization factor $(\ell + 1 - a_\ell)^{-1}$ when working with eigen-differentials

$$(\ell + 1 - a_\ell) \int_P^Q \omega \;=\; \sum_{i=1}^{\ell+1} \left(\int_{Q_i}^Q \omega \;-\; \int_{P_i}^P \omega \right).$$

From the point of view of earlier sections, the ℓ-isogenous neighbors P_i of the CM point P correspond to the action of prime ideals of norm ℓ on the underlying quadratic form or, equivalently, on the oriented elliptic curve.

The Hecke-symmetrized sum of tiny integrals therefore reflects the horizontal class-group action on orientations, transported through the Jacquet–Langlands and Eichler–Shimura correspondences to homology and differentials on $X_0(N)$.

ℓ-adic vector. Fix a basis $\{\omega_1, \dots, \omega_d\}$ of the relevant Hecke-stable subspace of $S_2(\Gamma_0(N))$. Applying the above procedure to each ω_j yields a vector of ℓ-adic integrals

$$\Pi(P) := \big(\langle \omega_1, \gamma_{\mathfrak{a}} \rangle_\ell, \dots, \langle \omega_d, \gamma_{\mathfrak{a}} \rangle_\ell\big) \ \in \ \mathbb{Q}_\ell^d,$$

where $\gamma_{\mathfrak{a}} \in H_1(X_0(N), C; \mathbb{Z})$ is the relative homology class determined by the CM points P and Q.

6. The Modular Symbol Inversion Problem

6.1. **Path-encoded homology classes.** We now isolate the core hardness assumption underlying our constructions: the difficulty of recovering a short relative homology class from partial information about its ℓ-adic period pairings.

Let

$$H' \subseteq H_1(X_0(N), C; \mathbb{Z})$$

be the Hecke-stable $\mathbb{Z}$-lattice fixed in Section 4. Although the definition of H' is representation-theoretic, all homology classes used in practice will arise from explicitly described and combinatorially simple paths, see § 4. These paths are most naturally described in terms of the Bruhat–Tits tree associated with $\mathrm{PGL}_2(\mathbb{Q}_\ell)$, where vertices correspond to suitable lattices or orientations and edges correspond to elementary isogenies.

In concrete cryptographic applications, and in particular when computing ℓ-adic period integrals, we will work with the modular-symbol realization of Construction 2 in §4.2 and evaluate periods using the algorithms of Chen-Kedlaya-Lau [10]. This avoids the need to construct an explicit algebraic or rigid-analytic model of $X_0(N)$ and allows direct computation of ℓ-adic integrals associated with modular symbols.

We therefore assume that there is a distinguished finite generating set

$$\mathcal{S} = \{\sigma_1, \dots, \sigma_r\} \subset H'$$

such that each σ_i represents an elementary step in the underlying combinatorial structure, e.g. an oriented edge in the Bruhat–Tits graph or a basic Manin symbol. A *path of length L* is an expression

$$\gamma = \sigma_{i_1} + \cdots + \sigma_{i_L},$$

subject to local compatibility constraints ensuring that successive steps assemble into a valid path.

We denote by $\mathcal{W}_L$ the set of all valid paths of length at most L. Combinatorially, the cardinality of $\mathcal{W}_L$ grows exponentially in L, with growth rate determined by the branching of the underlying graph. This exponential growth underlies both the expressive power of the construction and the conjectured hardness of the inversion problems below.

6.2. **Definition of MSI.** Let

$$\Pi_m : H' \longrightarrow (\mathbb{Z}/\ell^m\mathbb{Z})^d$$

be the truncated ℓ-adic period map defined in Section 5.2,.

Definition 8 (MSI relation)**.** The *Modular Symbol Inversion relation* R_{MSI} is the subset of $(\mathbb{Z}/\ell^m\mathbb{Z})^d \times \mathcal{W}_L$ given by

$$R_{\mathrm{MSI}} := \{(y, \gamma) : \gamma \in \mathcal{W}_L,\ y = \Pi_m(\gamma)\}.$$

We write $(y, \gamma) \in R_{\mathrm{MSI}}$ to indicate that γ is a valid *short homology preimage* of y under Π_m.

Definition 9 (MSI problem)**.** Given an element $y \in (\mathbb{Z}/\ell^m\mathbb{Z})^d$ that is promised to satisfy

$$y = \Pi_m(\gamma^\star)$$

for some (unknown) $\gamma^\star \in \mathcal{W}_L$, the *Modular Symbol Inversion (MSI) problem* is to find *any* $\gamma \in \mathcal{W}_L$ such that $(y, \gamma) \in R_{\mathrm{MSI}}$.

Note that $\gamma^\star$ need not be unique; there may be multiple short paths or homology classes with the same period vector. The problem is to find any valid witness γ.

6.3. **Comparison with SIS, LWE, and isogeny-path.** Fix a $\mathbb{Z}$-basis $\{\sigma_1, \ldots, \sigma_r\}$ of H', where $r = \mathrm{rank}_{\mathbb{Z}}(H')$. Any homology class $\gamma \in H'$ can be represented by a vector $\mathbf{x} \in \mathbb{Z}^r$ satisfying additional relations encoding the path constraints.

With respect to this basis, the map Π_m is represented by a matrix

$$A \in M_{d\times r}(\mathbb{Z}/\ell^m\mathbb{Z})$$

such that

$$\Pi_m(\gamma) \equiv A\mathbf{x} \pmod{\ell^m}.$$

If one ignores the combinatorial path constraint $\gamma \in \mathcal{W}_L$, the MSI problem reduces to finding a short integer vector $\mathbf{x}$ solving the linear congruence $A\mathbf{x} \equiv y \pmod{\ell^m}$, which is formally similar to lattice problems of SIS type, [1, 31]. However, this analogy is limited and should not be overstated; in the MSI framework, the matrix A is highly structured, coming from period pairings, and admissible vectors $\mathbf{x}$ are restricted to a sparse, exponentially small subset corresponding to valid paths.

Similarly, MSI differs fundamentally from LWE. In LWE, one recovers a secret vector from noisy linear samples, [53]. In MSI, the relation is exact, but the difficulty arises from the structured sparsity of the solution space. As a result, known worst-case/average-case reductions for SIS or LWE do not apply to MSI, and no polynomial-time reduction between these problems is currently known.

The MSI problem is conceptually closer to isogeny-based path-finding problems, such as those underlying SQISign [9, 21], as both involve searching for short paths in exponentially large graphs. The analogy is nonetheless imperfect. In isogeny-based problems, the graph is the supersingular isogeny graph, vertices are elliptic curves, and edges are isogenies. In MSI, the underlying graph is implicit: it is the combinatorial structure generating H', e.g. a quotient of a Bruhat–Tits tree or the modular-symbol graph, and vertices correspond to partial homology states rather than curves.

At present, there are no known reductions between MSI and isogeny path problems. We treat them as distinct conjecturally hard problems, sharing only a common exponential path-search flavor.

6.4. **Heuristic hardness and parameter choices.** Heuristically, one may model Π_m as a random linear map on the set of short paths. Let $\mathcal{W}_L$ denote the set of valid paths of length at most L and suppose $\#\mathcal{W}_L \approx \exp(cL)$ for some branching constant $c > 0$. If Π_m behaves like a random function from $\mathcal{W}_L$ to a set of size ℓ^{md}, then the expected number of collisions among elements of $\mathcal{W}_L$ is about

$$\frac{(\#\mathcal{W}_L)^2}{2\ell^{md}} \approx \frac{\exp(2cL)}{2\ell^{md}}.$$

Choosing parameters such that

$$\ell^{md} \gg \exp(2cL)$$

ensures that, with overwhelming heuristic probability, Π_m is injective on $\mathcal{W}_L$.

Even if collisions occur, the MSI problem only asks for some preimage $\gamma \in \mathcal{W}_L$, not for uniqueness. The best generic attacks on MSI are brute-force or meet-in-the-middle exploration of the path space, with complexity exponential in L or in $L/2$ with meet-in-the-middle. Alternatively, one can rely on lattice-based attacks on the linear system $A\mathbf{x} = y$, followed by attempts to "round" the resulting short vectors to valid paths. These are also exponential in a suitable dimension, and their effectiveness in exploiting the path constraint is currently unknown.

Quantumly, one can expect at most generic quadratic speedups (e.g. Grover search, [33]) on such search spaces, leading to complexities of order $\exp(c'L)$ for some $c' < c$ but still exponential in L.

As noted in Section 4, the map from orientations to homology classes may not be injective, due to the kernel of ρ and the stabilizer $\mathrm{Stab}(\gamma_0)$. This means that several orientations may yield the same homology class γ, and hence the same period vector $\Pi_m(\gamma)$. This non-injectivity does not weaken the MSI assumption. The secret object in MSI is the homology class γ, not the orientation itself. Any finite multiplicity in the orientation-to-homology map only increases the entropy of representations and does not provide an adversary with a shortcut for inverting Π_m.

7. Cryptographic Constructions

We now sketch two basic primitives whose security can be phrased in terms of MSI-type assumptions. We fix the following global parameters:

- a prime p and an order $\mathcal{O} \subset K$ in an imaginary quadratic field K;
- a supersingular curve $E_0/\overline{\mathbb{F}}_p$ and an optimal embedding $\iota_0 : \mathcal{O} \hookrightarrow \mathrm{End}(E_0)$;
- a level N with $(N, p) = 1$ and a modular curve $X_0(N)$ with cusps C;
- a homology submodule $H' \subseteq H_1(X_0(N), C; \mathbb{Z})$ and a representation $\rho : \mathrm{Pic}(\mathcal{O}) \to \mathrm{Aut}_{\mathbb{Z}}(H')$ as in Section 4;
- a base class $\gamma_0 \in H'$ and a generating set $\mathcal{S}$ of elementary path steps, together with a path length bound L defining $\mathcal{W}_L$;

- an analysis prime ℓ, a precision m, and a set of cusp forms $f_1, \dots, f_d$ defining $\Pi_m : H' \to (\mathbb{Z}/\ell^m\mathbb{Z})^d$.

7.1. **An identification protocol.** A user chooses as secret key a random short homology class $\gamma_{\mathrm{sk}} \in \mathcal{W}_L$ and sets

$$y_{\mathrm{pk}} = \Pi_m(\gamma_{\mathrm{sk}})$$

as public key. The identification protocol proceeds as follows:

(1) Prover (with secret γ_{sk}) commits to a random path $\gamma_{\mathrm{com}} \in \mathcal{W}_L$ and sends $t = \Pi_m(\gamma_{\mathrm{com}})$ to the Verifier.

(2) Verifier samples a random challenge $c \in \{0, 1\}$, or more generally $c \in \mathbb{Z}_q$ for a small public modulus q, and sends c to the Prover.

(3) Prover computes the response homology class

$$\gamma_{\mathrm{resp}} := \gamma_{\mathrm{com}} + c\,\gamma_{\mathrm{sk}} \ \in \ H',$$

using a fixed reduction procedure to ensure that γ_{resp} is again represented by a valid short path $\gamma_{\mathrm{resp}} \in \mathcal{W}_{L'}$, and sends γ_{resp} to the Verifier.

(4) *Verification.* Verifier checks that $\gamma_{\mathrm{resp}} \in \mathcal{W}_{L'}$ and that

$$\Pi_m(\gamma_{\mathrm{resp}}) \ \equiv \ t + c\,y_{\mathrm{pk}} \pmod{\ell^m}.$$

Completeness follows from the homomorphism property of Π_m. Special soundness holds in the usual sense: given two accepting transcripts with the same commitment t and two distinct challenges $c \neq c'$, one can extract

$$\gamma_{\mathrm{sk}} = \frac{\gamma_{\mathrm{resp}} - \gamma'_{\mathrm{resp}}}{c - c'}$$

as a short homology class solving the MSI problem. The hardness of producing such a witness without knowledge of γ_{sk} is therefore reduced to MSI. Honest-Verifier zero-knowledge follows from the fact that commitments t are distributed as images of random short paths.

7.2. **A PRF based on iterated period mappings.** One may also envision pseudorandom functions keyed by short homology classes, in the spirit of lattice- and isogeny-based PRFs [3, 32, 48].

Let $\gamma_{\mathrm{sk}} \in \mathcal{W}_L$ be the secret key. Given an input bitstring $x \in \{0, 1\}^*$, we can interpret x as a word in the generators $\mathcal{S}$, yielding a short path $\gamma_x \in \mathcal{W}_{L_x}$. Define a combined path $\gamma_{\mathrm{sk},x}$ using a fixed path-combination rule such as concatenation followed by reduction to bounded length. We output

$$F_{\gamma_{\mathrm{sk}}}(x) := \mathsf{KDF}\big(\Pi_m(\gamma_{\mathrm{sk},x})\big),$$

where KDF is a standard hash-based key-derivation, e.g. HKDF [44] or a NIST-approved PRF-based KDF [19] used to map $(\mathbb{Z}/\ell^m\mathbb{Z})^d$ to a uniformly distributed bitstring.

Assuming the hardness of MSI and suitable pseudorandomness properties of Π_m on short paths, the resulting function is expected to be computationally indistinguishable from a random function for adversaries without knowledge of γ_{sk}. A full proof

would require a precise model of the combinatorial structure of $\mathcal{W}_L$ and of potential correlations introduced by the path-combination operation.

7.3. **Security parameters and parameter selection.** We choose parameters so that recovering a short path $\gamma \in \mathcal{W}_L$ from its truncated ℓ-adic period vector

$$\Pi_m(\gamma) \in (\mathbb{Z}/\ell^m\mathbb{Z})^d$$

requires exponential work. Here ℓ is the prime used for ℓ-adic integration, m is the truncation depth, and d is the number of independent period coordinates, which is typically the dimension of the chosen Hecke component.

Let B be the effective branching factor of the underlying path model, e.g. Bruhat–Tits trees or Manin-symbol dynamics. Heuristically $\#\mathcal{W}_L \approx B^L$, so generic search costs $\Theta(B^L)$, while meet-in-the-middle costs $\Theta(B^{L/2})$. To target λ-bit classical security we require $B^L \gtrsim 2^\lambda$ ($B^{L/2} \gtrsim 2^\lambda$ under generic quantum quadratic speedups).

The output space has size $\#(\mathbb{Z}/\ell^m\mathbb{Z})^d = \ell^{md}$. To suppress collision- style and meet-in-the-middle attacks that exploit Π_m, we impose the separation condition

$$\ell^{md} \gtrsim (\#\mathcal{W}_L)^2 \approx B^{2L},$$

which heuristically makes Π_m essentially injective on $\mathcal{W}_L$.

For efficient ℓ-adic integration we typically take $\ell \in \{3, 5\}$ and then choose (m, L) to satisfy the inequalities above. The level N governs both the ambient lattice size and the number of available period coordinates:

$$r = \operatorname{rank}_{\mathbb{Z}} H_1(X_0(N), C; \mathbb{Z}) = 2g(X_0(N)) + \#C - 1, \qquad d \le \dim S_2(\Gamma_0(N)).$$

Increasing N tends to increase r and d, strengthening the entropy ℓ^{md} but also increasing the cost of modular-symbol and modular-form computations. In prototypes we may take small N and compensate with larger (m, L); for security-oriented parameters we take N so that d is large (e.g. $d \ge 128$) allowing moderate m while keeping generic attacks beyond 2^{128}.

Finally, the characteristic prime p used for supersingular sampling is independent of q; in security-oriented instantiations we take p at the $\sim$ 256-bit scale as in OSIDH/SQISign-style parametrizations, while $\ell \in \{3, 5\}$ is reserved for efficient period computations.

8. Conclusion and future work

We have proposed a new algebraic–analytic encoding of oriented supersingular elliptic curves into modular symbols and ℓ-adic period vectors.

On the cryptographic side, we isolated the Modular Symbol Inversion problem as a natural candidate hardness assumption: given a period vector $y = \Pi_m(\gamma^\star)$ arising from a short homology class, find any short homology class γ with $\Pi_m(\gamma) = y$. MSI sits at the intersection of lattice linear algebra and combinatorial path problems.

We sketched how MSI can underlie identification schemes, signatures, and pseudorandom functions. These constructions are at an exploratory stage and future work consists in analyzing parameter selection, implementations, and resistance to structural attacks.

References

[1] M. Ajtai. Generating hard instances of lattice problems. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing (STOC '96)*. Association for Computing Machinery, New York, NY, USA, pp. 99–108, 1996.

[2] L. Amorós, A. Iezzi, K. Lauter, C. Martindale and J. Sotáková. Explicit connections between supersingular isogeny graphs and Bruhat–Tits trees. In *Women in Numbers Europe III: Research Directions in Number Theory*, Springer International Publishing, pp. 39–73, 2021.

[3] B. Applebaum and P. Raykov. Fast Pseudorandom Functions Based on Expander Graphs. In: *Hirt, M., Smith, A. (eds) Theory of Cryptography. TCC 2016*. Lecture Notes in Computer Science, vol **9985**. Springer, Berlin, Heidelberg, 2016.

[4] J. Balakrishnan and J. Tuitman. Explicit Coleman integration for curves. In: *Mathematics of Computation*, vol **89**-326, pp. 2965–2984, 2020.

[5] J.S. Balakrishnan, R.W. Bradshaw and K.S. Kedlaya. Explicit Coleman Integration for Hyperelliptic Curves. In: *Algorithmic Number Theory*. Lecture Notes in Computer Science, vol **6197**. Springer, Berlin, Heidelberg, 2010.

[6] J. Belding. *Number Theoretic Algorithms For Elliptic Curves*. PhD Thesis. University of Maryland, College Park, 2008.

[7] A. Broise-Alamichel, J. Parkkonen and F. Paulin. *Equidistribution and Counting Under Equilibrium States in Negative Curvature and Trees*. Progress in Mathematics, Birkhäuser Cham, 2020.

[8] W. Castryck, T. Lange, C. Martindale, L. Panny and J. Renes. CSIDH: an efficient post-quantum commutative group action. In: T. Peyrin and S. Galbraith (eds.) ASIACRYPT 2018. LNCS, vol. **11274**, Springer, Cham, pp. 395–427, 2018.

[9] D.X. Charles, E.Z. Goren and K.E. Lauter. Cryptographic Hash Functions from Expander Graphs. In *Journal of Cryptology*, vol. **22**, pp. 93–113, 2009.

[10] M. Chen, K. Kedlaya and J.B. Lau. Coleman Integration on Modular Curves. In *ArXiv*, 2024. `https://arxiv.org/abs/2401.14513`

[11] R.F. Coleman. Torsion Points on Curves and p-Adic Abelian Integrals. In: *Annals of Mathematics*, vol **121**.1, pp. 111–168, 1985.

[12] L. Colò and D. Kohel. Orienting supersingular isogeny graphs. In: *Journal of Mathematical Cryptology* 14, 2020.

[13] L. Colò and D. Kohel. On the modular OSIDH protocol. *preprint*.

[14] D.A. Cox. *Primes of the Form x2+ny2: Fermat, Class Field Theory, and Complex Multiplication*. Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts, 2nd Edition, John Wiley & Sons, 2014.

[15] J.E. Cremona. *Algorithms for Modular Elliptic Curves*. Cambridge University Press, 1992.

[16] H. Darmon. *Rational Points on Modular Elliptic Curves*. American Mathematical Society, 2004.

[17] H. Darmon, F. Diamond and R. Taylor. *Fermat's Last Theorem*. Current Developments in Mathematics, 1:1157, 1995.

[18] I.V. Cerednik. Uniformization of algebraic curves by discrete arithmetic subgroups of $\mathrm{PGL}_2(k_w)$ with compact quotients. In: *Mathematics*, vol. **29**.1, USSR Sbornik, pp. 55–78, 1976.

[19] L Chen. Recommendation for Key Derivation Using Pseudorandom Functions. NIST Computer Security Resource Center, 2024.

[20] S. Dasgupta and J. Teitelbaum. The p-adic upper half plane. In *p-adic geometry. Lectures from the 2007 10th Arizona winter school*, Tucson, AZ, USA, pp.65–121, 2007.

[21] L. De Feo, D. Kohel, A. Leroux, C. Petit and B. Wesolowski. SQISign: Compact Post-quantum Signatures from Quaternions and Isogenies. In: *Moriai, S., Wang, H. (eds) Advances in Cryptology - ASIACRYPT 2020*. Lecture Notes in Computer Science, vol **12491**, Springer, 2020.

[22] M. Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, In *Abhandlungen aus dem Mathematischen Seminar*. Hamburg **14**, 1941.

[23] F. Diamond and J. Shurman. *A First Course in Modular Forms*. Graduate Texts in Mathematics, Springer Science & Business Media, 2006.

[24] P. Deligne and M. Rapoport. Les schémas de modules de courbes elliptiques, Modular functions of one variable, II. Proceedings of the International Summer School on "Modular functions of

one variable and arithmetical applications", University of Antwerp, Antwerp, Springer Berlin, 1973.

[25] L. Dembélé and J. Voight. Explicit Methods for Hilbert Modular Forms. In *Elliptic Curves, Hilbert Modular Forms and Galois Deformations. Advanced Courses in Mathematics*, Springer Basel. 135–198, 2013.

[26] V.G. Drinfel'd. Coverings of p-adic symmetric regions. In: *Functional Analysis and Its Applications*, vol. **10**.2, pp. 107–115, 1976.

[27] M. Eichler. The basis problem for modular forms and the traces of the Hecke operators. In *Lecture Notes in Mathematics*, vol **320**, Springer, pp. 75–152, 1973.

[28] N. Elkies. Elliptic and modular curves over finite fields and related computational issues. In: *Computational Perspectives on Number Theory. Proceedings of a Conference in Honor of A.O.L. Atkin.*, Ed. by D. Buell and J. Teitelbaum. AMS, pp. 21–76, 1998.

[29] C. Franc. *Nearly rigid analytic modular forms and their values at CM points.* PhD thesis, McGill University, 2011.

[30] C. Franc and M. Masdeu. Computing fundamental domains for the Bruhat–Tits tree for $\mathrm{GL}_2(\mathbf{Q}_p)$, p -adic automorphic forms, and the canonical embedding of Shimura curves. In *LMS Journal of Computation and Mathematics*. vol **17**.1, pp. 1–23, 2014.

[31] C. Gentry, C. Peikert and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the fortieth annual ACM symposium on Theory of computing (STOC '08)*. Association for Computing Machinery, New York, NY, USA, pp. 197–206, 2008.

[32] O. Goldreich, S. Goldwasser and S. Micali. How To Construct Random Functions. In *25th Annual Symposium on Foundations of Computer Science*, Singer Island, FL, USA, pp. 464–479, 1984.

[33] L.K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing (STOC '96)*. Association for Computing Machinery, New York, NY, USA, pp. 212–219. 1996.

[34] P.E. Gunnells *Modular Symbols.* Notes from the 2014 UNCG Summer School in Computational Number Theory: Modular Forms and Geometry. Online notes. Available at `https://mathstats.uncg.edu/number-theory/summer_school/2014/`

[35] H. Hijikata, A. Pizer and T. Shemanske. Orders in quaternion algebras. In *Journal für die reine und angewandte Mathematik*, vol. **394**, pp. 59–106, 1989.

[36] H. Hijikata, A. Pizer and T. Shemanske. The basis problem for modular forms on $\Gamma_0(N)$. In *Memoirs of the American Mathematical Society*, vol. **82**, 1989.

[37] H. Iwaniec *Topics in Classical Automorphic Forms.* Graduate Studies in Mathematics, American Mathematical Society, 1997.

[38] B.W. Jordan and R. Livné. Local diophantine properties of Shimura curves. In: *Mathematische Annalen*, vol. **270**.2, pp. 235–248, 1984.

[39] K. Kedlaya. Counting Points on Hyperelliptic Curves using Monsky-Washnitzer Cohomology. In: *Journal of the Ramanujan Mathematical Society*, vol. **16**, 2001.

[40] N. Koblitz *Introduction to Elliptic Curves and Modular Forms.* Graduate texts in mathematics, Springer New York, 1984.

[41] D. Kohel. *Endomorphism rings of elliptic curves over finite fields*, Ph.D. thesis, U.C. Berkeley, 1996.

[42] D. Kohel. Computing modular curves via quaternions. *Unpublished notes based on talk at Computational Algebraic Number Theory*, Sydney, 1997.

[43] D. Kohel. Hecke module structure of quaternions. In *Class Field Theory – Its Centenary and Prospect*, Advanced Studies in Pure Mathematics, vol. **30**, pp. 177-196, 2000.

[44] H. Krawczyk and P. Eronen. RFC 5869: HMAC-based Extract-and-Expand Key Derivation Function (HKDF). RFC Editor, USA, 2010.

[45] Y.I. Manin. Parabolic points and zeta-functions of modular curves. In *Mathematics of the USSR-Izvestiya*, vol. **6**.1, pp. 19–64, 1972.

[46] K. Martin. The basis problem revisited. In *Transactions of the American Mathematical Society*, vol. **373**, pp. 4523–4559, 2020.

[47] J.S. Milne *Modular Functions and Modular Forms.* Online notes. Available at `https://www.jmilne.org/math/CourseNotes/mf.html`.

[48] M. Naor and O. Reingold. Number-theoretic constructions of efficient pseudo-random functions. In *Journal of the ACM*, vol. **51**.2, pp. 231–262, 2004.

[49] H. Onuki. On oriented supersingular elliptic curves. In: *Finite Fields and Their Applications*, vol. **69**, 2021.
[50] A. Pizer. An Algorithm for Computing Modular Forms on $\Gamma_0(N)$. In *Journal of Algebra*, vol. **64**, pp. 340–390, 1980.
[51] R. Pollack and G. Stevens. Overconvergent modular symbols and p-adic L-functions. In *Annales scientifiques de l'École Normale Supérieure*, Serie 4, vol. **44**.1, pp. 1–42, 2011.
[52] R. Pries. Current results on Newton polygons of curves. In *arXiv*, 2018. `https://arxiv.org/abs/1806.04654`
[53] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. In *Journal of the ACM*, vol. **56**.6, Article 34, 2009.
[54] K. Ribet and W. Stein. *Lectures on Modular Forms and Hecke Operators*. Online book. Available at `https://wstein.org/books/ribet-stein/`.
[55] J.P. Serre. Arbres, amalgames, SL_2. *Cours au Collège de France, rédigé avec la collaboration de Hyman Bass.* vol. **46**. Astérisque. Société Mathèmatique de France, 1977.
[56] G. Shimura. *Introduction to the Arithmetic Theory of Automorphic Functions*. Publications of the Mathematical Society of Japan: Kanō memorial lectures, Princeton University Press, 1971.
[57] J.H. Silverman. *The arithmetic of elliptic curves*. Vol. **106** of Graduate Texts in Mathematics, Springer-Verlag, 1986.
[58] K.E. Stange. Quadratic forms, lattices, and ideal classes. University of Colorado, 2021. *Online notes*. Available at `https://math.colorado.edu/~kstange/teaching-resources/numthy/quad-forms-class-gp.pdf`
[59] W.A. Stein. *Modular Forms, a Computational Approach.* Volume **79** of Graduate studies in mathematics, American Mathematical Society, 2007.
[60] A.V. Sutherland. Isogeny volcanoes. In *Algorithmic Number Theory 10th International Symposium (ANTS X)*, Open Book Series 1, MSP, pp. 507–530, 2013.
[61] J. Teitelbaum. On Drinfeld's universal formal group over the p-adic upper half plane. In *Mathematische Annalen* vol **284**.4, pp. 647–674, 1989.
[62] J. Tuitman. Counting points on curves using a map to $\mathbb{P}^1$. In *Mathematics of computation*, vol. **85**.298, pp. 961–981, 2015.
[63] J. Vélu. Isogénies entre courbes elliptiques. In: *Comptes rendus hebdomadaires des séances de l'Académie des sciences: Sciences chimiques*, Série A. vol. **273**, pp. 238–241, 1971.
[64] J. Wehler. *Modular Forms and Elliptic Curves. Online course notes.* Available at `https://www.mathematik.uni-muenchen.de/~wehler/Lehrveranstaltungen_WS_2020_2021.php#_Script`.