Christelle Vincent
University of Vermont

Summary of Past Research

This is a long-form summary of my past research, and some forthcoming, for students who are interested in working with me to read.

Contents

1 Construction of curves whose Jacobian has complex multiplication

For the past ten years, in collaboration with many mathematicians but in particular Sorina Ionica and Kristin Lauter, I have worked on the problem of constructing exact models for hyperelliptic curves of genus 3 whose Jacobian has complex multiplication by a sextic field. Our early work on the subject [BILV16a, BILV16b], developing Sage code that allows the computation of period matrices of abelian threefolds with complex multiplication, inspired a flurry of follow up work in which I was not involved: [KLL$^+$18, AE19, KLGS20, KLLG$^+$20, DI20, LSV21, DIS23]. (Though I wrote an appendix for the article [LSV21], the work in the body of the article is completely independent from mine.)

We set up some notation and vocabulary to lighten the prose below. A number field K is called a **CM field** (short for *complex multiplication* field) if it is a totally imaginary degree-2 extension of a totally real field. The **ring of integers** of a number field is denoted $\mathcal{O}_K$. An **endomorphism** of an abelian variety is an algebraic map from the variety to itself that respects its group structure and has finite kernel; the set of endomorphisms of an abelian variety along with the zero map forms a ring called the **endomorphism ring** of the abelian variety. An abelian variety is said to have **CM by** $\mathcal{O}_K$, or sometimes **CM by** K for short, if its endomorphism ring is isomorphic to $\mathcal{O}_K$ for some CM field K. One can associate to a complex abelian variety a **period matrix**, which is

a symmetric complex matrix with positive definite imaginary part, and which contains all of the complex-analytic (and hence algebro-geometric) information of the abelian variety. Finally, a **hyperelliptic Jacobian** (or a **plane quartic Jacobian**, respectively) is the Jacobian of a hyperelliptic curve (or the Jacobian of a plane quartic curve, respectively) and a **CM Jacobian** is a Jacobian with CM by some field K.

1.1 Background and motivation

The motivation for the problem of constructing CM Jacobians is both theoretical and practical. On the theoretical side, there is considerable interest in understanding CM Jacobians of large dimension, spurred by Coleman's conjecture [Col87] stating that for $g \geq 8$, there are only finitely many complex curves X of genus g, up to isomorphism, such that their Jacobian has CM by some K.

On the practical side, where my work takes place, one can use the so-called *CM method* to generate an abelian variety A defined over a finite field $\mathbb{F}_p$ of prime order with a certain prescribed number of rational points. To put it extremely succinctly, if K is a CM field and p a prime that splits completely in K, the complex abelian varieties with CM by K are defined over a number field, and their reduction modulo $\mathfrak{p}$ for $\mathfrak{p}|p$ have a number of rational points given by the norm of a certain element in K called a Weil number that is known *a priori*. Therefore, by choosing a field K where p splits completely and containing a Weil number with suitable norm, we can construct an abelian variety over $\mathbb{F}_p$ with a prescribed point count. As mentioned, one application of this construction is to generate groups useful for applications to cryptography relying on the discrete log problem. Indeed, for abelian varieties with suitable point counts, the group of rational points behaves (as far as we currently understand) as a black-box group.

My work specifically focuses on constructing threefolds with CM by the ring of integers of a sextic CM field; constructing elliptic curves with complex multiplication is classical, and the case of abelian surfaces with CM is now understood [BY06, GL07, Yan10, Yan13, GL12, LV15a, LV15b, LV15c]. The CM method allows us not only to construct an abelian variety with CM by a given CM field, but also to ensure that the variety we will obtain is geometrically simple and principally polarizable, if that is possible. In that case, since A is a geometrically simple, principally polarizable threefold, A is isomorphic to the Jacobian of a curve X of genus 3. Hence for computational applications, when we speak of **constructing a CM Jacobian** we mean giving a model for the underlying curve X, since this allows any computation on the points of its Jacobian. Therefore in our work we focus on providing a model, or equation, for this curve.

The issue with doing this in practice is subtle: The CM method allows us to construct a period matrix for the Jacobian A; this was understood by Shimura and Taniyama [ST61] and practically implemented in SageMath in the case of CM abelian threefolds in our early work on the topic [BILV16a, BILV16b]. This period matrix is an object that belongs to an analytic parameter space for abelian varieties, called the Siegel upper half-plane, and our software obtains its entries as floating-point decimals. From the entries of the matrix we can obtain a model for the curve X to any fixed precision we wish, but we require an exact model – with the coefficients expressed as algebraic numbers – to reduce the coefficients of the model of X modulo some prime $\mathfrak{p}$ belonging to the field of definition of X. My work is concerned with the problem of "rounding" the floating-point approximations obtained by our computations to exact algebraic numbers.

1.2 Curve invariants

Recall our goal of computing comparatively simple models for curves X whose Jacobian has complex multiplication. By "simple," I mean here that we wish to find a model defined over the field of definition of X rather than an extension of it. For example, in the genus 1 case, when computing an elliptic curve with CM, one might begin by computing the j-invariant of the curve, which belongs to the field of definition of the curve, and then construct the curve from its j-invariant using this formula (if $j \neq 0, 1728$):

$$y^2 + xy = x^3 - \frac{36}{j - 1728}x - \frac{1}{j - 1728}.$$

This approach – first computing curve invariants and then obtaining a model from the invariants – has the advantage that the curve invariants are defined over the field of moduli of the curve, and the model we obtain from the invariants is defined over the field of definition of the curve. In this manner we can obtain as simple a model for our curve as possible.

Curves of genus 3 also have invariants, similar to the j-invariant for elliptic curves. A small wrinkle in this setting is that there is not one family of invariants for all curves of genus 3; rather, we have the **Shioda invariants**

for hyperelliptic curves (those that admit a model of the form $y^2 = f(x)$ for f of degree 7 or 8) and the **Dixmier-Ohno invariants** for plane quartic curves (the curves of genus 3 that do not admit a hyperelliptic model over any field extension; these curves do all admit a model of the form $f(x, y) = 0$ for f a quartic polynomial).

Thankfully, given the period matrix of a simple principally polarized abelian threefold – which we know to be a Jacobian as remarked above – we can tell relatively easily if we have a hyperelliptic or a plane quartic Jacobian using **theta functions with characteristics**. First, for $\omega \in \mathbb{C}^3$, and Z a period matrix, define

$$\vartheta(\omega, Z) = \sum_{n \in \mathbb{Z}^3} \exp(\pi i n^T Z n + 2\pi i n^T \omega).$$

Then for $\xi = \begin{pmatrix} \xi_1 & \xi_2 \end{pmatrix} \in \frac{1}{2}\mathbb{Z}^6$, where $\xi_1, \xi_2 \in \frac{1}{2}\mathbb{Z}^3$, we define the values

$$\vartheta[\xi](Z) = \exp(\pi i \xi_1^T Z \xi_1 + 2\pi i \xi_1^T \xi_2)\vartheta(\xi_2 + Z\xi_1, Z),$$

which we call the **theta constants** associated to the period matrix Z. We have that $\vartheta[\xi](Z) = 0$ identically for every period matrix Z when $4(\xi_1 \cdot \xi_2) \equiv 1 \pmod 2$, and we call the remaining theta constants – which can potentially be nonzero – the **even theta constants** associated to the period matrix Z. Then we have the following result:

Theorem 1.2.1 ([Gla80, LG22])**.** Let A be a principally polarized threefold defined over a field of characteristic different from 2, and Z be a period matrix for this threefold. Then

- A is a plane quartic Jacobian if and only if none of the even theta constants associated to Z vanish;
- A is a hyperelliptic Jacobian if and only if exactly one even theta constant associated to Z vanishes;
- A is isomorphic to a product of a simple abelian surface and an elliptic curve as a polarized abelian variety if and only if 6 of the even theta constants associated to Z vanish; and
- A is isomorphic to a product of three elliptic curves as a polarized abelian variety if and only if nine of the even theta constants associated to Z vanish.

Once we have determined if we have a plane quartic or a hyperelliptic Jacobian, recent work allows us to compute the appropriate invariants from the theta constants; [LR] does this for the Dixmier-Ohno invariants, and [LG22] for the Shioda invariants. From the invariants, we also know how to recover a model for the curve; [LR12] does it in the hyperelliptic case and [LRS20] in the plane quartic case.

We thus turn our attention to finding the exact value of curve invariants from their floating-point approximation obtained using the period matrix. To do this, we compute the minimal polynomial over $\mathbb{Q}$ of each invariant. This in turn can be done in the following manner: Given a curve X whose Jacobian has CM by $\mathcal{O}_K$, the Galois conjugates of this curve over $\mathbb{Q}$ also all have CM by $\mathcal{O}_K$. Hence if $\tilde{Z}$ is the period matrix of a Jacobian with CM by $\mathcal{O}_K$ and J_k is a curve invariant, the minimal polynomial of $J_k(\tilde{Z})$ divides

$$\prod_{Z \text{ has CM by } \mathcal{O}_K} (x - J_k(Z)) \in \mathbb{Q}[x]. \tag{1.1}$$

It therefore suffices to compute this polynomial, which is called a **class polynomial** in the literature.

We can finally explicitly describe the crux of the difficulty of carrying out this research program: While a CM Jacobian (or more generally a CM abelian variety) has potential good reduction everywhere, the associated curve can have bad reduction (those will be primes of decomposable – but good! – reduction for the Jacobian). Hence the invariants of the curve X are algebraic numbers but not algebraic integers. As a consequence, computing the polynomial of equation (1.1) exactly requires knowledge of the primes that divide the denominators of the coefficients of this polynomial, and the powers to which they can appear, *a priori*. Indeed, this is necessary as the coefficients are rational numbers, which can only be provably rounded to the correct value with knowledge of their denominator. (This explains why the case of elliptic curves is simpler than the higher genera cases: Elliptic curves being their own Jacobian, the j-invariant of a CM elliptic curve is an algebraic integer and the coefficients of polynomial (1.1) are integers. These can be provably correctly rounded by ensuring that the final computation is accurate within at least 0.5 of the correct values, without any further knowledge of the values of the coefficients.)

1.3 My work on the topic

For simplicity, we will refer below to the rational primes that divide the denominators of the coefficients of the polynomial (1.1) as the **rational primes dividing the denominator of that invariant**. As a first result on these primes, in [IKL$^+$19], we prove that the odd rational primes dividing the denominator of a *hyperelliptic* invariant, under certain very mild conditions which apply to the Shioda invariants, are divisible only by primes of bad reduction of the curve.

The significance of our result is the following: if X has bad reduction at a prime $\mathfrak{p}|p$, then the endomorphism ring of A, which we know to be $\mathcal{O}_K$, embeds in the endomorphism ring of $A_\mathfrak{p}$, its reduction modulo $\mathfrak{p}$. Since X has bad reduction, $A_\mathfrak{p}$ is decomposable, and because of this we can show that $\mathrm{End}(A_\mathfrak{p})$ is contained in a matrix algebra over the quaternions $B_{p,\infty}$. Embedding $\mathcal{O}_K$ in such a matrix algebra is a strong condition on the prime p, and in the follow up article [IKL$^+$], we use this embedding to give a bound on the rational primes p that divide the denominators of hyperelliptic invariants as a function of the CM field K. Our article exhibits the first bound small enough to be practical for computational purposes, greatly improving earlier results [BCL$^+$15, KLL$^+$20].

2 Shapes of rings

Though currently my main research interests are in mathematical post-quantum cryptography, I continue to work on interesting, purely number-theoretic problems when they cross my path. In addition to the fun I have working on these projects, sometimes this serendipitously allows me to bring highly technical mathematical expertise to cryptographic problems.

This section presents a recent example of this: I began getting interested in the equidistribution of shapes of number fields in speaking with my friend Piper Harris (then Piper Harron) a few years ago, and we are working on a project extending the results of their PhD thesis on this topic. Then, this summer I was invited to join a group of mathematicians working on isogeny-based post-quantum cryptography at a workshop in Banff. I was surprised and delighted to find out that one of the project leaders, Ha Tran, was interested in computing shapes of rings of endomorphisms of supersingular elliptic curves. Thanks to my expertise on the subject of shapes of rings, I was able to co-lead the project and contribute several directions of investigation inspired by my research in "pure" number theory.

2.1 Background

In this section, let M be a free $\mathbb{Z}$-module of rank $n-1$. For concreteness, suppose further that M is a full rank lattice in $\mathbb{R}^{n-1}$: as a $\mathbb{Z}$-module, M has a basis that can be expressed as a set of $n-1$ $\mathbb{R}$-linearly independent vectors in $\mathbb{R}^{n-1}$. Associating this basis to an element $\mathrm{GL}_{n-1}(\mathbb{R})$ and remembering that any two $\mathbb{Z}$-bases of M are $\mathrm{GL}_{n-1}(\mathbb{Z})$-equivalent, M then corresponds to an element of the quotient

$$\mathrm{GL}_{n-1}(\mathbb{Z})\backslash \mathrm{GL}_{n-1}(\mathbb{R}).$$

For such a module M, we wish to define a notion of **shape**. Intuitively, a "shape" should be invariant under rotations and dilations, which on the basis of M as an element of $\mathrm{GL}_{n-1}(\mathbb{R})$ correspond to multiplication by a nonzero real scalar and an action of the real orthogonal group on the right, respectively. Consequently we define the shape of the module M to be its image in the quotient

$$\mathcal{S}_{n-1} = \mathrm{GL}_{n-1}(\mathbb{Z})\backslash \mathrm{GL}_{n-1}(\mathbb{R})/\mathbb{R}^\times O_{n-1}(\mathbb{R}),$$

which we call the **space of shapes**.

If K is a number field of degree n over $\mathbb{Q}$, let M be the set of algebraic integers of trace zero in K. Then M is a free $\mathbb{Z}$-module of rank $n-1$, and we define the **shape of the field** K to be the shape of this module. In their PhD thesis, in joint work with their advisor Bhargava, Harris studies the distribution in $\mathcal{S}_{n-1}$ of the shapes of degree-n fields with Galois group S_n for $n = 3, 4, 5$ [BH16]. More precisely, they show that as the discriminant of the degree-n S_n-fields are allowed to go to infinity, their shapes are equidistributed in the space of shapes $\mathcal{S}_{n-1}$ under its Haar measure.

2.2 Joint shapes of fields

Bhargava and Harris's result is obtained by working in the spaces parametrizing rings with unity of rank n for $n = 3, 4, 5$ given by Bhargava in [Bha04a, Bha04b, Bha08]. Crucially, to obtain his parametrization, Bhargava classifies *pairs of rings* (R, S), where R is a ring of unity of rank n (the objects we wish to study), and S is a

resolvent ring of R, an object which we refrain from defining here. The specific property of resolvent rings which we will need here is that if R is an order in an S_n-field K of degree n over $\mathbb{Q}$, then S is an order in the **resolvent field** F of K. We denote the degree of F over $\mathbb{Q}$ by r, where r is $2, 3, 6$, respectively, when n is $3, 4$ and 5, respectively.

This setup prompts the following question: For R an order in an S_n-field K of degree n, define the **joint shape** of the ring-resolvent pair (R, S) to be the pair consisting of the shape of the trace-zero submodule of R and the shape of the trace-zero submodule of S. Are these joint shapes equidistributed in $\mathcal{S}_{n-1} \times \mathcal{S}_{r-1}$ as the discriminant of R is allowed to go to infinity? Harris and I can show that this is the case, that the shape of (the trace-zero submodule of) a ring R does not constrain the shape of (the trace-zero submodule of) its resolvent ring when $n = 4, 5$. (The result is trivial when $n = 3$, as the resolvent ring then has rank 2, so its trace-zero submodule has rank 1; but of course the shape space $\mathcal{S}_1$ is a point, as all rank-1 $\mathbb{Z}$-modules differ by a dilation.)

A more involved question asks about the equidistribution of the joint shapes of the field-resolvent pairs (K, F). The reason why this question is significantly more difficult is that if $R = \mathcal{O}_K$ is the ring of integers of K, then its resolvent ring $S_{\mathcal{O}_K}$ is not usually the full ring of integers of F. Hence the joint shape of the ring-resolvent pair $(\mathcal{O}_K, S_{\mathcal{O}_K})$ is not the joint shape of the field-resolvent pair (K, F), and in fact Bhargava's parametrization spaces do not contain *any* integral points corresponding to the pair of rings $(\mathcal{O}_K, \mathcal{O}_F)$ in general.

In work in progress, Harris and I construct for each field-resolvent pair (K, F) a pair of $\mathbb{Z}$-modules $(R_{\mathcal{O}_F}, \mathcal{O}_F)$ such that the joint shape of (the trace-zero submodules of) this pair is the joint shape of the pair (K, F) and the trace-zero submodule of $\mathcal{O}_F$ acts as the resolvent of the trace-zero submodule of $R_{\mathcal{O}_F}$ (here we stress that $R_{\mathcal{O}_F}$ is not a ring). This allows us to show that if we restrict to degree-n S_n-fields such that the index $[\mathcal{O}_F : S_{\mathcal{O}_K}]$ is fixed, then the joint shapes of the field-resolvent pairs (K, F) are equidistributed as the discriminant of K tends to infinity, still for $n = 4, 5$. What remains to do now to obtain equidistribution for all field-resolvent pairs (K, F) is a delicate analysis of the error term for each fixed value of $[\mathcal{O}_F : S_{\mathcal{O}_K}]$.

2.3 Shapes of endomorphism rings of supersingular elliptic curves

Let E be an elliptic curve defined over $\overline{\mathbb{F}}_p$ for some prime p. Then we say that E is **supersingular** if its geometric endomorphism ring is noncommutative. (More background on elliptic curves is given in Section 4.1.) In that case, the endomorphism ring will be isomorphic to a maximal order in the quaternion algebra $B_{p,\infty}$ ramified at p and ∞. Conversely, every such maximal order is isomorphic to the endomorphism ring of a supersingular elliptic curve, and in fact Deuring [Deu41] showed that there is a one-to-one correspondence between Galois conjugacy classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$ and isomorphism classes of maximal orders in $B_{p,\infty}$.

Motivated by cryptographic applications about which I will say more in Section 4, there is currently considerable interest in, given a supersingular elliptic curve E over $\overline{\mathbb{F}}_p$, computing explicitly the isomorphism class of its endomorphism ring. This is a problem which is currently considered hard in the cryptographic sense, and which is believed to be post-quantum.

By results of [CG14], the maximal orders of $B_{p,\infty}$ corresponding to supersingular elliptic curves defined over $\mathbb{F}_p$ are characterized by three successive minima and two shortest vectors of a certain sublattice of rank 3 sometimes called the *Gross lattice* [Yan08, Kan09] of the order. This result was then strengthened considerably in [GL], which showed that the successive minima of the Gross lattice are enough to completely characterize the endomorphism ring of a supersingular elliptic curve, as long as the shortest vector has length at least 8 (which is very small).

In joint work with Chenfeng He, Gaurish Korpal and Ha Tran, we further improve the results of the two articles above by using the successive minima of the Gross lattice of the endomorphism ring of a supersingular elliptic curve to classify if its j-invariant belongs to $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$. We also obtain several results about the geometry of the ring of endomorphisms when the elliptic curve has an endomorphism of small degree.

3 Learning With Errors

In 2005, Regev [Reg09] proposed two novel problems called the Learning With Errors problems, or LWE problems for short. The hardness of these problems relies on the difficulty of solving a variation of the shortest vector problem for a lattice, which is a well-studied hard problem in computational number theory. Variations on these problems, the Ring Learning With Errors (RLWE) problems, are now the basis for two of the three post-quantum cryptographic standards released by the National Institute for Standards and Technologies this past August.

As post-quantum standards are implemented in real-world systems, cybersecurity professionals must be trained to use and deploy them. To prepare students to take a leadership role in such positions, I believe it is imperative to offer research experiences and project-based learning opportunities for undergraduate students that allow them to develop expertise on lattice-based cryptography. I have led two undergraduate research projects on this topic already

at the University of Vermont, which I present in Section 3.3.1, and look forward to leading more undergraduate projects in this area.

Research also continues at the highest levels both to test the security of these and related cryptographic schemes and to develop variants with smaller key sizes. Working in this area is a great opportunity for graduate students in mathematics who wish to develop skills that are in high demand in the industry at the moment, in addition to being exciting mathematics in its own right.

3.1 The LWE problems

Let $q \in \mathbb{Z}$ be a prime throughout. To define the LWE problems, we need to first define **LWE pairs**:

Definition 3.1.1. Let q be a prime, χ a random distribution on $\mathbb{F}_q$, and n a positive integer be fixed, and choose a vector $\vec{s} \in \mathbb{F}_q^n$. An $\mathbf{LWE}_{q,\chi,\vec{s}}$ **pair** is a tuple $(\vec{a}, b) \in \mathbb{F}_q^n \times \mathbb{F}_q$ such that

- the coordinates of $\vec{a} \in \mathbb{F}_q^n$ are drawn uniformly and independently at random, and
- $b = \vec{a} \cdot \vec{s} + e$ for e drawn from the distribution χ, where $\vec{a} \cdot \vec{s}$ denotes the usual dot product.

Though χ may be arbitrary, to fix ideas we note that in practice the reduction modulo q of a truncated discrete Gaussian distribution on the integers with some variance σ^2 and constraint $-\lfloor \frac{q}{2} \rfloor \leq x \leq \lfloor \frac{q}{2} \rfloor$ is often used. Regev then proposes two problems:

Definition 3.1.2. Given m $\mathrm{LWE}_{q,\chi\vec{s}}$ pairs

$$(\vec{a}_1, b_1), \ldots, (\vec{a}_m, b_m) \tag{3.1}$$

the **search LWE problem** asks to recover the vector $\vec{s}$.

And:

Definition 3.1.3. Given m pairs

$$(\vec{a}_1, b_1), \ldots, (\vec{a}_m, b_m)$$

with $(\vec{a}_i, b_i) \in \mathbb{F}_q^n \times \mathbb{F}_q$, the **decision LWE problem** asks to determine if the pairs are $\mathrm{LWE}_{q,\chi,\vec{s}}$ for some error distribution χ and secret $\vec{s}$, or if the values $\vec{a}_i$ and b_i were drawn uniformly and independently at random from $\mathbb{F}_q^n$ and $\mathbb{F}_q$, respectively.

3.2 Application of LWE to differential privacy

In 2005, Regev [Reg09] proposed two novel problems called the Learning With Errors problems, or LWE problems for short. The hardness of these problems relies on the difficulty of solving a variation of the shortest vector problem for a lattice, which is a well-studied hard problem in computational number theory. In our article [**?**], the first author proposes a novel method to sum vectors in a differentially private way. More precisely, the article proposes a multi-party computation protocol that allows a group of people to collectively compute the sum of their vectors without any one person revealing their vector to the others. The key idea is to use LWE pairs to create a string that behaves effectively as a one-time pad to encrypt the vectors to be summed.

Indeed, a set of LWE pairs can be rewritten as a matrix equation

$$A\vec{s} = \vec{b},$$

where $\vec{s} \in \mathbb{F}_q^n$ as before, $A \in M_{m \times n}(\mathbb{F}_q)$ is the matrix whose rows are the vectors $\vec{a}_i$, and $\vec{b}$ is the vector of values b_i. With this notation, the hardness of the decision LWE problem is equivalent to saying that the vector $\vec{b}$ is indistinguishable from a vector in $\mathbb{F}_q^m$ whose entries are chosen independently and uniformly at random. Therefore this vector is suitable for use as noise in a differentially private addition scheme, and knowledge of the secret vector $\vec{s}$ allows the removal of the mask $\vec{b}$.

In this collaboration, I provided expertise on the Learning With Errors decision problem, advising on whether its use was sound in this context and selecting the parameters necessary for security.

3.3 Research with students on RLWE

The main flaw of the LWE problems as a basis for a cryptosystem is, roughly speaking, that the LWE pairs $(\vec{a}_i, b_i)$ only allow the encryption of one bit at a time, since the dot product $\vec{a}_i \cdot \vec{s}$ is one-dimensional. It quickly [Mic07, LM06, PR06, LMPR08, LM08, Lyu09, LPR10, LPR13] became clear that considerably more information could be encrypted at once by using vectors $\vec{a}_i$ and $\vec{s}$ belonging to a *ring* R_q isomorphic to $\mathbb{F}_q^n$, resulting in a noisy product $\vec{b}_i \in \mathbb{F}_q^n$.

A ready source of such rings is the following: If K is a number field of degree n over $\mathbb{Q}$ and the rational prime q splits completely in K, then

$$\mathcal{O}_K/q\mathcal{O}_K \cong \mathcal{O}_K/\mathfrak{q}_1 \times \cdots \times \mathcal{O}_K/\mathfrak{q}_n \cong \mathbb{F}_q^n,$$

by Sun Zi's Remainder Theorem. It is then natural to define:

Definition 3.3.1. Let K be a number field, q a rational prime that splits completely in K, and χ a random distribution on $\mathcal{O}_K/q\mathcal{O}_K$ be fixed, and choose an element $s \in \mathcal{O}_K/q\mathcal{O}_K$. An $\mathbf{RLWE}_{K,q,\chi,s}$ **pair** is a tuple $(a, b) \in (\mathcal{O}_K/q\mathcal{O}_K)^2$ such that

- $a \in \mathcal{O}_K/q\mathcal{O}_K$ is drawn uniformly at random, and
- $b = as + e$ for e drawn from the distribution χ, and where as denotes the multiplication in $\mathcal{O}_K/q\mathcal{O}_K$.

We can then define the search and decision RLWE problems similarly to the search and decision LWE problems. We note that providing suitable distributions χ, which offer adequate security guarantees while being efficient to sample from, is an active area of investigation as different error distributions offer different performance trade-offs.

3.3.1 Attacks via the error distribution

In [ELOS15], the authors present an attack on the search RLWE problem: Let $\phi\colon \mathcal{O}_K/q\mathcal{O}_K \to \mathbb{F}_q$ be a ring homomorphism, which is necessarily given by reduction modulo $\mathfrak{q}$ for $\mathfrak{q}|q$. Under certain circumstances, the image of the distribution χ under ϕ may be statistically distinguishable from the uniform distribution on $\mathbb{F}_q$. When these circumstances are met, the authors observe that if the given pairs $(a_i, b_i) \in (\mathcal{O}_K/q\mathcal{O}_K)^2$ are RLWE with secret s and $g \in \mathbb{F}_q$ is such that $\phi(s) = g$, then

$$\phi(b_i) - \phi(a_i)g = \phi(e_i).$$

As the values e_i are drawn from the distribution χ, we have a statistically significant chance of being able to distinguish the set of values $\{\phi(e_i)\}$ from the set of values $\{\phi(b_i) - \phi(a_i)g\}$ which are generated when g is not the image of s under ϕ, since we expect this second set to be uniformly random. If $\mathbb{F}_q$ is not too large, we can simply guess $\phi(s)$ by computing the values $\{\phi(b_i) - \phi(a_i)g\}$ for each element $g \in \mathbb{F}_q$, and returning g such that the distribution of the values $\{\phi(b_i) - \phi(a_i)g\}$ is not uniformly random. Once we have obtained the reduction of s modulo $\mathfrak{q}$ for one prime $\mathfrak{q}$, repeating this process for every prime $\mathfrak{q}|q$ yields $s \in \mathcal{O}_K/q\mathcal{O}_K$.

There was significant follow-up work on this attack [ELOS16, CIV16, CLS17a, CLS17b] until this was all put into a unified framework by Peikert [Pei16]. More precisely, the author works with the dual version of the RLWE problems, where s belongs to the dual ring $\mathcal{O}_K^\vee$ of $\mathcal{O}_K$, assumes that χ is Gaussian, and gives a uniform lower bound on the variance of χ and an upper bound on q depending only on the degree of the number field K such that dual-RLWE problems satisfying these parameters are safe against these attacks.

In a similar direction, Theorem 3 of [CLS17b] shows that the field $K = \mathbb{Q}(\zeta_{2^n})$ is invulnerable to these sorts of attacks when $q < 2^{2n}$ is a totally split prime, and

$$\left(\frac{1 + \frac{\sqrt{q}}{2^n}}{2}\right)^r < \frac{1}{2}, \tag{3.2}$$

where r is the variance of χ (which is not quite Gaussian but shifted-binomial in this theorem). We note that the inequality (3.2) remains true when q and r are both decreased. This hints at the possibility that Peikert's security conditions may not be sharp, and that for small values of q, error distributions with small variance may still be safe against these attacks.

Under my supervision, a vertically integrated team consisting of my PhD student Sarah Days-Merrill and an undergraduate student pursuing an Honors thesis conducted extensive numerical experiments to confirm that there does appear to be increased security for prime ideals of small norm at smaller values of r. This research continued the following year when Days-Merrill and I supervised work by a student that was funded by the NSF Research Experience for Undergraduates supplement awarded to my NSF personal grant.

3.3.2 PLWE-type error sampling for non-monogenic integer rings

Days-Merrill's PhD work considers a family of instances of the Ring Learning With Errors problems, often called the Polynomial Learning With Errors (PLWE) problems, which are characterized by their error distribution χ: Let K be a number field of degree n with **monogenic** ring of integers $\mathcal{O}_K$, by which we mean that there is $\alpha \in K$ such that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Then for q a prime that splits completely in K, we can define a probability distribution χ on $\mathcal{O}_K/q\mathcal{O}_K$ in the following manner:

1. Draw n integers e_i, $i = 0, \ldots, n-1$, from a truncated discrete Gaussian distribution on the integers with constraint $-\lfloor \frac{q}{2} \rfloor \leq x \leq \lfloor \frac{q}{2} \rfloor$.
2. Form the element
$$e = e_0 + e_1\alpha + \cdots + e_{n-1}\alpha^{n-1} \in \mathcal{O}_K$$
3. Return $\bar{e} \equiv e \pmod{q}$, where
$$\bar{e} = \bar{e}_0 + \bar{e}_1\tilde{\alpha} + \cdots + \bar{e}_{n-1}\tilde{\alpha}^{n-1} \in \mathcal{O}_K/q\mathcal{O}_K,$$
for $\bar{e}_i \equiv e_i \pmod{q}$ and $\tilde{\alpha}$ a representative of the class $\alpha + q\mathcal{O}_K$.

In other words, the definition of the distribution χ uses the fact that in this case, the reduction map $\mathcal{O}_K \to \mathcal{O}_K/q\mathcal{O}_K$ can be given explicitly as a map $\mathbb{Z}[\alpha] \to \mathbb{F}_q[\tilde{\alpha}]$. In this situation we have the best of both worlds: A straightforward reduction map modulo q that allows efficient sampling in characteristic zero, and the security results that ensure that the reduction modulo q of the "coordinate-wise discrete Gaussian" on $\mathcal{O}_K$ is sufficiently statistically close to the uniform distribution. This is an advantageous situation in which we would like to find ourselves more often.

The Dedekind-Kummer theorem states that for a general number field K, if q splits completely in K and does not divide the index $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ for $\alpha \in \mathcal{O}_K$, then

$$\mathcal{O}_K/q\mathcal{O}_K \cong \mathbb{F}_q[\tilde{\alpha}]$$

for $\tilde{\alpha}$ a representative of the class $\alpha + q\mathcal{O}_K$. In other words, while $\mathcal{O}_K$ is not monogenic in general, its reduction modulo q often is. Days-Merrill's PhD work aims to characterize the distributions on $\mathbb{Z}[\alpha] \subsetneq \mathcal{O}_K$, when $\mathcal{O}_K$ is not monogenic, such that their reduction modulo q offers the same security properties enjoyed by monogenic rings. This would extend the range of cases where PLWE-type sampling can be used.

4 Supersingular isogeny graphs

In 2005, Charles, Goren and Lauter [CGL09] first proposed the problem of navigating the so-called ℓ-isogeny graph for supersingular elliptic curves over $\overline{\mathbb{F}}_p$, for p and ℓ distinct primes and p of cryptographic size, as a post-quantum hard problem. They then built a cryptographic hash function from random walks on the graph. Shortly after, De Feo, Jao, and Plût [DFJ11, DFJP14] proposed an encryption scheme called **supersingular-isogeny Diffie-Hellman**, or SIDH, whose security relied on an easier version of the same problem. Though the CGL hash function cannot be used without a so-called secure supersingular elliptic curve [EHL$^+$18] and SIDH is now broken [CD23, MM22, Rob23], research in applications of supersingular isogeny graphs to post-quantum cryptography continues, and several promising protocols are currently being studied as the field matures, such as CSIDH (commutative-SIDH) [CLM$^+$18], OSIDH (oriented-SIDH) [CK20], M-SIDH and MD-SIDH (masked (torsion points)-SIDH and masked degree-SIDH) [FMP23], and protocols that are not even named SIDH, such as SQISign [FKL$^+$20] and GPS [GPS20].

What is becoming clear is that isogeny-based cryptography has tremendous potential as the basis for post-quantum cryptography, but requires considerable mathematical sophistication to be deployed securely. The development of this potential depends on deep connections between the mathematical and cryptographic communities, as we link fundamental concepts in pure mathematics about isogeny graphs and endomorphism rings of elliptic curves with the practical objectives of building new cryptographic primitives and investigating their security and feasibility. Personally, I find it very exciting to do research that is as immediately practically important as it is deeply technically beautiful.

4.1 Background

As in Section 2.3, let E be a supersingular elliptic curve defined over $\overline{\mathbb{F}}_p$ for some prime p, by which we mean that its geometric endomorphism ring is noncommutative. An **isogeny** is an algebraic map of curves $\phi\colon E \to E_1$, where E_1 is also an elliptic curve over $\overline{\mathbb{F}}_p$, and ϕ is a group homomorphism. For ℓ a prime different from p, we define an **ℓ-isogeny** to be an isogeny with kernel cyclic of size ℓ. If E is supersingular and there is a nonzero isogeny $\phi\colon E \to E_1$, then E_1 is also supersingular. We can therefore define the following graph:

Definition 4.1.1. The **supersingular ℓ-isogeny graph over $\overline{\mathbb{F}}_p$**, for p and ℓ distinct primes, is the graph whose vertices are the set of isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$ (which is finite) and whose edges are ℓ-isogenies up to post-composition by an automorphism.

This graph (technically an oriented multigraph) is $(\ell+1)$-regular and connected, and by [Piz90], it is a **Ramanujan graph**. For us, the significance of this result is the following: Starting from a fixed supersingular elliptic curve E defined over $\overline{\mathbb{F}}_p$, the distribution of the endpoint of a long-enough random walk on this graph is indistinguishable from the uniform distribution. In practice, this means that the supersingular ℓ-isogeny graph is "hard to navigate"; given two supersingular elliptic curves E and E_1 chosen uniformly at random, it is a hard problem to give a path in the ℓ-isogeny graph joining them. One can trapdoor this hard problem by taking a supersingular elliptic curve E and a long random walk in the ℓ-isogeny graph, then publishing the endpoint of the walk and keeping the path secret.

An important wrinkle in this story is a consequence of the **Deuring correspondence**, which associates each Galois conjugacy class of supersingular elliptic curve E over $\overline{\mathbb{F}}_p$ to the isomorphism class of its endomorphism ring. Indeed, this correspondence yields a graph isomorphic to the supersingular ℓ-isogeny graph, whose vertices are the maximal orders of the quaternion algebra $B_{p,\infty}$ and whose edges are connecting ideals of norm ℓ, but this graph *can* be effectively navigated thanks to our understanding of computing in quaternion algebras.

Thus, the significance of the Deuring correspondence in this case is the following: The ability to effectively compute the isomorphism class of the endomorphism ring of a supersingular elliptic curve is equivalent to the ability to effectively navigate the supersingular ℓ-isogeny graph. Indeed, if one can compute endomorphism rings of supersingular elliptic curves, one can find the corresponding orders in the graph of maximal orders of $B_{p,\infty}$, find a path between them, and exhibit the corresponding path in the supersingular ℓ-isogeny graph.

As a consequence of the Deuring correspondence, several cryptographic protocols require a **secure** supersingular elliptic curve [CGL09, DFMPS19, ADFMP20, BDF21, LGDdSG21, Ste22, Bas23], an elliptic curve whose endomorphism ring is (provably) unknown to everyone. This prevents a nefarious actor from gaining an advantage by passing to the graph of maximal orders. Unfortunately, at present we do not have algorithms that can efficiently generate supersingular elliptic curves without leaking information about their endomorphism ring. Indeed, current algorithms either generate information about the endomorphism ring as a by-product of obtaining the supersingular curve (such as when we obtain a supersingular elliptic curve as the endpoint of a random walk in the supersingular isogeny graph) or generate supersingular elliptic curves with particularly easy-to-compute rings of endomorphism (such as the CM method; supersingular elliptic curves are characterized by their point count so the methods of Section 1.1 can also be used to construct supersingular elliptic curves).

As a consequence, to obtain a curve with unknown endomorphism ring, currently we must either rely on a trusted third party to construct the curve and forget the endomorphism ring information, or generate a curve through a zero-knowledge multiparty computation; these curves can only be trusted by the parties to the computation since the parties could collude to generate a supersingular elliptic curve whose endomorphism is known to them. In other words, the problem of generating a secure supersingular elliptic curve has yet to be solved in the trustless setting.

4.2 Quantum random walks

In [BBD+22], in joint work with a large team of authors we present a survey of the best failed attempts to generate a secure supersingular elliptic curve to date, with a detailed analysis of each failure and of which improvements might allow the technique to work. In the part of the paper to which I contributed, we propose performing a **quantum** random walk on the supersingular isogeny graph, using the work of [KSS22], and returning the endpoint as the secure curve. The idea is the following: using the set of j-invariants over $\mathbb{F}_{p^2}$ as a computational basis and starting from a qubit with probability concentrated at a supersingular j-invariant, we can apply the "ℓ-isogeny operator" T_ℓ, which is Hermitian, several times to generate a qubit consisting of a superposition of j-invariants, each of whose coefficient is the probability that a (quantum) random walk of that length would end at that point. Upon observing the superposition, we obtain our random supersingular j-invariant.

An obstacle to implementing this method is the following: The distribution of the endpoints of a finite quantum random walk is not the same as the distribution of endpoints of the analogous finite classical random walk, and it is not yet proven that the distribution of endpoints of the proposed quantum random walk does not give information about the ring of endomorphisms of the endpoint. To remedy this issue, one can instead consider the limiting distribution of the random walk, letting its length tend to infinity. We can sample directly from this distribution (without approximating it by taking an exponentially long walk) using phase estimation [Dol23], at least heuristically, but the method leaks information about an eigenvalue of the operator T_ℓ related to the curve, which is ultimately sampled. More work must be done to ensure that this eigenvalue information does not reveal information about the endomorphism ring of the sampled curve.

4.3 A recursive zero-knowledge proof of computation solution

The idea of the multiparty computation that allows the computation of a secure supersingular elliptic curve goes roughly as follows: Starting from a known supersingular elliptic curve E_0 with known endomorphism ring, the first party to the computation computes an isogeny $\phi_1 \colon E_0 \to E_1$ and publishes the curve E_1, the second party computes an isogeny $\phi_2 \colon E_1 \to E_2$ and publishes E_2, and so on. The curve published by the last party to the computation is then the secure curve. Indeed, the first party to the computation can compute the endomorphism ring of the curve E_1, but since they do not have an isogeny from E_1 to E_2, or to any other curve in the chain, they cannot compute the endomorphism ring of any of the other curves $E_2, E_3, \ldots$ The rest of the parties to the computation do have any endomorphism ring information, and therefore – if every party has been honest – the last curve is a secure supersingular elliptic curve.

The condition that every party be honest is important, because if this protocol is applied naively, the last party to the computation has the opportunity to deceive everyone: They can ignore the curve E_{n-1} they have just received, compute an isogeny $\phi_n \colon E_0 \to E_n$ and publish E_n. Then they could obtain the endomorphism ring of E_n using their isogeny from E_0, and no one would be the wiser. To guard against such a malicious party, at each step, along with the curve E_i, the ith party should also *prove knowledge* of an isogeny $\phi_i \colon E_{i-1} \to E_i$, without leaking any information about the isogeny ϕ_i. The current state of the art in this field is the article [**?**], which improves on the zero-knowledge proofs of [**?**, **?**].

For every party to the computation to be satisfied that every other party has behaved honestly requires every party to verify every other party's proof of knowledge. Since only parties to the computation can be assured of the security of the curve, and because the protocol must be performed sequentially, every improvement in speeding up both the proofs of knowledge and the verification of these proofs is welcome so that large numbers of parties can quickly and conveniently generate a curve they trust. In joint work with my PhD student Krystal Maughan and her co-advisor Joe Near, from the Department of Computer Science at the University of Vermont, we implement the latest and fastest techniques in recursive zero-knowledge proofs and proof-carrying computing languages to yield an asymptotically-faster solution to this problem [**?**].

5 Development work for the LMFDB

The L-functions and modular forms database [**?**], or LMFDB, is an online, searchable repository of information on objects arising in number theory and arithmetic geometry, whose aim is to illustrate some of the mathematical connections predicted by the Langlands program. In joint work with Dupuy, Kedlaya, and Roe, I contributed to this site a database of isogeny classes of abelian varieties of dimension g defined over $\mathbb{F}_q$, for small values of g and reasonable values of q. For each isogeny class it contains, our database displays several isogeny class invariants, and we detail the theoretical underpinnings of our work in [**?**]. In follow-up work [**?**] we use the database to disprove, using counterexamples, a conjecture of Ahmadi and Shparlinski [**?**].

Our database is already in wide use in the research community, and has inspired and been used in further work: The articles [**?**, **?**, **?**, **?**] all use our database nontrivially in at least one proof. In addition, our enumeration of isogeny classes revealed some errors in the literature bounding the coefficients of Weil polynomials, which were corrected in [**?**], and [**?**] uses our database to verify some calculations. Beyond these applications, our database is a source of examples and data in several articles. Finally, to sort the database we have defined labels that uniquely identify isogeny classes of abelian varieties over finite fields, which are now the standard way to refer to them in the literature.

6 Solving the S-unit equation

In this section, we let K be any number field, and S be a finite subset of its places, which includes all of the infinite places. Further, we define $\mathcal{O}_{K,S}$, the **S-units of K**, to be the set of elements of K of the form $\frac{\alpha}{\beta}$ where α and β are in $\mathcal{O}_K$ and the principal ideals (α) and (β) are only divisible by places contained in S. We note that $\mathcal{O}_{K,S} \cong C_w \times C_\infty^t$ as groups, where C_w is the cyclic group of order w where w is the number of roots of unity contained in K, C_∞ is the cyclic group $(\mathbb{Z}, +)$ in multiplicative notation, and t is an explicit positive integer. Fixing generators $\rho_0, \rho_1, \ldots, \rho_t$ for the cyclic factors of $\mathcal{O}_{K,S}$, to every element $x \in \mathcal{O}_{K,S}$ we can associate a vector of exponents $\vec{a}$ such that $x = \rho_0^{a_0} \rho_1^{a_1} \cdots \rho_t^{a_t}$.

In this setting, the **S-unit equation** asks the following: Enumerate all pairs $x, y \in \mathcal{O}_{K,S}$ – it is known that there are finitely many [**?**, **?**, **?**] – such that $x + y = 1$. In [**?**], we give the first publicly available (distributed through SageMath [**?**]) open-source implementation of an algorithm giving all solutions to the S-unit equation for a general K and S. Our work is based on descriptions of algorithms implemented by Smart [**?**, **?**, **?**] and implements de Weger's method [**?**] to solve the S-unit equation. To summarize at a very high level, this method uses bounds on absolute values of $\mathbb{Q}$-linear combinations of logarithms [**?**, **?**, **?**, **?**] to bound the exponents $\vec{a}$ appearing in a solution to the S-unit equation [**?**, **?**].

Unfortunately, currently our implementation is too slow to handle the case of $K = \mathbb{Q}$ as soon as S contains more than three finite primes, and suffers from even worse performance for nontrivial extensions of $\mathbb{Q}$. This is very poor compared to an implementation of the algorithm presented in [**?**], which only solves the S-unit equation for $K = \mathbb{Q}$, but which can do so in under one second even when S contains five finite primes, or to the work in progress [**?**] which has been used to solve the S-unit equation for a sextic field K and S containing the finite primes above 2 and 3 in fewer than thirty seconds. To make our implementation competitive with these works, in joint work with the same group as above, I am working on implementing further improvements to de Weger's bound on the exponents of the solutions, based on [**?**, **?**].

7 $\mathfrak{p}$-adic Drinfeld modular forms and Weierstrass points on $X_0(\mathfrak{p})$

Both my doctoral thesis and work completed shortly after was in the Drinfeld setting, an expression used to refer to constructions over the function field $\mathbb{F}_q(T)$ that are analogous to classical elliptic curves, modular curves, and modular forms over $\mathbb{Q}$. My early work on "$\mathfrak{p}$-adic Drinfeld modular forms" [**?**, **?**] is now widely cited in the discipline, though I did not continue to work in that area. In addition, the main part of my thesis work developed the theory of $\mathfrak{p}$-adic Drinfeld modular forms with the aim of obtaining information about the Weierstrass points of the Drinfeld modular curves $X_0(\mathfrak{p})$, for $\mathfrak{p}$ a prime of $\mathbb{F}_q[T]$ [**?**]. First we remark that as in the classical case, these modular curves have reduction modulo $\mathfrak{p}$ consisting of two copies of $\mathbb{P}^1$ that intersect transversally at the supersingular Drinfeld modules. My result is then the following: The reduction of the Weierstrass points of $X_0(\mathfrak{p})$ are all supersingular Drinfeld modules (which was already known by [**?**] but which I proved using a different technique), and what is more, every supersingular Drinfeld module is the reduction modulo $\mathfrak{p}$ of a Weierstrass points of $X_0(\mathfrak{p})$. These results are analogous to those in the classical setting [**?**, **?**, **?**].

8 References

[ADFMP20] Navid Alamati, Luca De Feo, Hart Montgomery, and Sikhar Patranabis. Cryptographic group actions and applications. In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology – ASIACRYPT 2020*, pages 411–439, Cham, 2020. Springer International Publishing.

[AE19] Sonny Arora and Kirsten Eisenträger. Constructing Picard curves with complex multiplication using the Chinese remainder theorem. In *Proceedings of the Thirteenth Algorithmic Number Theory Symposium*, volume 2 of *Open Book Ser.*, pages 21–36. Math. Sci. Publ., Berkeley, CA, 2019.

[Bas23] Andrea Basso. A post-quantum round-optimal oblivious PRF from isogenies. Cryptology ePrint Archive, Paper 2023/225, 2023. `https://eprint.iacr.org/2023/225`.

[BBD+22] Jeremy Booher, Ross Bowden, Javad Doliskani, Tako Boris Fouotsa, Steven D. Galbraith, Sabrina Kunzweiler, Simon-Philipp Merz, Christophe Petit, Benjamin Smith, Katherine E. Stange, Yan Bo Ti, Christelle Vincent, José Felipe Voloch, Charlotte Weitkämper, and Lukas Zobernig. Failing to hash into supersingular isogeny graphs. Extended abstract appeared in *CFAIL 2022*, full article submitted for publication, 2022.

[BCL+15] Irene Bouw, Jenny Cooley, Kristin E. Lauter, Elisa Lorenzo García, Michelle Manes, Rachel Newton, and Ekin Ozman. Bad reduction of genus 3 curves with complex multiplication. In *Women in Numbers Europe*, volume 2 of *Association of Women in Mathematics*, pages 57–82, 2015.

[BDF21] Jeffrey Burdges and Luca De Feo. Delay encryption. In *Advances in Cryptology – EUROCRYPT 2021: 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17–21, 2021, Proceedings, Part I*, page 302–326, Berlin, Heidelberg, 2021. Springer-Verlag.

[BH16] Manjul Bhargava and Piper Harron. The equidistribution of lattice shapes of rings of integers in cubic, quartic, and quintic number fields. *Compos. Math.*, 152(6):1111–1120, 2016.

[Bha04a] Manjul Bhargava. Higher composition laws. II. On cubic analogues of Gauss composition. *Ann. of Math. (2)*, 159(2):865–886, 2004.

[Bha04b] Manjul Bhargava. Higher composition laws. III. The parametrization of quartic rings. *Ann. of Math. (2)*, 159(3):1329–1360, 2004.

[Bha08] Manjul Bhargava. Higher composition laws. IV. The parametrization of quintic rings. *Ann. of Math. (2)*, 167(1):53–94, 2008.

[BILV16a] Jennifer S. Balakrishnan, Sorina Ionica, Kristin Lauter, and Christelle Vincent. Constructing genus-3 hyperelliptic Jacobians with CM. *LMS J. Comput. Math.*, 19(suppl. A):283–300, 2016.

[BILV16b] Jennifer S. Balakrishnan, Sorina Ionica, Kristin Lauter, and Christelle Vincent. Genus 3. `https://github.com/christellevincent/genus3`, 2016.

[BY06] Jan Bruinier and Tonghai Yang. CM-values of Hilbert modular functions. *Inventiones Mathematicae*, 163(2):229–288, 2006.

[CD23] Wouter Castryck and Thomas Decru. An efficient key recovery attack on SIDH. In *Advances in Cryptology – EUROCRYPT 2023*, pages 423–447, Cham, 2023. Springer Nature Switzerland.

[CG14] Ilya Chevyrev and Steven D. Galbraith. Constructing supersingular elliptic curves with a given endomorphism ring. *LMS Journal of Computation and Mathematics*, 17(A):71–91, 2014.

[CGL09] Denis X. Charles, Eyal Z. Goren, and Kristin E. Lauter. Cryptographic hash functions from expander graphs. *J. Cryptology*, 22(1):93–113, 2009.

[CIV16] Wouter Castryck, Ilia Iliashenko, and Frederik Vercauteren. Provably weak instances of Ring-LWE revisited. In *Advances in cryptology—EUROCRYPT 2016. Part I*, volume 9665 of *Lecture Notes in Computer Science*, pages 147–167. Springer, Berlin, 2016.

[CK20] Leonardo Colò and David Kohel. Orienting supersingular isogeny graphs. *J. Math. Cryptol.*, 14(1):414–437, 2020.

[CLM+18] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: an efficient post-quantum commutative group action. In *Advances in cryptology—ASIACRYPT 2018. Part III*, volume 11274 of *Lecture Notes in Computer Science*, pages 395–427. Springer, Cham, 2018.

[CLS17a] Hao Chen, Kristin Lauter, and Katherine Stange. Attacks on search RLWE problem with small errors. *SIAM Journal on Applied Algebra and Geometry*, 1(1), 2017.

[CLS17b] Hao Chen, Kristin Lauter, and Katherine Stange. Security considerations for Galois non-dual RLWE families. In *Selected areas in cryptography—SAC 2016*, volume 10532 of *Lecture Notes in Computer Science*, pages 443–462. Springer, Cham, 2017.

[Col87] Robert F. Coleman. Torsion points on curves. In *Galois representations and arithmetic algebraic geometry (Kyoto, 1985/Tokyo, 1986)*, volume 12 of *Adv. Stud. Pure Math.*, pages 235–247. North-Holland, Amsterdam, 1987.

[Deu41] Max Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hansischen Univ.*, 14:197–272, 1941.

[DFJ11] Luca De Feo and David Jao. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In *Post-quantum cryptography*, volume 7071 of *Lecture Notes in Computer Science*, pages 19–34. Springer, Heidelberg, 2011.

[DFJP14] Luca De Feo, David Jao, and Jérôme Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *Journal of Mathematical Cryptology*, 8(3):209–247, 2014.

[DFMPS19] Luca De Feo, Simon Masson, Christophe Petit, and Antonio Sanso. Verifiable delay functions from supersingular isogenies and pairings. In Steven D. Galbraith and Shiho Moriai, editors, *Advances in Cryptology – ASIACRYPT 2019*, pages 248–277, Cham, 2019. Springer International Publishing.

[DI20] Bogdan Adrian Dina and Sorina Ionica. Genus 3 hyperelliptic curves with CM via Shimura reciprocity. In *ANTS XIV—Proceedings of the Fourteenth Algorithmic Number Theory Symposium*, volume 4 of *Open Book Ser.*, pages 161–178. Math. Sci. Publ., Berkeley, CA, 2020.

[DIS23] Bogdan Dina, Sorina Ionica, and Jeroen Sijsling. Isogenous hyperelliptic and non-hyperelliptic Jacobians with maximal complex multiplication. *Math. Comp.*, 92(339):349–383, 2023.

[Dol23] Javad Doliskani. How to sample from the limiting distribution of a continuous-time quantum walk. *IEEE Transactions on Information Theory*, pages 1–1, 2023.

[EHL+18] Kirsten Eisenträger, Sean Hallgren, Kristin Lauter, Travis Morrison, and Christophe Petit. Supersingular isogeny graphs and endomorphism rings: Reductions and solutions. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2018*, pages 329–368, Cham, 2018. Springer International Publishing.

[ELOS15] Yara Elias, Kristin Lauter, Ekin Ozman, and Katherine Stange. Provably weak instances of Ring-LWE. In *Advances in cryptology—CRYPTO 2015. Part I*, volume 9215 of *Lecture Notes in Computer Science*, pages 63–92. Springer, Heidelberg, 2015.

[ELOS16] Yara Elias, Kristin Lauter, Ekin Ozman, and Katherine Stange. Ring-LWE cryptography for the number theorist. In *Directions in number theory*, volume 3 of *Association of Women in Mathematics*, pages 271–290. Springer, Cham, 2016.

[FKL+20] Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski. SQISign: compact post-quantum signatures from quaternions and isogenies. In *International Conference on the Theory and Application of Cryptology and Information Security–ASIACRYPT 2020*, pages 64–93. Springer, 2020.

[FMP23] Tako Boris Fouotsa, Tomoki Moriya, and Christophe Petit. M-SIDH and MD-SIDH: countering SIDH attacks by masking information. In *Advances in cryptology—EUROCRYPT 2023. Part V*, volume 14008 of *Lecture Notes in Comput. Sci.*, pages 282–309. Springer, Cham, [2023] ©2023.

[GL] E. Goren and J. Love. On elements of prescribed norm in maximal orders of a quaternion algebra. Accepted for publication in *Canadian Journal of Mathematics*.

[GL07] E. Goren and K. Lauter. Class invariants for quartic CM fields. *Ann. Inst. Fourier*, 57(2):457–480, 2007.

[GL12] E. Goren and K. Lauter. Genus 2 curves with complex multiplication. *Int. Math. Res. Not. IMRN*, 5:1068–1142, 2012.

[Gla80] J. P. Glass. Theta constants of genus three. *Compositio Math.*, 40(1):123–137, 1980.

[GPS20] Steven D. Galbraith, Christophe Petit, and Javier Silva. Identification protocols and signature schemes based on supersingular isogeny problems. *J. Cryptology*, 33(1):130–175, 2020.

[IKL+] Sorina Ionica, Pınar Kılıçer, Kristin Lauter, Elisa Lorenzo García, Adelina Mânzăţeanu, and Christelle Vincent. Determining the primes of bad reduction of cm curves of genus 3. Submitted for publication.

[IKL+19] Sorina Ionica, Pınar Kılıçer, Kristin Lauter, Elisa Lorenzo García, Maike Massierer, Adelina Mânzăţeanu, and Christelle Vincent. Modular invariants for genus 3 hyperelliptic curves. *Research in Number Theory*, 5(1), 2019.

[Kan09] Ben Kane. CM liftings of supersingular elliptic curves. *J. Théor. Nombres Bordeaux*, 21(3):635–663, 2009.

[KLGS20] Pınar Kılıçer, Elisa Lorenzo García, and Marco Streng. Primes dividing invariants of CM Picard curves. *Canad. J. Math.*, 72(2):480–504, 2020.

[KLL+18] Pınar Kılıçer, Hugo Labrande, Reynald Lercier, Christophe Ritzenthaler, Jeroen Sijsling, and Marco Streng. Plane quartics over $\mathbb{Q}$ with complex multiplication. *Acta Arith.*, 185(2):127–156, 2018.

[KLL+20] Pınar Kılıçer, Kristin Lauter, Elisa Lorenzo Garcìa, Rachel Newton, Ekin Ozman, and Marco Streng. A bound on the primes of bad reduction for CM curves of genus 3. *Proceedings of the American Mathematical Society*, 148(7):2843–2861, 2020.

[KLLG+20] Pınar Kılıçer, Kristin Lauter, Elisa Lorenzo García, Rachel Newton, Ekin Ozman, and Marco Streng. A bound on the primes of bad reduction for CM curves of genus 3. *Proc. Amer. Math. Soc.*, 148(7):2843–2861, 2020.

[KSS22] Daniel M. Kane, Shahed Sharif, and Alice Silverberg. Quantum money from quaternion algebras. *Mathematical Cryptology*, 2(1):60–83, Oct. 2022.

[LG22] Elisa Lorenzo García. On different expressions for invariants of hyperelliptic curves of genus 3. *J. Math. Soc. Japan*, 74(2):403–426, 2022.

[LGDdSG21] Yi-Fu Lai, Steven D. Galbraith, and Cyprien Delpech de Saint Guilhem. Compact, efficient and uc-secure isogeny-based oblivious transfer. In Anne Canteaut and François-Xavier Standaert, editors, *Advances in Cryptology – EUROCRYPT 2021*, pages 213–241, Cham, 2021. Springer International Publishing.

[LM06] Vadim Lyubashevsky and Daniele Micciancio. Generalized compact knapsacks are collision resistant. In *Automata, languages and programming. Part II*, volume 4052 of *Lecture Notes in Comput. Sci.*, pages 144–155. Springer, Berlin, 2006.

[LM08] Vadim Lyubashevsky and Daniele Micciancio. Asymptotically efficient lattice-based digital signatures. In Ran Canetti, editor, *Theory of Cryptography*, pages 37–54, Berlin, Heidelberg, 2008. Springer Berlin Heidelberg.

[LMPR08] Vadim Lyubashevsky, Daniele Micciancio, Chris Peikert, and Alon Rosen. SWIFFT: A modest proposal for FFT hashing. In Kaisa Nyberg, editor, *Fast Software Encryption*, pages 54–72, Berlin, Heidelberg, 2008. Springer Berlin Heidelberg.

[LPR10] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. In *Advances in cryptology—EUROCRYPT 2010*, volume 6110 of *Lecture Notes in Comput. Sci.*, pages 1–23. Springer, Berlin, 2010.

[LPR13] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. A toolkit for ring-LWE cryptography. In *Advances in cryptology—EUROCRYPT 2013*, volume 7881 of *Lecture Notes in Comput. Sci.*, pages 35–54. Springer, Heidelberg, 2013.

[LR] Reynald Lercier and Christophe Ritzenthaler. Siegel modular forms of degree three and invariants of ternary quartics. *Proceedings of the American Mathematical Society.* in press.

[LR12] Reynald Lercier and Christophe Ritzenthaler. Hyperelliptic curves and their invariants: geometric, arithmetic and algorithmic aspects. *J. Algebra*, 372:595–636, 2012.

[LRS20] Reynald Lercier, Christophe Ritzenthaler, and Jeroen Sijsling. Reconstructing plane quartics from their invariants. *Discrete Comput. Geom.*, 63(1):73–113, 2020.

[LSV21] Joan-C. Lario, Anna Somoza, and Christelle Vincent. An inverse Jacobian algorithm for Picard curves. *Res. Number Theory*, 7(2):Paper No. 32, 23, 2021.

[LV15a] K. Lauter and B. Viray. An arithmetic intersection formula for denominators of Igusa class polynomials. *Amer. J. Math.*, 137(2):497–533, 2015.

[LV15b] K. Lauter and B. Viray. Denominators of Igusa class polynomials. In *Numéro consacré au trimestre Méthodes arithmétiques et applications, automne 2013*, Publ. Math. Besançon Algèbre Théorie Nr. 2014/2, pages 5–29. Presses Univ. Franche-Comté, 2015.

[LV15c] K. Lauter and B. Viray. On singular moduli for arbitrary discriminants. *Int. Math. Res. Not.*, 19:9206–9250, 2015.

[Lyu09] Vadim Lyubashevsky. Fiat-Shamir with aborts: Applications to lattice and factoring-based signatures. In Mitsuru Matsui, editor, *Advances in Cryptology – ASIACRYPT 2009*, pages 598–616, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg.

[Mic07] Daniele Micciancio. Generalized compact knapsacks, cyclic lattices, and efficient one-way functions. *Comput. Complexity*, 16(4):365–411, 2007.

[MM22] Luciano Maino and Chloe Martindale. An attack on SIDH with arbitrary starting curve. Cryptology ePrint Archive, Paper 2022/1026, 2022. `https://eprint.iacr.org/2022/1026`.

[Pei16] Chris Peikert. How (not) to instantiate Ring-LWE. In *Security and cryptography for networks*, volume 9841 of *Lecture Notes in Comput. Sci.*, pages 411–430. Springer, Cham, 2016.

[Piz90] Arnold K. Pizer. Ramanujan graphs and Hecke operators. *Bull. Amer. Math. Soc. (N.S.)*, 23(1):127–137, 1990.

[PR06] Chris Peikert and Alon Rosen. Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices. In *Theory of cryptography*, volume 3876 of *Lecture Notes in Comput. Sci.*, pages 145–166. Springer, Berlin, 2006.

[Reg09] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM*, 56(6):Art. 34, 40 pp., 2009.

[Rob23] Damien Robert. Breaking SIDH in polynomial time. In Carmit Hazay and Martijn Stam, editors, *Advances in Cryptology – EUROCRYPT 2023*, pages 472–503, Cham, 2023. Springer Nature Switzerland.

[ST61] Goro Shimura and Yutaka Taniyama. *Complex multiplication of abelian varieties and its applications to number theory*, volume 6 of *Publications of the Mathematical Society of Japan*. Mathematical Society of Japan, Tokyo, 1961.

[Ste22] Bruno Sterner. Commitment schemes from supersingular elliptic curve isogeny graphs. *Mathematical Cryptology*, 1(2):40–51, Mar. 2022.

[Yan08] Tonghai Yang. Minimal CM liftings of supersingular elliptic curves. *Pure Appl. Math. Q.*, 4(4):1317–1326, 2008.

[Yan10] Tonghai Yang. An arithmetic intersection formula on Hilbert modular surfaces. *American Journal of Mathematics*, 132:1275–1309, 2010.

[Yan13] Tonghai Yang. Arithmetic intersection on a Hilbert modular surface and the Faltings height. *Asian Journal of Mathematics*, 17(2):335–381, 2013.