Computational aspects of class group actions and applications to post-quantum cryptography

Houben, M.R.

Chapter 3

Main Results

In this chapter, we summarize and highlight the main ideas and results of the thesis. The full and precise versions of these results appear in joint works presented in the later chapters.

3.1 Pairing-based attacks on class group action based cryptography

This section accompanies two joint research works, corresponding to Chapters 4 and 5. The first is a joint work on breaking the decisional Diffie–Hellman problem for class group action based schemes, together with Wouter Castryck, Frederik Vercauteren, and Benjamin Wesolowski. The second is a joint work on weak instances of the CRS protocol, together with Sam van Buuren, Wouter Castryck, Simon-Philipp Merz, Marzio Mula, and Frederik Vercauteren. We start this section by an introduction of our main tool: *self-pairings* on elliptic curves. Then, we introduce the *isogeny interpolation problem*; a partial solution to this problem turned out to break the SIDH scheme (Example 2.3.1). In Section 3.1.3, we show how these two ideas come together, as we highlight simplified versions of the ideas and main results of the two papers mentioned above.

3.1.1 Self-pairings

Let E/k be an elliptic curve over a field k of characteristic $p \geq 0$ and let $m \in \mathbf{Z}_{>0}$ be such that $p \nmid m$. We denote by $\mu_m \subseteq \overline{k}^\times$ the m-th roots of unity. Pairings are bilinear maps that send a pair of points on (subgroups of) two isogenous elliptic curves over k to the unit group $\overline{k}^\times$ of the algebraic closure of the field of definition of the curves. The typical example is the *Weil-pairing* $e_m : E[m] \times E[m] \to \mu_m \subseteq \overline{k}^\times$ [11, III.8]. It is an alternating, Galois-invariant, non-degenerate bilinear map, which is compatible with isogenies $\varphi : E \to E'$ in the sense that

$$e_m(\varphi(P), \varphi(Q)) = e_m(P, Q)^{\deg \varphi} \tag{3.1}$$

for all $P, Q \in E[m]$. We study the following notion related to pairings.

Definition 3.1.1 A *self-pairing* on a subgroup G of an elliptic curve E/k is a map $f : G \to \overline{k}^\times$ such that

$$f(\lambda P) = f(P)^{\lambda^2} \tag{3.2}$$

for all $\lambda \in \mathbf{Z}$ and all $P \in G$. △

Note that any bilinear map $e : G \times G \to \overline{k}^\times$ gives rise to a self-pairing $f : G \to \overline{k}^\times$, $P \mapsto e(P, P)$.

Example 3.1.2 Let $e_m : E[m] \times E[m] \to \mu_m$ denote the Weil pairing. If $\tau \in \mathrm{End}(E)$ is any endomorphism, then we obtain a self-pairing

$$f : E[m] \to \mu_m,\ P \mapsto e_m(P, \tau(P)), \tag{3.3}$$

which we call the (τ-)*twisted Weil self-pairing*. ☆

Example 3.1.3 Let E/K be an elliptic curve over a number field K. Then the canonical (Néron–Tate) height $\hat{h}_K : E \to \mathbf{R}$ satisfies (3.2), but is not a self-pairing, since $\mathbf{R} \not\subseteq \overline{K}^\times$. ☆

Similar to Equation (3.1), self-pairings have a notion of compatibility with isogenies.

Definition 3.1.4 Let E, E' be elliptic curves over k with self-pairings $f : G \to \overline{k}^\times$, $f' : G' \to \overline{k}^\times$ on subgroups $G \subseteq E$, $G' \subseteq E'$. Let $\varphi : E \to E'$ be an isogeny. We say that the self-pairings f, f' are *compatible* with φ if

$$\varphi(G) \subseteq G', \quad \text{and} \quad f'(\varphi(P)) = f(P)^{\deg(\varphi)} \tag{3.4}$$

for all $P \in G$. △

Example 3.1.5 Consider the twisted Weil self-pairing f of Example 3.1.2, and let $\varphi : E \to E$ be any endomorphism that commutes with τ. Then $\varphi(E[m]) \subseteq E[m]$ and

$$f(\varphi(P)) = e_m(\varphi(P), \tau(\varphi(P))) = e_m(\varphi(P), \varphi(\tau(P))) = e_m(P, \tau(P))^{\deg(\varphi)} = f(P)^{\deg(\varphi)},$$

hence f is compatible with φ. ☆

Definition 3.1.6 For a self-pairing $f : G \to \overline{k}^\times$ on a finite subgroup G, the *order* of f is the smallest positive integer m such that $f(G) \subseteq \mu_m$. △

3.1.2 Isogeny interpolation

Let $\varphi : E_0 \to E_1$ be an isogeny of degree d. It is an elementary result that φ is fixed once its images under $N > 4d$ points are known.

Lemma 3.1.7 *[14, Lemma 3.1]. Let $\varphi_1, \varphi_2 : E_0 \to E_1$ be isogenies of degree $\leq d$. Suppose that $\#\ker(\varphi_1 - \varphi_2) > 4d$. Then $\varphi_1 = \varphi_2$.*

The *isogeny interpolation problem* asks to recover an isogeny given sufficiently many image points. This problem can be effectively solved in certain cases.

Theorem 3.1.8 *Let E_0, E_1 be elliptic curves over a finite field of characteristic $p > 0$. Let $\varphi : E_0 \to E_1$ be an isogeny of known degree d coprime to p. Let $N \in \mathbf{Z}_{>0}$ such that $N^2 > 4d$ and $\gcd(N, d) = 1$. Suppose that we are given either of the following:*

(i) the images $\varphi(P), \varphi(Q)$ for a basis P, Q of $E[N]$; or

(ii) the image $\varphi(P)$ for a point $P \in E[N^2]$ of order N^2.

Then one can recover φ in polynomial time.

Proof. Case (i) is by Damien Robert [9, Thm. 1.1], following ideas from Castryck, Decru [4], Maino, and Martindale [8]. Case (ii) follows from case (i) by a reduction argument first proposed by Luca De Feo. A sketch of this argument appears in our joint work in Chapter 5; see below Remark 5.6.1. □

This result allows to break SIDH in polynomial time. For instance, in Example 2.3.1, by applying the theorem to $\varphi = \varphi_A, P = P_B, Q = Q_B, d = 2^a$, and $N = 3^b$.

3.1.3 Main contributions

Weak instances of CRS

We now highlight results of joint work with Sam van Buuren, Wouter Castryck, Simon-Philipp Merz, Marzio Mula, and Frederik Vercauteren. The full version of this work can be found in Chapter 5.

The main obstruction in applying the Isogeny Interpolation Theorem 3.1.8 to schemes that are based on class group actions, such as CSIDH and CRS, is that in such schemes no image points under the secret isogeny are shared. We studied whether it is possible to use self-pairings to obtain information about image points anyway, in an attempt to make class group action schemes vulnerable to the same attacks that broke SIDH. In what follows, we assume for ease of exposition that m is an *odd* integer. The following is a relatively straightforward result about self-pairings.

Lemma 3.1.9 *Let $f : G \to \overline{k}^\times$ be a self-pairing and let $P \in G$ of odd order m. Then $f(P)$ is an m-th root of unity.*

Proof. See Lemma 5.4.6. □

We call a self-pairing on a subgroup G for which $\#G = m$ *primitive* if its image contains a primitive m-th root of unity. By the lemma, this implies that G is cyclic. The main idea of how self-pairings could be used to obtain information about image points is as follows.

Idea 3.1.10 Let $\varphi : E \to E'$ be an unknown isogeny of known degree d. Suppose that we have primitive self-pairings $f : C \to \mu_m$ and $f' : C' \to \mu_m$ on cyclic subgroups $C = \langle P \rangle \subseteq E$ and $C' = \langle P' \rangle \subseteq E'$ of order m that are compatible with φ. Then, since $\varphi(P) \in C'$, it follows that $\varphi(P) = \lambda P'$ for some $\lambda \in \mathbf{Z}$. Now, since

$$f(P)^d = f'(\varphi(P)) = f'(P')^{\lambda^2}, \tag{3.5}$$

we can determine $\lambda^2 \pmod m$ from the values of $f(P)$, $f'(P')$, and d, by a discrete logarithm computation in μ_m.

Knowing $\lambda^2 \pmod m$, the idea is then to guess $\lambda \pmod m$, and hence $\varphi(P)$. Then, if m is large, smooth, and square, we can recover φ using case (ii) of Theorem 3.1.8. The next natural question is when such self-pairings exist. If the self-pairings are assumed to be compatible with isogenies coming from a class group action (i.e. if the above attack strategy applies to CSIDH and CRS), then our main result gives a complete classification.

Theorem 3.1.11 (van Buuren, Castryck, Houben, Merz, Mula, Vercauteren) *Let k be a field of characteristic $p \geq 0$, let $\mathcal{O}$ be an imaginary quadratic order of discriminant D, and let $m \in \mathbf{Z}_{>0}$ be odd and such that $p \nmid m$. Primitive self-pairings of order m compatible with $\mathcal{O}$-oriented isogenies (through the recipe of Section 2.2.2) exist if and only if $m \mid D$.*

Proof. See Prop 5.4.8 and Section 5.5. □

In CSIDH and CRS, we have $\mathcal{O} = \mathbf{Z}[\pi]$, which has discriminant $t^2 - 4q$. For CSIDH we have that $t = 0$ and $q = p$ is prime, hence the discriminant does not contain large smooth square factors, and CSIDH remains completely insusceptible to isogeny interpolation combined with self-pairings. We show, however, that exceptionally weak instances of CRS admit polynomial time key-recovery attacks. See Example 5.6.4 for an explicit such weak instance.

On the Decisional Diffie–Hellman problem

We now highlight results of joint work with Wouter Castryck, Frederik Vercauteren, and Benjamin Wesolowski. The full version of this work can be found in Chapter 4.

The pairing-based attack described above solves the Vectorization Problem 2.2.2(i). It was shown by Castryck, Sotáková, and Vercauteren [6] that there are cases in which the Decisional Diffie–Hellman Problem 2.2.2(iii) can be solved in classical polynomial time using Tate pairings. We present a new approach based on the Weil pairing that is more general, conceptually simpler, and oftentimes more efficient than the previous method.

In what follows, we denote by $m \in \mathbf{Z}_{>0}$ an odd *prime number*. Suppose $f : G \to \mu_m$ is a self-pairing on a subgroup of an elliptic curve E. We define an equivalence relation on $\mu_m \setminus \{1\}$ by setting $x \sim y \iff \exists \lambda \in \mathbf{Z} : y = x^{\lambda^2}$. This partitions $\mu_m \setminus \{1\}$ into two equivalence classes S_1, S_2. There are now four options for the image of G under

f. Indeed, $f(G)$ equals either $\{1\}$, μ_m, $\{1\} \cup S_1$, or $\{1\} \cup S_2$. In the last two cases, we call f *ramified*.

Idea 3.1.12 Suppose that $\varphi : E \to E'$ is an unknown isogeny of (unknown) degree d coprime to m. Suppose that we have ramified self-pairings $f : G \to \mu_m$ and $f' : G' \to \mu_m$ on subgroups $G \subseteq E$ and $G' \subseteq E'$ that are compatible with φ. Let $P \in E$ and $P' \in E'$ be such that $f(P)$ and $f'(P')$ are primitive m-th roots of unity. Since f' is ramified, we find that

$$f(P)^d = f'(\varphi(P)) \sim f'(P').$$

It follows that we can determine whether d is a quadratic or non-quadratic residue modulo m by computing whether or not $f(P) \sim f'(P')$.

To check whether $f(P) \sim f'(P')$, a discrete logarithm computation in μ_m followed by a Legendre symbol computation suffices. Indeed,

$$\left(\frac{\log_{f(P)} f'(P')}{m}\right) = \begin{cases} 1 & \text{if } f(P) \sim f'(P'); \\ -1 & \text{if } f(P) \not\sim f'(P'). \end{cases}$$

Equivalently,

$$\left(\frac{d}{m}\right) = \left(\frac{\log_{f(P)} f'(P')}{m}\right).$$

Our main result classifies when ramified self-pairings compatible with isogenies coming from a class group action exist.

Theorem 3.1.13 (Castryck, Houben, Vercauteren, Wesolowski) *Let k be a field, let $\mathcal{O}$ be an imaginary quadratic order of discriminant D, and let $m \in \mathbf{Z}_{>0}$ be an odd prime number different from* $\operatorname{char} k$. *Ramified self-pairings of order m compatible with $\mathcal{O}$-oriented isogenies (through the recipe of Section 2.2.2) exist if and only if $m \mid D$. In that case, an explicit family of ramified self-pairings is given by the twisted Weil pairing*

$$f : E[m] \to \mu_m,\ P \mapsto e_m(P, \sigma(P)),$$

for some generator σ of $\mathcal{O} = \mathbf{Z}[\sigma]$ of norm coprime to m.

Proof. See Theorem 4.1.1. □

This leads to the following attack strategy against the Decisional Diffie–Hellman Problem 2.2.2(iii). Using ramified self-pairings of order m compatible with the class group action, we can determine whether the norm of (a representative of) a connecting ideal class $[\mathfrak{a}]$, or equivalently, the degree of an isogeny $\varphi_{\mathfrak{a}} : E_0 \to [\mathfrak{a}]E_0$, is a square or not modulo m. A Diffie–Hellman quadruple $E_0, [\mathfrak{a}]E_0, [\mathfrak{b}]E_0, [\mathfrak{a}][\mathfrak{b}]E_0$ now yields the verifiable equality

$$\left(\frac{N(\mathfrak{a})}{m}\right)\left(\frac{N(\mathfrak{b})}{m}\right) = \left(\frac{N(\mathfrak{ab})}{m}\right).$$

However, if $\mathcal{O}$ has ideal classes of both square and non-square norm modulo m, this equality should fail with probability 50% when $[\mathfrak{a}][\mathfrak{b}]$ is replaced by a random ideal class $[\mathfrak{c}] \in \mathrm{Cl}(\mathcal{O})$, thus giving a non-negligible distinguishing advantage.

3.2 Generalized class polynomials

This section accompanies joint work with Marco Streng on *generalized class polynomials*, corresponding to Chapter 6. After introducing (classical) class polynomials, we present and motivate the definition of a multivariate analogue. We then highlight the main results of our joint paper.

3.2.1 Class polynomials

Recall from Section 1.2.2) that the *Hilbert class polynomial* associated to an imaginary quadratic number τ in the complex upper half plane $\mathbf{H}$ is defined as

$$H_\tau(X) = \prod_{\sigma \in \mathrm{Gal}(K(j(\tau))/K)} (X - \sigma(j(\tau))) \in \mathbf{Z}[X]. \tag{3.6}$$

Hilbert class polynomials can be used to construct elliptic curves over finite fields with a prescribed number of points through the CM method; Algorithm 1.2.1. The bottleneck in this algorithm is in the computation of the Hilbert class polynomial; the main reason being that its coefficients are typically large, as illustrated by the following example.

Example 3.2.1 Let $\tau \in \mathbf{H}$ be an imaginary quadratic number of discriminant $D = -103$. Then

$$\begin{aligned} H_\tau(X) \;=\; & X^5 + 70292286280125X^4 + 8547528365929687 5X^3 \\ & + 4941005649165514137656250000X^2 \\ & + 133555277201141655061721191406 25X \\ & + 288266129370140290674661560058 59375. \end{aligned}$$

☆

For larger discriminants the situation gets worse rather quickly. For "typical" discriminants of size 10^9 the total size is already in the gigabytes [13]. One possible idea to remedy this, is to replace the j-function in (3.6) by a different modular function, in the hope that the resulting polynomial will have smaller coefficients. The resulting more general notion of class polynomial is captured by the following definition.

Definition 3.2.2 Let f be a modular function and $\tau \in \mathbf{H}$ imaginary quadratic. If $f(\tau) \in K(j(\tau))$ then we call (f, τ) a *class invariant*, and we define the associated class polynomial by

$$H_\tau[f](X) = \prod_{\sigma \in \mathrm{Gal}(K(f(\tau))/K)} (X - \sigma(f(\tau))).$$

△

Note that $K(f(\tau))/K$ is indeed automatically Galois, since $K(j(\tau))/K$ is an abelian extension.

Example 3.2.3 Let $\mathfrak{f}(z) = \zeta_{48}^{-1}\eta(\frac{z+1}{2})/\eta(z)$, where ζ_{48} is a primitive 48-th root of unity, and

$$\eta(z) = q^{1/24}\prod_{n=1}^{\infty}(1-q^n), \quad \text{where} \quad q = \exp(2\pi i z) \tag{3.7}$$

is the Dedekind η-function. Let τ be as in Example 3.2.1. Then

$$H_\tau[\mathfrak{f}](X) = X^5 + 2X^4 + 3X^3 + 3X^2 + X - 1. \tag{3.8}$$

☆

The modular function $\mathfrak{f}$ from the example is known as *Weber's function* (well, one of three such functions [15, §34]). It is related to the modular j-function by the equation

$$(\mathfrak{f}^{24} - 1)^3 - j\mathfrak{f}^{24} = 0. \tag{3.9}$$

For any τ of discriminant $\equiv 1 \pmod 8$, we have that $(\mathfrak{f}, \tau)$ is a class invariant. The resulting class polynomials can be used in place of Hilbert class polynomials in the CM method; the only extra step one needs is to compute a j-invariant from an "$\mathfrak{f}$-invariant" using (3.9). The phenomenon that the Weber function yields smaller class polynomials can be explained through the following definition.

Definition 3.2.4 The *reduction factor* of a modular function f of level N is

$$r(f) = \frac{\deg(j : X(N) \to \mathbf{P}^1)}{\deg(f : X(N) \to \mathbf{P}^1)}.$$

△

At imaginary quadratic $\tau \in \mathbf{H}$, the value of the modular j-function $j(\tau)$ is an algebraic number (in fact, an algebraic integer). We denote by $h(j(\tau))$ its logarithmic height. For a (possibly multivariate) nonzero polynomial F over $\mathbf{C}$, we denote by $|F|_\infty \in \mathbf{R}_{>0}$ the maximum of the absolute values of its coefficients.

Proposition 3.2.5 *Let f be a modular function that has a q-expansion with coefficients in a number field, and let $\tau_1, \tau_2, \ldots \in \mathbf{H}$ be a sequence of imaginary quadratic*

numbers such that $h(j(\tau_i)) \to \infty$. *Suppose that* $K(f(\tau_i)) = K(j(\tau_i))$ *for all* i. *Then*

$$\frac{\log |H_{\tau_i}[j](X)|_\infty}{\log |H_{\tau_i}[f](X)|_\infty} \to r(f). \tag{3.10}$$

Proof. This result follows from [7, Prop. B.3.5]; see the argument on the bottom of page 9 of [2]. □

Essentially, the proposition says that for a modular function f, asymptotically, the bitsize of the largest coefficient of its class polynomials are a factor $r(f)$ less than that of Hilbert class polynomials. For Weber's function $\mathfrak{f}$, the reduction factor is 72, which means that asymptotically we would require about 72 times fewer digits to write down the largest coefficient of a class polynomial for $\mathfrak{f}$ when compared to j. No modular function with a reduction factor larger than 72 is known. In fact, according to the following result, we cannot do much better.

Theorem 3.2.6 (Bröker–Stevenhagen, 2008) *Let* f *be a modular function. Then* $r(f) \leq 32768/325 \approx 100.82$.

Proof. See [2, Thm. 4.1]. □

The upper bound on $r(f)$ can be further improved to 96 if one assumes Selberg's eigenvalue conjecture [10].

3.2.2 Main contributions

We now highlight results of joint work with Marco Streng. The full version of this work can be found in Chapter 6.

Since the reduction factors of class polynomials are limited by the Bröker-Stevenhagen bound, we considered a multivariate extension that we call *generalized class polynomials*. A univariate polynomial over a field k can be seen as a function on the projective line $\mathbf{P}^1(k)$ whose poles are restricted to the unique point at infinity. Class polynomials can thus be described, up to a multiplicative constant, by their divisor as a function on $\mathbf{P}^1$.

$$\operatorname{div} H_\tau[f] = \sum_{\sigma \in G} (\sigma(f(\tau))) - \#G(\infty), \qquad \text{where } G = \operatorname{Gal}(K(f(\tau))/K).$$

In other words, for a class invariant (f, τ), the class polynomial represents a function on $\mathbf{P}^1$ that has a simple zero at every element of the Galois orbit of $f(\tau)$, and a pole at the unique point at infinity; see Figure 3.1.

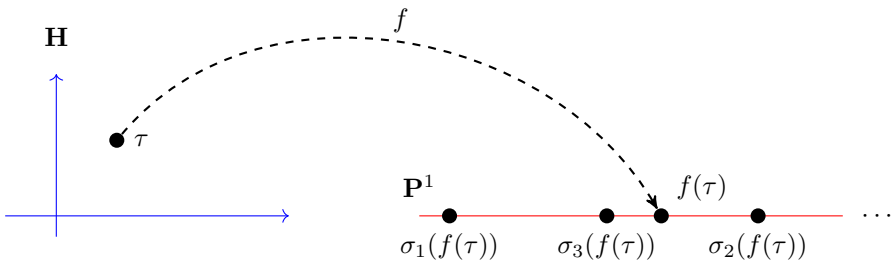

Figure 3.1: The Galois orbit of a class invariant.

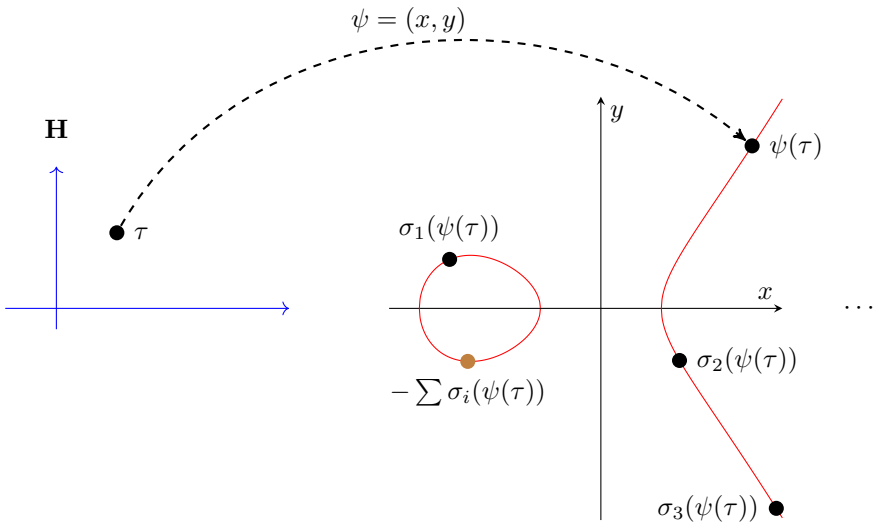

Figure 3.2: The Galois orbit of a pair of class invariants satisfying the equation of an elliptic curve.

Now suppose that we are given, instead of one class invariant, a pair $(x, \tau), (y, \tau)$ of class invariants. Since any pair of modular functions is algebraically dependent, the modular functions x, y satisfy the equation of a (possibly singular) planar curve. Let us suppose for simplicity that this is an elliptic curve E given by a Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Then $\psi(\tau) := (x(\tau), y(\tau))$ defines a point on $E(K(j(\tau))$, hence we can again consider its Galois orbit. Setting $G := \mathrm{Gal}(K(x(\tau), y(\tau))/K)$, the *generalized class polynomial* $H_\tau[E] \in K[X, Y]$ is now defined, uniquely up to a non-zero multiplicative scalar, by

its divisor

$$\operatorname{div} H_\tau[E] = \sum_{\sigma\in G}\Big(\sigma(\psi(\tau))\Big) + \underbrace{\Big(-\sum_{\sigma\in G}\sigma(\psi(\tau))\Big)}_{\text{sum on } E} - (\#G+1)\Big(\infty\Big),$$

where $\infty \in E$ denotes the unique point at infinity. Note that the extra term (the negative of the sum of the points in the Galois orbit) is now necessary to ensure that the resulting divisor is principal; see Figure 3.2.

Example 3.2.7 Consider the modular curve $E = X_+^0(119)$; i.e. the quotient of $X^0(119) = \mathbf{H}/\Gamma^0(119)$ by the Fricke-Atkin-Lehner involution $\tau \mapsto -119/\tau$. Then E is an elliptic curve, and a modular parametrization is given by

$$E : y^2 + 3xy - y = x^3 - 3x^2 + x,$$

where x, y are modular functions for $\Gamma^0(119)$ with q-expansions

$$\begin{aligned} x &= q^{-2} + q^{-1} + 1 + q + 2q^2 + 2q^3 + 3q^4 + 3q^5 + 4q^6 + 5q^7 + \dots \\ y &= q^{-3} + 1 + 2q + 2q^2 + 4q^3 + 4q^4 + 7q^5 + 9q^6 + 12q^7 + \dots \end{aligned}$$

where $q = \exp(2\pi i\tau/119)$. Let τ be an imaginary quadratic number of discriminant -103. Then, further depending on τ, there are two options for the generalized class polynomial:[1]

$$\begin{aligned} H_{\tau_1}[E] &= X^3 + 2X^2 + XY + 2X + Y, \\ H_{\tau_2}[E] &= X^3 - 2X^2 - XY + X + 2Y + 1. \end{aligned}$$

One can compare this with Examples 3.2.1, 3.2.3. ☆

We may expect to estimate the size reduction of the coefficients of generalized class polynomials compared to Hilbert class polynomials through the following generalization of Definition 3.2.4.

Definition 3.2.8 The *reduction factor* of a modular curve C is

$$r(C) := \frac{\deg(j : X(N) \to \mathbf{P}^1)}{\deg(\psi : X(N) \to C)},$$

where ψ is any covering of C by the modular curve $X(N)$ for some $N \in \mathbf{Z}_{>0}$. △

For the case of rational elliptic curves with a finite number of points, this indeed correctly measures the expected asymptotic size reduction.

[1] For $X_0^+(119)$, the number of distinct class polynomials per discriminant is always at most two.

Theorem 3.2.9 (Houben, Streng) *Assume C is an elliptic curve over $\mathbf{Q}$ of rank 0, and that the map $\psi = (x, y) : \mathbf{H} \to \mathbf{C}$ consists of a pair of modular functions corresponding to Weierstrass coordinates of C and whose q-expansions are rational. If $\tau \in \mathbf{H}$ ranges over a sequence of imaginary quadratic points for which $K(\psi(\tau)) = K(j(\tau))$ and*

$$\frac{h(j(\tau))}{\log\log(\#\operatorname{Cl}(\mathcal{O}))} \to \infty, \tag{3.11}$$

then

$$\frac{\log|H_\tau[j]|_\infty}{\log|H_\tau[C]|_\infty} \to r(C). \tag{3.12}$$

Proof. See Theorem 6.3.4. □

For the case of the modular curve in Example 3.2.7, the reduction factor is 72; equal to the one for Weber's function. We did not find any elliptic curve with a reduction factor better than 72. Though this might seem somewhat disappointing, we believe there are several interesting conclusions and challenges for further work. For example:

(i) Weber's function is only known to yield class invariants for discriminants $\equiv 1 \pmod 8$. The generalized class polynomials associated to $X_+^0(119)$ are the first known to yield class invariants of reduction factor ≥ 72 for discriminants $\not\equiv 1 \pmod 8$.

(ii) The coordinate function x on $X_+^0(119)$ yields previously unknown univariate class polynomials. Its reduction factor of 36 already beats all previously known class invariants along a subset of imaginary quadratic discriminants of positive density (defined by a congruence condition). As a result, we expect that the further study of generalized class polynomials could provide new insights into the univariate case as well.

(iii) We know that there exist higher genus curves whose reduction factors exceed the Bröker-Stevenhagen bound. For example, the modular curve $X_+^0(239)$ has genus 3 and reduction factor $r(X_+^0(239)) = 120$. It remains to study whether the analogue of Theorem 3.2.9 holds for this curve.

It should be further noted that Theorem 3.2.9 only provides an asymptotic and concludes nothing about the speed of convergence. Some practical height reduction factors for $X_+^0(119)$, i.e. the left hand side of (3.12), for fundamental discriminants of prime class number are plotted in Figure 3.3.

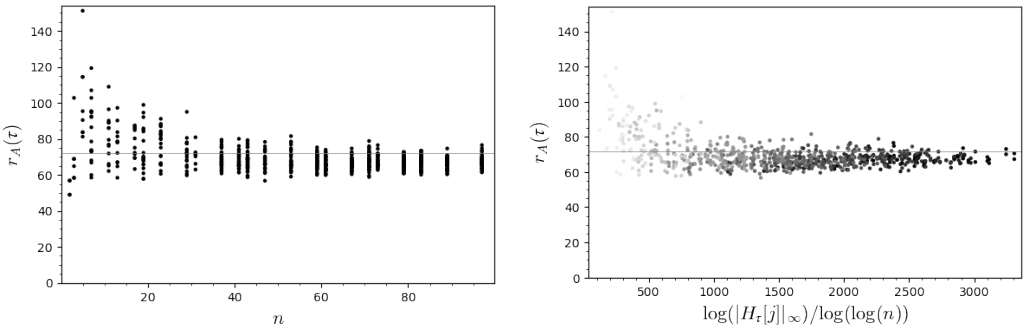

Figure 3.3: Practical reduction factors for $H_\tau[X_+^0(119)]$ for fundamental discriminants D with $\gcd(D, 119) = 1$ and prime class number $n < 100$. In the graph on the right, the x-axis plots the parameter from (3.11), and class polynomials with lower class number correspond to points with a lighter shade.

3.3 Radical isogenies

This section accompanies joint work with Wouter Castryck, Thomas Decru, and Frederik Vercauteren on *horizontal racewalking using radical isogenies*, corresponding to Chapter 7. After introducing and motivating the study of radical isogenies, we summarize and highlight the main contributions of our joint paper.

3.3.1 Computing isogeny chains

One of the main disadvantages of isogeny-based cryptography compared to other post-quantum proposals, such as lattice-based cryptography, is that it is relatively slow. Therefore, there has been continued interest in optimizing the algorithms underlying the evaluation of isogeny-based protocols. Most isogeny-based protocols rely on computing isogenies of small degree between elliptic curves. This often takes the form of *isogeny walks*, such as in Figure 2.6, which typically consist of chains of isogenies of small degree. For example, in CSIDH-512, see Example 2.2.3, one computes isogenies of degree up to 587 in chains of length up to 5. Since isogenies of smaller degree are typically easier to evaluate, a straightforward optimization to the CSIDH protocol is to skew the possible lengths of the chains; i.e. to take longer chains using isogenies of small degree and shorter chains using isogenies of larger degree. This happens, for example, in CSURF-512 [3]. The topic of our research is an attempt to make the evaluation of chains of isogenies of a *given* degree faster. For this, we would like to be able to extend isogeny chains efficiently, i.e., assuming we have computed a chain

$$E_0 \xrightarrow{\varphi_1} E_1 \xrightarrow{\varphi_2} \cdots \xrightarrow{\varphi_k} E_k \tag{3.13}$$

of isogenies of degree N of length $k \geq 1$ such that the composition of the isogenies is cyclic[2] of degree N^k, we would like to efficiently compute an isogeny $\varphi_k : E_k \to E_{k+1}$ of degree N that cyclically extends the chain. More precisely, we study the following problem.

Problem 3.3.1 *Let $E/\mathbf{F}_q$ be an elliptic curve and let $N \in \mathbf{Z}_{>1}$ coprime to $\operatorname{char} \mathbf{F}_q$. Let $P \in E(\mathbf{F}_q)[N]$ and consider the cyclic isogeny $\varphi : E \to E' = E/\langle P \rangle$ of degree N. Find P' on $E'(\overline{\mathbf{F}_q})$ such that the composition $E \xrightarrow{\varphi} E' \to E'/\langle P' \rangle$ is a cyclic isogeny of degree N^2.*

One possible method, if say $E'[N](\mathbf{F}_q) \cong (\mathbf{Z}/N\mathbf{Z})$, is to sample a random point $Q \in E'(\mathbf{F}_q)$, and to multiply by a suitable cofactor $P' := (\#E'(\mathbf{F}_q)/N)Q$. This results in a suitable point P' of order N with probability $\phi(N)/N$, where ϕ is Euler's totient function. However, this is non-deterministic, and relatively slow, since we must multiply a point on $E'(\mathbf{F}_q)$ by the (in case of cryptographic applications) large integer $\#E'(\mathbf{F}_q)/N \approx q$. Alternatively, one could

(i) find the j-invariant of $E'/\langle P' \rangle$ by extracting a root of the modular polynomial $\Phi_N(j(E'), X)$ different from $j(E)$ over $\mathbf{F}_q$; or

(ii) extract a root over $\mathbf{F}_q$ of the N-division polynomial on $E'(\mathbf{F}_q)$,

but these root-finding algorithms are typically even slower. A different approach is suggested by *radical isogenies*, first introduced by Castryck, Decru, and Vercauteren [5]. We will illustrate the idea with an example, which will make use of the following notion.

Definition 3.3.2 Let k be a field of characteristic $p \geq 0$ and let E/k be an elliptic curve. Let $P \in E(k)$ be a point of order $N \geq 4$ such that $p \nmid N$. Then there exist unique $b, c \in k$ such that E admits an isomorphism $\varphi : E \to E_{b,c}$ to the Weierstrass curve

$$E_{b,c} : y^2 + (1-c)xy - by = x^3 - bx^2 \tag{3.14}$$

for which $\varphi(P) = (0,0)$ [12, Lemma 2.1]. Such a Weierstrass model is called the *Tate normal form* of the pair (E, P). △

Example 3.3.3 (Radical 5-isogenies) Consider Problem 3.3.1 for the case $N = 5$. Using the Tate normal form, any elliptic curve with a point of order 5 can be written as

$$E : y^2 - (1-b)xy - by = x^3 - bx^2, \text{ where } P = (0,0).$$

for some value of the parameter b. Instead of specifying this parameter, we consider it as a formal variable and write down the general equation for $E/\langle P \rangle$ using Vélu's

[2] That is, the kernel of the isogeny is a cyclic subgroup of E_0. For example, if N is prime, this is equivalent to the condition that $\ker \varphi_i \neq \ker \hat{\varphi}_{i-1}$ for all $i = 2, \ldots, k$.

formulae (1.3):

$$y^2 + (1-b)xy - by = x^3 - bx^2 - 5b(b^2+2b-1)x - b(b^4+10b^3-5b^2+15b-1).$$

By finding an appropriate root of the 5-division polynomial on this curve, still written in terms of the formal variable b, we can obtain a formula for the coordinates of a 5-torsion point $P' = (x'_0, y'_0)$ on $E/\langle P\rangle$ that cyclically extends the isogeny $E \to E/\langle P\rangle$.

$$\begin{aligned} x'_0 &= 5\alpha^4 + (b-3)\alpha^3 + (b+2)\alpha^2 + (2b-1)\alpha - 2b, \\ y'_0 &= 5\alpha^4 + (b-3)\alpha^3 + (b^2-10b+1)\alpha^2 + (13b-b^2)\alpha - b^2 - 11b, \end{aligned}$$

where $\alpha = \sqrt[5]{b}$. Putting the curve-point pair $(E/\langle P\rangle, P')$ in Tate normal form, we obtain the following Weierstrass model for (the isomorphic curve) $E' \cong E/\langle P\rangle$:

$$E' : y^2 - (1-b')xy - b'y = x^3 - b'x^2, \text{ where } b' = \alpha\frac{\alpha^4+3\alpha^2+4\alpha^2+2\alpha+1}{\alpha^4-2\alpha^3+4\alpha^2-3\alpha+1},$$

thus obtaining an equation for the corresponding Tate-normal-form parameter b' of the curve E'. Now, computing a chain of 5-isogenies of elliptic curves over $\mathbf{F}_q$ amounts to iteratively computing b' from b. If $\gcd(5, q-1) = 1$ then this is deterministic, and, for fields $\mathbf{F}_q$ of cryptographic size, faster than any other known method of computing chains of 5-isogenies. ☆

In general, if (b, c) denote the Tate normal form parameters of a curve E together with a point of order $N > 3$, there exists a formal expression (depending on N) for the Tate normal form parameters (b', c') of a next curve E' in an N-isogeny chain. This expression is an algebraic function of b, c, and $\alpha = \sqrt[N]{\rho(b,c)}$, where $\rho(b, c)$ is another explicit algebraic function of b and c; cf. the formula for b' in Example 3.3.3. Such an expression is known as a *radical isogeny formula* and its general existence was shown in [5, Thm. 5].

3.3.2 Main contibutions

We now highlight results of joint work with Wouter Castryck, Thomas Decru, and Frederik Vercauteren. The full version of this work can be found in Chapter 7.

Though radical isogeny formulae always exist, they are not always easy to find. The approach suggested by Example 3.3.3 to use the N-division polynomial on E' was employed in [5], but proved computationally infeasible for $N > 13$. We developed an alternative way to compute radical isogeny formulae, which allowed to extend the range from $N \leq 13$ up to all primes $N \leq 41$. In addition to that, we rewrote and simplified the formulae up to degree $N = 19$. As an example, we compare expressions for the old and new radical 8-isogeny formulae below.

Example 3.3.4 (Old radical 8-isogeny formula, from [5])

$$\begin{aligned} A' &= \frac{-A^3+6A^2-12A+8}{A^2}\alpha^7 + \frac{4A^3-24A^2+48A-32}{A^3+4A^2-4A}\alpha^6 + \\ &\quad \frac{-4A^3+24A^2-48A+32}{A^3+4A^2-4A}\alpha^5 + \frac{2A^3-12A^2+24A-16}{A^3+4A^2-4A}\alpha^4 + \\ &\quad \frac{A-2}{A}\alpha^3 + \frac{-2A^2+4A}{A^2+4A-4}\alpha^2 + \frac{3A^2-4}{A^2+4A-4}\alpha + \frac{-A^2+2A}{A^2+4A-4}, \end{aligned}$$

where $\alpha = \sqrt[8]{(-A^3+A^2)/(A^4-8A^3+24A^2-32A+16)}$. ☆

This is equivalent to the following.

Example 3.3.5 (New radical 8-isogeny formula, from Chapter 7)

$$A' = \frac{-2A(A-2)\alpha^2 - A(A-2)}{(A-2)^2\alpha^4 - A(A-2)\alpha^2 - A(A-2)\alpha + A},$$

where $\alpha = \sqrt[8]{-A^2(A-1)/(A-2)^4}$. ☆

To evaluate radical isogenies, specifically to obtain α, one needs to compute an N-th root over $\mathbf{F}_p$. If p is odd, then for even degrees N such an N-th root is never unique. It turns out that choosing an incorrect root sometimes yields an N-isogeny that does not come from the class group action, i.e. an isogeny that is not *horizontal* in the sense of Lemma 1.2.2. We conjectured, and proved for $N \leq 14$, a simple criterion to select the right root, which allows for faster deterministic computation of isogeny walks in even degree. The combined optimizations and improvements to the radical isogeny formulae led to a speed up of 12% over the previous implementation of CSIDH-512 using radical isogenies (which in turn obtained a speed up of 19% over an implementation of 512-bit CSIDH without radical isogenies [1]). Using radical 16-isogenies, we obtained about a factor of 3 speed up for the computation of long chains of 2-isogenies over 512-bit prime fields.

3.4 Bibliography

[1] Daniel J. Bernstein, Luca De Feo, Antonin Leroux, and Benjamin Smith. Faster computation of isogenies of large prime degree. In *ANTS XIV—Proceedings of the Fourteenth Algorithmic Number Theory Symposium*, volume 4 of *Open Book Ser.*, pages 39–55. Math. Sci. Publ., Berkeley, CA, 2020.

[2] Reinier Bröker and Peter Stevenhagen. Constructing elliptic curves of prime order. In *Computational arithmetic geometry*, volume 463 of *Contemp. Math.*, pages 17–28. Amer. Math. Soc., Providence, RI, 2008.

[3] Wouter Castryck and Thomas Decru. CSIDH on the surface. In Jintai Ding and Jean-Pierre Tillich, editors, *PQCrypto 2020*, volume 12100 of *Lecture Notes in Computer Science*, pages 111–129. Springer, 2020.

[4] Wouter Castryck and Thomas Decru. An efficient key recovery attack on SIDH. In *Eurocrypt 2023 Pt. 5*, volume 14008 of *Lecture Notes in Computer Science*, pages 423–447. Springer, 2023.

[5] Wouter Castryck, Thomas Decru, and Frederik Vercauteren. Radical isogenies. In *Proceedings of Asiacrypt 2020 Part II*, volume 12492 of *Lecture Notes in Computer Science*, pages 493–519. Springer, 2020.

[6] Wouter Castryck, Jana Sotáková, and Frederik Vercauteren. Breaking the decisional Diffie-Hellman problem for class group actions using genus theory. In *Crypto 2020 Pt. 2*, volume 12171 of *Lecture Notes in Computer Science*, pages 92–120. Springer, 2020.

[7] Marc Hindry and Joseph H. Silverman. *Diophantine geometry*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. An introduction.

[8] Luciano Maino, Chloe Martindale, Lorenz Panny, Giacomo Pope, and Benjamin Wesolowski. A direct key recovery attack on SIDH. In *Eurocrypt 2023 Pt. 5*, volume 14008 of *Lecture Notes in Computer Science*, pages 448–471. Springer, 2023.

[9] Damien Robert. Breaking SIDH in polynomial time. In *Eurocrypt 2023 Pt. 5*, volume 14008 of *Lecture Notes in Computer Science*, pages 472–503. Springer, 2023.

[10] Atle Selberg. On the estimation of Fourier coefficients of modular forms. In *Proc. Sympos. Pure Math., Vol. VIII*, pages 1–15. Amer. Math. Soc., Providence, R.I., 1965.

[11] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, second edition, 2009.

[12] Marco Streng. Generators of the group of modular units for $\Gamma^1(N)$ over the rationals. *Ann. H. Lebesgue*, 6:95–116, 2023.

[13] Andrew V. Sutherland. Accelerating the CM method. *LMS J. Comput. Math.*, 15:172–204, 2012.

[14] David Urbanik and David Jao. SoK: The problem landscape of SIDH. In *Proceedings of the 5th ACM on ASIA Public-Key Cryptography Workshop*, APKC '18, page 53–60, New York, NY, USA, 2018. Association for Computing Machinery.

[15] H. Weber. *Lehrbuch der Algebra*, volume III. Chelsea Publishing Company, 1902.