Towards Computing Cyclic Isogenies for the Discrete Logarithm Problem for Curves of Genus 2

Dudeanu Alina
LACAL, I&C, EPFL

***Abstract*—The difficulty of the Discrete Logarithm Problem (DLP) in some specific groups G is the basis for many cryptographical schemes. The classical choice is the multiplicative group $\mathbb{Z}/p\mathbb{Z}^*$, p a large prime, for whom the best known running time attack is subexponential in $\log p$ [1].**

In order to overcome subexponential attacks, one could pick G as a large prime order group $E(\mathbb{K})$ of points on an ordinary, non-anomalous elliptic curve E defined over a finite field $\mathbb{K}$. These constraints on $\#E(\mathbb{K})$ are due to current attacks. The curves over $\mathbb{K}$, with the same $\#E(\mathbb{K})$, can be linked through a rational map, called isogeny, that preserves the group structure. Providing the computation of the isogeny between two curves is feasible, one can reduce the DLP on a strong curve to the DLP on a vulnerable one (assuming it exists). This is equivalent to determine a path in the isogeny graph between two vertexes that represent different isomorphism classes of isogenous curves. The structure of the graph is due to the connection between endomorphism rings of elliptic curves and orders $\mathcal{O}$ in the same imaginary quadratic field, between $\mathcal{O}$-ideal classes and isogenies.

A natural topic of research is the study whether a similar argument for the DLP on genus 2 curves exists.

***Index Terms*—discrete logarithm problem, isogenies, elliptic curves, imaginary quadratic fields, orders, ideal class group**

Proposal submitted to committee: August 21st, 2012; Candidacy exam date: August 28th, 2012; Candidacy exam committee: Ruediger Urbanke, Arjen Lenstra, Philippe Michel.

This research plan has been approved:

Date: _____

Doctoral candidate: _____
(name and signature)

Thesis director: _____
(name and signature)

Thesis co-director: _____
(if applicable) (name and signature)

Doct. prog. director: _____
(R. Urbanke) (signature)

I. Introduction

Isogenies play an important role in the theory of elliptic curves and its application to cryptography. The Elliptic Curve Discrete Logarithm Problem (ECDLP) is one of the main applications and a current goal in cryptanalysis is still finding an attack that is faster than Pollard-rho [16] for more classes of elliptic curves defined over finite fields.

Definition 1 (ECDLP): Let E be an elliptic curve over a finite field $\mathbb{F}_q$. Let N be the order of the group $E(\mathbb{F}_q)$ and let $P \in E(\mathbb{F}_q)$. Given $r = \mathrm{ord}(P)$ and $Q \in \langle P \rangle$, find the unique integer $m \in [0, \ldots, r-1]$ such that $Q = [m]P$.

Two elliptic curves $\mathbf{E}_1, \mathbf{E}_2$ over $\mathbb{F}_q$, with $\#\mathbf{E}_1(\mathbb{F}_q) = \#\mathbf{E}_2(\mathbb{F}_q)$, are isogenous over $\mathbb{F}_q$ and since an isogeny is a group homomorphism, one can relate the two logarithm problems. Therefore, a natural question is whether the ECDLP is equally hard for both curves and extrapolating, for every elliptic curve over the same finite field having the same number of points. For most elliptic curves defined in this manner, the work of Jao, Miller and Venkatesen [13] gives an affirmative formal response. It depends on the one-to-one correspondence between ideal classes of an order in an imaginary quadratic field and the elliptic curve isomorphism classes with the same endomorphism ring.

Moreover, this correspondence leads to an extension by Galbraith, Hesse and Smart in [8] of the Weil descent attack in [11], applied to elliptic curves defined over fields of the form $\mathbb{F}_{q^n}$, where $q = 2^l$ and the positive integers l, n are coprime. The GHS reduces the ECDLP in $\mathbf{E}(\mathbb{F}_{q^n})$ to the DLP in a subgroup of the Jacobian $J_C(\mathbb{F}_q)$ of an hyperelliptic curve over $\mathbb{F}_q$.

Definition 2: A *hyperelliptic curve* C over a finite field $\mathbb{F}_q$ is defined by

$$C : y^2 + h(x)y = f(x), \qquad h, f \in \mathbb{F}_q[x]$$

with $\deg(h) \leq g$ and $\deg(f) = 2g + 1$. The integer $g \geq 0$ is the *genus* of the curve and elliptic curves correspond to the $g = 1$ case.

The Jacobian of a curve C is isomorphic to $Pic^0(\mathbf{C})$, defined in the next section, and it could be used for cryptographic purposes. Therefore, a point of interest is the study of the DLP for isogenous hyperelliptic curves. A first future step is to determine the structure of the isogeny graph. In our research we will focus mainly on curves of genus 2 or 3 because for curves of higher genus, Adleman et al. [2] provided a subexponential algorithm. Smith proved in [19] that approximately 18% of the hyperelliptic curves of genus

3 are prone to an index-calculus attack [1].

II. Curves

In this section, the main focus is introducing concepts in algebraic geometry that are indispensable for defining a genus g curve, and in particular an elliptic curve. The main reference is Silverman's book on elliptic curves [18, Chapter I,II].

Let $\mathbb{K}$ be a field of arbitrary characteristic and let $\overline{\mathbb{K}}$ be the algebraic closure of $\mathbb{K}$. Consider the affine plane $\mathbb{A}^2(\overline{\mathbb{K}}) = \{(x,y) \,|\, x,y \in \overline{\mathbb{K}}\}$ and the projective plane $\mathbb{P}^2(\overline{\mathbb{K}}) = \{[x:y:z] \,|\, x,y,z \in \overline{\mathbb{K}}\}$ of equivalence classes representing projective points. A curve over $\mathbb{K}$ is a projective algebraic variety of dimension one i.e, there is a homogeneous polynomial $\mathbf{f} \in \mathbb{K}[x,y,z]$ such that for all projective points $P \in \mathbf{C}$, $\mathbf{f}(P) = 0$.

Let $\mathbf{C}$ be a curve defined over $\mathbb{K}$ and consider its affine equation $\mathbf{f}(x,y) = 0$. Let $\mathbb{K}[\mathbf{C}]$ be the affine coordinate ring, polynomials over $\mathbb{K}$, modulo $\mathbf{f}$. $\mathbb{K}[\mathbf{C}]$ is an integral domain and its field of fractions $\mathbb{K}(\mathbf{C})$ is called the function field of $\mathbf{C}$ over $\mathbb{K}$.

Consider the point on the curve $P \in \mathbf{C}$ and let $M_P = \{f \in \overline{\mathbb{K}}[\mathbf{C}] \,|\, f(P) = 0\}$ be the maximal ideal of the local ring of $\mathbf{C}$ at P, $\overline{\mathbb{K}}[\mathbf{C}]_P = \{F \in \overline{\mathbb{K}}(\mathbf{C}) : F = f/g \text{ for some } f,g \in \overline{\mathbb{K}}[\mathbf{C}] \text{ and } g(P) \neq 0\}$.

One states that $f \in \overline{\mathbb{K}}(\mathbf{C})$ is regular at P if and only if $f \in \overline{\mathbb{K}}[\mathbf{C}]_P$, meaning f can be evaluated at P. A rational map between curves is $\phi = [f_1, f_2] : \mathbf{C}_1 \to \mathbf{C}_2$, with $\mathbf{C}_1, \mathbf{C}_2$ curves defined over the same field $\mathbb{K}$ and for all $P \in \mathbf{C}_1$ with $f_i \in \overline{\mathbb{K}}[\mathbf{C}_1]_P$, $\phi(P) \in \mathbf{C}_2$.ϕ is a regular map at P if there is $g \in \overline{\mathbb{K}}(\mathbf{C}_1)$ such that gf_1, gf_2 are regular at P and at least one of them is non-zero. A **morphism** $\phi : \mathbf{C}_1 \to \mathbf{C}_2$ is a rational map regular at any point $P \in \mathbf{C}_1$.

In order to understand the properties of a morphism, we introduce the notions of order and ramification index further on. Consider a smooth (non-singular) point $P \in \mathbf{C}$ i.e., $\frac{\partial \mathbf{f}}{\partial x}(P) \neq 0$ or $\frac{\partial \mathbf{f}}{\partial y}(P) \neq 0$. The **order of a function** f **in** $\overline{\mathbb{K}}[\mathbf{C}]_P$ **at** P is denoted as $ord_P(f)$ and is the integer $d > 0$ such that $f \in M_P^d$, but $f \notin M_P^{d+1}$. One extends the notion to rational functions, for $F = f/g \in \overline{\mathbb{K}}(\mathbf{C})$ we have $ord_P(F) = ord_P(f) - ord_P(g)$. In this context, P is a zero of f if $ord_P(F) > 0$ and a pole if $ord_P(F) < 0$. The function F is well regular at P if $ord_P(F) \geq 0$, otherwise we write $f(P) = \infty$. In case $ord_P(F) = 1$, F is called an **uniformizer at** P**.**

Utilizing the above mathematical concepts, Silverman demonstrates in [18] that a rational map $\phi : \mathbf{C}_1 \to \mathbf{C}_2$ is actually a morphism when $\mathbf{C}_1$ is a smooth curve. One can prove that ϕ is either constant or surjective $\phi(\mathbf{C}_1) = \mathbf{C}_2$, and it induces an injection of function fields: $\phi^* : \mathbb{K}(\mathbf{C}_2) \to \mathbb{K}(\mathbf{C}_1)$ of the form $\phi^*(f) = f \circ \phi$. Moreover $\mathbb{K}(\mathbf{C}_1)$ is a finite field extension of $\phi^*(\mathbb{K}(\mathbf{C}_2))$ and one defines the **degree of a non-constant morphism** as the degree of the extension $[\mathbb{K}(\mathbf{C}_1) : \phi^*(\mathbb{K}(\mathbf{C}_2))]$. We say that ϕ is separable, inseparable or purely inseparable depending on the corresponding field extension property. A degree one morphism between smooth curves is an isomorphism.

One defines the **ramification index of** ϕ **at** P as $e_\phi(P) = ord_P(\phi^* t_{\phi(P)})$, where $t_{\phi(P)}$ is a uniformizer at $\phi(P)$. Then, the degree of a non-constant morphism between smooth curves is equal to $\sum_{P \in \phi^{-1}(Q)} e_\phi(P)$ independent of $Q \in \mathbf{C}_2$. Thus, the degree is the number of different points on the first curve, together with their multiplicity, corresponding via the rational map to a particular point on the second curve. If $e_\phi(P) = 1$ for all P, then the map is unramified and for all $Q \in \mathbf{C}_2$, $deg\, \phi = \#\phi^{-1}(Q)$.

One denotes $Div(\mathbf{C})$ as the **divisor group of a curve** $\mathbf{C}$ and any element $D \in Div(\mathbf{C})$ is of the form $\sum_{P \in \mathbf{C}} n_P(P)$, with $n_P \in \mathbb{Z}$ and $n_P \neq 0$ for finitely many P. The degree of a divisor is $\sum_{P \in \mathbf{C}} n_P$. D is effective if, by definition, $n_P \geq 0$ for all $P \in \mathbf{C}$. One writes $D_1 \geq D_2$ if $D_1 - D_2$ is effective.

Let f be a rational function in $\overline{\mathbb{K}}(\mathbf{C})^*$, $\mathbf{C}$ smooth. Naturally, we define the divisor of f as $div(f) = \sum_{P \in \mathbf{C}} ord_P(f)(P)$. We notice that $deg(div(f)) = 0$ and consequently, the map $div : \overline{\mathbb{K}}(\mathbf{C})^* \to Div^0(\mathbf{C})$ is a group homomorphism, $Div^0(\mathbf{C})$ is the degree 0 divisors. A **principal divisor** is then a divisor corresponding to a rational function f and two divisors are linearly equivalent, $D_1 \sim D_2$, iff there is a rational function $f \in \overline{\mathbb{K}}(\mathbf{C})^*$ such that $D_1 - D_2 = div(f)$. The **Picard group** or the divisor class group $Pic(\mathbf{C})$ is the divisor group of $\mathbf{C}$ modulo the principal divisors $Princ(\mathbf{C})$. The degree 0 divisor class group $Div^0(\mathbf{C})/Princ(\mathbf{C})$ is denoted $Pic^0(\mathbf{C})$.

Next step is to define a canonical divisor. First let $\Omega_{\mathbf{C}}$ be the **set of differentials over** $\mathbf{C}$. In [18] it is stated that $\Omega_{\mathbf{C}}$ is a one dimensional $\overline{\mathbb{K}}(\mathbf{C})$-vector space and dx is a basis for $x \in \overline{\mathbb{K}}(\mathbf{C})$ iff $\overline{\mathbb{K}}(\mathbf{C})/\overline{\mathbb{K}}(x)$ is a finite separable extension. Automatically, when t is an uniformizer at P on the curve $\mathbf{C}$ and $\omega \in \Omega_{\mathbf{C}}$, there exists an unique function g depending on ω and t such that $\omega = gdt$. The value $ord_P(g)$ is independent of the choice of t and thus, we can define $ord_P(\omega) := ord_P(g)$. The divisor associated to the differential is $div(\omega) = \sum_{P \in \mathbf{C}} ord_P(\omega)P$ and it is well defined as $ord_P(\omega)$ is non-zero for finitely many points. A differential ω is holomorphic if $ord_P(\omega) \geq 0$ for all $P \in \mathbf{C}$ and non-vanishing if $ord_P(\omega) \leq 0$ for all $P \in \mathbf{C}$. Since for any non-zero $\omega_1, \omega_2 \in \Omega_{\mathbf{C}}$ there exists $f \in \overline{\mathbb{K}}(\mathbf{C})$ such that $\omega_2 = f\omega_1$, we can define the **canonical class on** $\mathbf{C}$ as the image in $Pic(\mathbf{C})$ of $div(\omega)$, for any $\omega \in \Omega_{\mathbf{C}}^*$.

Next, in order to finally state the Riemann-Roch theorem, we define $\mathcal{L}(D)$ as $\{0\} \cup \{f \in \overline{\mathbb{K}}(\mathbf{C})^* \,|\, div(f) \geq -D\}$. The dimension of $\mathcal{L}(D)$ as a vector space over $\overline{\mathbb{K}}$ is denoted $l(D)$. For instance in case of a canonical divisor on $\mathbf{C}$, $K_{\mathbf{C}} = div(\omega) \in Div(\mathbf{C})$, then there is an isomorphism between the set of holomorphic differentials on $\mathbf{C}$ and $\mathcal{L}(K_{\mathbf{C}})$ as any other differential is of the form $f\omega$, for some $f \in \overline{\mathbb{K}}(\mathbf{C})^*$.

Theorem 1: Let $\mathbf{C}$ be a smooth curve defined over $\mathbb{K}$ and let $K_{\mathbf{C}}$ be a canonical divisor on $\mathbf{C}$. Then there is an integer $g \geq 0$, called the **genus of the curve**, such that for any divisor $D \in Div(\mathbf{C})$,

$$l(D) - l(K_{\mathbf{C}} - D) = deg(D) - g + 1. \tag{1}$$

III. Elliptic Curves

Definition 3: An elliptic curve $\mathbf{E}$ defined over $\mathbb{K}$, denoted $\mathbf{E}/\mathbb{K}$, is a non-singular genus one curve over $\mathbb{K}$, together with a point $\mathcal{O} \in \mathbf{E}(\mathbb{K})$.

Proposition 1 ([18]): Let $\mathbf{E}$ be an elliptic curve defined over $\mathbb{K}$.

- There exist functions $x, y \in \mathbb{K}(\mathbf{E})$ such that $\phi : \mathbf{E} \to \mathbf{P}^2(\mathbb{K})$, $\phi = [x, y, 1]$, gives an isomorphism from $\mathbf{E}/\mathbb{K}$ to a smooth curve given by Weierstrass equation
$$Y^2Z+a_1XYZ+a_3YZ^2 = X^3+a_2X^2Z+a_4XZ^2+a_6Z^3 \quad (2)$$
with coefficients in $\mathbb{K}$ and $\phi(\mathcal{O}) = [0 : 1 : 0]$.
- Conversely, every smooth Weierstrass curve as above, together with $[0 : 1 : 0]$, is an elliptic curve defined over $\mathbb{K}$ with base point $\mathcal{O} = [0 : 1 : 0]$.
- Given two pairs of Weierstrass coordinates (x, y) and (x', y') of the same curve $\mathbf{E}$, they are related through
$$x = u^2x' + r \text{ and } y = u^3y' + u^2sx' + t$$
where $u, r, s, t \in \mathbb{K}$ and $u \neq 0$.

Assume $char(\mathbb{K}) \neq 2, 3$. After two consecutive changes of variables:
$$y \to \frac{1}{2}(y - a_1x - a_3)$$
and
$$(x, y) \to \left(\frac{x - 3d_2}{36}, \frac{y}{108}\right)$$
where $d_2 = a_1^2+4a_2$, the elliptic curve has a short Weierstrass equation:
$$E : y^2 = x^3 - 27c_4x - 54c_6. \quad (3)$$
One denotes $c_4 = d_2^2 - 24d_4$ and $c_6 = -d_2^3 + 36d_2d_4 - 216d_6$, where $d_4 = 2a_4 + a_1a_3$, $d_6 = a_3^2 = 4a_6$ and $d_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$.

The condition of smoothness is equivalent to a non-zero discriminant of the Weierstrass equation
$$\Delta = \frac{c_4^3 - c_6^2}{1728}.$$
In case of a singular curve, the only singular point is a node if $c_4 = 0$ and a cusp if $c_4 \neq 0$. One also defines the j-invariant as a value in $\mathbb{K}$ that identifies the isomorphism class of $\mathbf{E}/\mathbb{K}$, meaning every isomorphic curve to $\mathbf{E}/\mathbb{K}$ has the same j-invariant. For instance for the short Weierstrass equation
$$j = c_4^3/\Delta,$$
Particular values are 0 when $c_4 = 0$ and 1728 when $c_6 = 0$. Let ω be the differential associated to the Weierstrass equation. Proposition III.1.5 of Silverman [18] shows that ω has neither poles, nor zeros and thus, $div(\omega) = 0$.

One restricts to $char(\mathbb{K}) \neq 2, 3$ for simplicity and let $\mathbf{E}/\mathbb{K} : y^2 = x^3 + ax + b$.

One defines an additive group law on $\mathbf{E}(\mathbb{K})$ in the following manner based on Bezout's theorem. Taking $P, Q \in \mathbf{E}(\mathbb{K})$, the line l_{PQ} through both of them (if $P = Q$ take the tangent at $\mathbf{E}$ in P) intersects the curve in a third point $R \in \mathbf{E}(\mathbb{K})$. Constructing the vertical through R it intersects the curve in $\mathcal{O}$ and a third point which we consider as $P + Q$.

The composition law has all the properties of a group law, i.e, symmetry, associativity, the identity element $\mathcal{O}$ and the existence of a unique inverse of any given element. In order to derive the explicit formulas, one writes the equation of l_{PQ}, substitutes it in the equation of $\mathbf{E}$ and takes the opposite of the point of intersection, i.e. for $R(x, y)$ the opposite is $(x, -y)$. The addition result is $(P + Q)(x_3, y_3) = P(x_1, y_1) + Q(x_2, y_2)$, with
$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2, \quad y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1.$$
When $P \neq -P$, the double $2P(x_3, y_3)$ has
$$x_3 = \left(\frac{3x^2 + a}{2y}\right)^2 - 2x, \quad y_3 = \left(\frac{3x^2 + a}{2y}\right)(x - x_3) - y.$$
These formulas are put in practice when computing $[m]P = \underbrace{P + ... + P}_{=m,\, m>0}$ or $[m]P = \underbrace{-P - ... - P}_{=m,\, m<0}$.

The geometric group law above is the same as the algebraic group law defined on the zero-degree divisors in $Pic^0(\mathbf{E})$. As proven in [18], any $D \in Div^0(\mathbf{E})$ is equivalent to $(P) - (\mathcal{O})$, with P uniquely determined on the curve and thus, the map $\sigma : Pic^0(\mathbf{E}) \to \mathbf{E}$, $(P) - (\mathcal{O}) \to P$ is a bijection of sets and a group homomorphism.

IV. Isogenies

Definition 4: A **non-zero isogeny** $\phi : \mathbf{E}_1 \to \mathbf{E}_2$ of degree d over $\mathbb{K}$ is a morphism of degree d over $\mathbb{K}$ with $\phi(\mathcal{O}_1) = \mathcal{O}_2$. Two elliptic curves are isogenous if there is a non-zero isogeny from $\mathbf{E}_1$ to $\mathbf{E}_2$.

In case $\phi = [0]$ then $deg(\phi) = 0$, otherwise $\phi(\mathbf{E}_1) = \mathbf{E}_2$. Since ϕ is a morphism of curves, there is an injection $\phi^* : \mathbb{K}(\mathbf{E}_2) \to \mathbb{K}(\mathbf{E}_1)$ and the type of isogeny corresponds to a particular type of field extension. One denotes by $Hom(\mathbf{E}_1, \mathbf{E}_2)$ the group of isogenies from $\mathbf{E}_1$ to $\mathbf{E}_2$ where for each $P \in \mathbf{E}_1$, we get $(\phi+\psi)(P) = \phi(P)+\psi(P)$. One can prove as in [18] that $Hom(\mathbf{E}_1, \mathbf{E}_2)$ is a torsion-free $\mathbb{Z}$-module.

In case the curves are identical, we can consider the composition of isogenies as a multiplication law, for each point $P \in \mathbf{E}$, $(\phi \cdot \psi)(P) = \phi(\psi(P))$. Moreover it is distributive over addition and thus, $Hom(\mathbf{E}, \mathbf{E})$ proves to be a ring, the **endomorphism ring of $\mathbf{E}$** and is denoted by $End(\mathbf{E})$. This ring is crucial in the next sections of the paper. The invertible elements of $End(\mathbf{E})$ form the automorphism group of an elliptic curve. First properties of $End(E)$ are the characteristic zero, the lack of zero divisors [18, Proposition III.4.2], and being a $\mathbb{Z}$-module of rank at most four as in [18, Corollary III.7.5].

Taking the previous sections into account, the multiplication by m on the set of points is a non-zero isogeny that acts on the same curve. The degree of this isogeny is m^2, a fact that gives the structure of the m-torsion subgroup of $\mathbf{E}$, $\mathbf{E}[m] = \{P \in \mathbf{E} \,|\, [m]P = \mathcal{O}\}$, as being isomorphic to a product of two cyclic groups $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. For a curve $\mathbf{E}/\mathbb{K}$, the torsion subgroup of $\mathbf{E}$ is the group $\mathbf{E}_{tors}(\mathbb{K})$ of points of finite order with coordinates in $\mathbb{K}$.

In case $char(\mathbb{K}) = p$, another isogeny is the **Frobenius endomorphism** π_q, with $\#\mathbb{K} = q = p^n$ for some integer $n > 0$, that is defined as $\pi_q : \mathbf{E} \to \mathbf{E}$, $(x, y) \to (x^q, y^q)$ and fixes $\mathbf{E}(\mathbb{K})$. The isogeny is purely inseparable of degree q.

Next, we list some important properties of a non-zero isogeny that appear mostly in [18]:

- An isogeny $\phi : \mathbf{E}_1 \to \mathbf{E}_2$ defined over $\mathbb{K}$ is a **group homomorphism** from $\mathbf{E}_1(\mathbb{K})$ to $\mathbf{E}_2(\mathbb{K})$ as $\phi(P+Q) = \phi(P) + \phi(Q)$ for all $P, Q \in \mathbf{E}_1$.
- The kernel of any isogeny $Ker_\phi = \{P \in \mathbf{E}_1 \mid \phi(P) = \mathcal{O}_2\}$ is finite and of order at most the degree of the isogeny.
- The separable degree of an isogeny is given by the cardinality of the set $\phi^{-1}(Q)$ for any $Q \in \mathbf{E}_2$ and the inseparable degree is the ramification index $e_\phi(P)$ for any $P \in \mathbf{E}_1$. The degree of the isogeny becomes $deg(\phi) = deg_s(\phi) \cdot deg_i(\phi)$. A separable isogeny is unramified and thus, has degree $\#Ker_\phi$ or $\#\phi^{-1}(P)$ for any $P \in \mathbf{E}_2$.
- *Theorem 2 ([7]):* Let $\mathbf{E}_1, \mathbf{E}_2, \mathbf{E}_3$ be elliptic curves over $\mathbb{K}$ and $\phi : \mathbf{E}_1 \to \mathbf{E}_2$, $\psi : \mathbf{E}_1 \to \mathbf{E}_3$ isogenies over $\mathbb{K}$. Let $Ker_\phi \subseteq Ker_\psi$ and ψ be separable.
  Then there is an unique isogeny $\lambda : \mathbf{E}_2 \to \mathbf{E}_3$ defined over $\mathbb{K}$ such that $\psi = \lambda \circ \phi$.
- *Theorem 3 ([7]):* Let $\mathbf{E}_1, \mathbf{E}_2$ be two elliptic curves defined over a finite field $\mathbb{K}$. There exists an isogeny $\phi : \mathbf{E}_1 \to \mathbf{E}_2$ over $\mathbb{K}$ if and only if the curves have the same number of points with coordinates in $\mathbb{K}$ i.e., $\#\mathbf{E}_1(\mathbb{K}) = \#\mathbf{E}_2(\mathbb{K})$.
  The converse implication is called Tate' isogeny theorem.
- For any isogeny $\phi : \mathbf{E}_1 \to \mathbf{E}_2$ over $\mathbb{K}$ of degree m, there is a unique isogeny of the same degree, called the **dual isogeny**, $\hat{\phi} : \mathbf{E}_2 \to \mathbf{E}_1$ such that $\phi \circ \hat{\phi} = [m]_{\mathbf{E}_2}$ and $\hat{\phi} \circ \phi = [m]_{\mathbf{E}_1}$. Other properties are stated in Theorem III.6.2 of [18].
  We specify them for $\mathbf{E}_1 = \mathbf{E}_2 = \mathbf{E}$, as the dual provides an anti-involution for the endomorphism ring $End(\mathbf{E})$. For any $\lambda : \mathbf{E} \to \mathbf{E}$ isogeny, $\widehat{(\lambda\phi)} = \hat{\phi} \cdot \hat{\lambda}$, $\widehat{(\lambda + \phi)} = \hat{\lambda} + \hat{\phi}$ and $\hat{\hat{\phi}} = \phi$. The definition of the dual isogeny, together with the fact that the degree map from $End(\mathbf{E})$ to $\mathbb{Z}$ is a positive definite quadratic form, proves that $\phi\hat{\phi}$ is a non-negative integer that is zero if and only if $\phi = [0]$.
  Taking all these characteristics into account, Theorem III.9.3 from [18] proves that the endomorphism ring $End(\mathbf{E})$ is one of the following types:
  a) isomorphic to $\mathbb{Z}$
  b) an order in an imaginary quadratic extension of $\mathbb{Q}$
  c) an order in a quaternion algebra over $\mathbb{Q}$
  If $char(\mathbb{K}) = 0$, the last case is impossible due to the commutative property of the endomorphism ring. If $\mathbb{K} = \mathbb{F}_q$ and $char(\mathbb{K}) = p$, the first case is impossible as proven in [18]. The third case is the case of supersingular curves, i.e, curves that have $\#\mathbf{E}(\mathbb{K}) = 1 \bmod p$.
  Thus, **the endomorphism of an ordinary (non-supersingular) elliptic curve over a finite field is an order in an imaginary quadratic field.** Moreover, any non-zero isogeny ϕ, including the Frobenius endomorphism, satisfies a quadratic characteristic polynomial, for each point $P \in E(\overline{\mathbb{K}})$,

$$\phi(\phi(P)) - [t]\phi(P) + [d]P = \mathcal{O}$$

  where $d = deg(\phi)$ and the integer t is the trace of the endomorphism.
  In case of the Frobenius, the characteristic polynomial $P(X) = X^2 - tX + q$ evaluated in 1 gives the cardinality of the group of points $\mathbf{E}(\mathbb{K})$. The Hasse theorem states that $-2\sqrt{q} \leq t \leq 2\sqrt{q}$ and thus, in case of ordinary elliptic curves, $t^2 - 4q < 0$ and we can identify the Frobenius with a complex number π_q, root of the polynomial P, and algebraic integer in the quadratic field $\mathbb{Q}[\sqrt{t^2 - 4q}]$. Hence, $\mathbb{Z}[\pi_q] \subseteq End(E)$ and both of them are orders in $\mathbb{Q}[\sqrt{t^2 - 4q}]$.

V. Orders in Quadratic Fields

In this section, we briefly define orders in quadratic fields and list some properties that are indispensable for the study of the endomorphism ring of a curve defined over a finite field.

A **number field** $\mathbb{K}$ is a finite degree extension of $\mathbb{Q}$. The degree d of $\mathbb{K}$ over $\mathbb{Q}$ is denoted $[\mathbb{K} : \mathbb{Q}]$. The set of all $\alpha \in \mathbb{K}$ that are roots of a monic integer polynomial is called the ring of algebraic integers of $\mathbb{K}$, denoted $\mathcal{O}_\mathbb{K}$. According to [15], $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$.

A quadratic field is a degree 2 extension of $\mathbb{Q}$, of the form $\mathbb{Q}[\sqrt{N}]$ where $N \neq 0, 1$ is a square free integer. $\mathbb{K}$ is called an **imaginary quadratic field** if $N < 0$ and it is called a **real quadratic field** otherwise.

The discriminant $d_\mathbb{K}$ of $\mathbb{Q}[\sqrt{N}]$ is defined to be

$$d_\mathbb{K} = \begin{cases} N & \text{if } N \equiv 1 \bmod 4 \\ 4N & \text{otherwise.} \end{cases}$$

The ring of integers becomes

$$\mathcal{O}_\mathbb{K} = \begin{cases} \mathbb{Z}[\sqrt{N}] & \text{if } N \not\equiv 1 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{N}}{2}\right] & \text{if } N \equiv 1 \pmod 4 \end{cases}$$

or equivalently,

$$\mathcal{O}_\mathbb{K} = \mathbb{Z}\left[\frac{d_\mathbb{K} + \sqrt{d_\mathbb{K}}}{2}\right].$$

Therefore, we can write the ring of integers in $\mathbb{Q}[\sqrt{N}]$ as a lattice in $\mathbb{Z}^2$, i.e., a $\mathbb{Z}$-module of basis $[1, w_\mathbb{K}]$ where $w_\mathbb{K} = \frac{d_K + \sqrt{d_K}}{2}$.

Definition 5 ([5]): An **order** $\mathcal{O}$ in a quadratic field $\mathbb{K}$ is a subset $\mathcal{O} \subset \mathbb{K}$ such that

(i) $\mathcal{O}$ is a subring of $\mathbb{K}$ containing 1.
(ii) $\mathcal{O}$ is a finitely generated $\mathbb{Z}$-module.
(iii) $\mathcal{O}$ contains a $\mathbb{Q}$-basis of $\mathbb{K}$.

Clearly, $\mathcal{O}_\mathbb{K}$ is always an order in $\mathbb{K}$ and moreover, since $\mathcal{O} \subseteq \mathcal{O}_\mathbb{K}$ for any order $\mathcal{O}$ of $\mathbb{K}$, $\mathcal{O}_K$ is the **maximal order** of $\mathbb{K}$.

Lemma 1 ([5]): An order $\mathcal{O}$ in a quadratic field $\mathbb{K}$ has finite index in $\mathcal{O}_\mathbb{K}$ and if $f = [\mathcal{O}_K : \mathcal{O}]$, then $\mathcal{O} = \mathbb{Z} + fw_K\mathbb{Z}$. This finite index f is the conductor of the order.

Let $\mathcal{O}$ be an order of basis $[\alpha, \beta]$ as a $\mathbb{Z}$-module and let $a \mapsto a'$ be the nontrivial automorphism of $\mathbb{K}$. Then the **discriminant** D of $\mathcal{O}$ is defined as the number

$$D = \left(\det \begin{pmatrix} \alpha & \beta \\ \alpha' & \beta' \end{pmatrix}\right)^2.$$

The discriminant is independent of the integral basis and when we chose the basis $\mathcal{O} = [1, fw_K]$, we obtain $D = f^2 d_K$.

Let $\mathfrak{a}$ be a nonzero ideal of $\mathcal{O}$, then according to [15], $\mathcal{O}/\mathfrak{a}$ is finite and the norm of $\mathfrak{a}$ is defined as $N(\mathfrak{a}) = |\mathcal{O}/\mathfrak{a}|$.

An ideal $\mathfrak{a}$ is called a **proper ideal** when $\mathcal{O} = \{\beta \in \mathbb{K} : \beta\mathfrak{a} \subset \mathfrak{a}\}$. An ideal $\mathfrak{b}$ of $\mathcal{O}$ is a **fractional ideal** if it is a nonzero finitely generated $\mathcal{O}$-module. It is of the form $\alpha\mathfrak{c}$ where $\alpha \in \mathbb{K}^*$ and $\mathfrak{c}$ is an $\mathcal{O}$-ideal. A fractional $\mathcal{O}$-ideal $\mathfrak{a}$ is **invertible** if there exists another fractional $\mathcal{O}$-ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} = \mathcal{O}$. The concept of proper fractional ideals and invertible fractional ideals are identical for orders in quadratic fields, as proven in [5]. The ideals $\alpha\mathcal{O}$ where $\alpha \in K^*$ are called **principal ideals** and are invertible. They form a group denoted $P(\mathcal{O})$.

Thus, the set of proper fractional $\mathcal{O}$-ideals is a multiplication group, denoted as $\mathcal{I}(\mathcal{O})$ and $P(\mathcal{O})$ is a subgroup. The quotient $Cl(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O})$ is called the **ideal class group of the order** $\mathcal{O}$ or commonly referred as the Picard group. The class number is the cardinality of this group $h(\mathcal{O}) = \#CL(\mathcal{O})$.

VI. Computing explicit isogenies

When dealing with isogenies, a first goal is to explicitly determine their formulas, together with the corresponding isogenous curve to our starting curve.

In this section, we cover two different cases, depending on the input being:

- the field, the curve and the isogeny kernel. The kernel gives the degree of the computed isogeny.
- the field, the j-invariant of the curve and the prime degree l. The choice of the isogeny degree is determined following Kohel's thesis [14] on the endomorphism ring of an elliptic curve, results mentioned later on in the Isogeny Graph section.

We restrict to prime degrees as according to [7], a separable isogeny $\phi : \mathbf{E}_1 \to \mathbf{E}_2$ defined over $\mathbb{K}$ can be decomposed as $\phi = \phi_1 \circ \phi_2 \circ ... \circ \phi_k \circ [n]$, with ϕ_i prime degree isogenies over $\mathbb{K}$ and $deg(\phi) = \prod_i deg(\phi_i) \cdot n^2$.

Moreover, a separable isogeny $\phi : \mathbf{E}_1 \to \mathbf{E}_2$, with $\mathbf{E}_1, \mathbf{E}_2$ defined by Weierstrass equations $\mathbf{E}_i : y^2 + a_1^i xy + a_3^i = x^3 + a_2^i x^2 + a_4^i x + a_6^i$, is given by a formula

$$\phi(x, y) = (\phi_1(x), cy\phi_1(x)' + \phi_3(x)),$$

where ϕ_1, ϕ_3 are rational functions in $\mathbb{K}(x)$, $\phi_1(x)'$ is the (formal) derivative of ϕ_1, c is a non-zero constant in $\overline{\mathbb{K}}$, and

$$2\phi_3(x) = -a_1^2\phi_1(x) - a_3^2 + c(a_1^1 x + a_3^1)\phi_1(x)'.$$

When $c = 1$, we say that the isogeny is normalized.

Now, in order to study the first case, we utilize the following result. Given an elliptic curve $\mathbf{E}_1$ and $\mathbb{G}$ a finite subgroup of $\mathbf{E}_1(\overline{\mathbb{K}})$ that is defined over $\mathbb{K}$, there is a unique elliptic curve $\mathbf{E}_2$ (up to an isomorphism) and a (not necessarily unique) isogeny such that $Ker_\phi = \mathbb{G}$. Velu's formulas and their extension due to Kohel use the structure of the kernel group in order to compute a separable, normalized isogeny and the corresponding $\mathbf{E}_2$.

Complexity: If $\mathbb{K} = \mathbb{F}_q$, $d = \#\mathbb{G}$ and $\mathbb{G} \subset E(\mathbb{K})$, then the complexity of computing Velu's formulas is asymptotically of order $O(d)$ field operations in $\mathbb{F}_q$.

The following consequence of Velu's method provides the explicit formulas of a degree l isogeny.

Lemma 2 ([7]): Let $\phi : \mathbf{E} \to \tilde{\mathbf{E}}$, written as $\phi(x, y) = (\phi_1(x), \phi_2(x, y))$, with ϕ_i rational functions in $\mathbb{K}(\mathbf{E})$, be a separable isogeny of odd degree l between elliptic curves over $\mathbb{K}$. Then,

$$\phi_1(x) = \frac{u(x)}{v(x)^2}, \quad \text{with } deg(u) = l,\ deg(v) = \frac{l-1}{2}$$

and

$$\phi_2(x, y) = \frac{yw_1(x) + w_2(x)}{v(x)^3},$$

$$\text{with } deg(w_1(x)) \leq \frac{3(l-1)}{2},\ deg(w_2(x)) \leq \frac{3l-1}{2}.$$

Next, we approach the second case by introducing the notion of an $l-$th modular polynomial. This is a symmetric polynomial denoted by $\Phi_l(S, T)$ with coefficients in $\mathbf{Z}$, which is equal to

$$\Phi_l(S, T) = S^{l+1} - S^l T^l + T^{l+1} + \sum_{i,j \leq l,\ i+j<2l} a_{ij} S^i T^j.$$

By Kronecker congruence relation,

$$\Phi_l(S, T) = (S^l - T)(T - S^l)\ (mod\ l).$$

The polynomial has the fundamental property related to isogenies:

Lemma 3 ([7]): For any field $\mathbb{K}$ of characteristic different than l and for every pair of curves $(\mathbf{E}, \tilde{\mathbf{E}})$ defined over $\mathbb{K}$, there is a non-zero separable isogeny $\phi : \mathbf{E} \to \tilde{\mathbf{E}}$ of degree l with cyclic kernel if and only if $\Phi_l(j(\mathbf{E}), j(\tilde{\mathbf{E}})) = 0$.

So, the solutions of $\Phi_l(j(E), S) = 0$ are the precise $j-$invariants of the isogenous curves with $\mathbf{E}$ and linked through degree l isogenies. There are $0, 1, 2$ or $l + 1$ roots (taking into account the multiplicity) as Kohel proves in [14].

Complexity: The coefficients of $\Phi_l(T, S)$ are large and the largest one is of order $O(l \log l)$. There are approximately l^2 coefficients so, the required space for Φ is of order $O(l^3 \log l)$. In order to compute $\Phi_l(x, y)$, Enge conjectured that the number of bit operations is expected to be of $O(l^3 \log l)$ and factorization is expected to asymptotically be $O(l^2 \log l \log q)$. After factoring the modular polynomial, the next step is computing the defining polynomial of the kernel with Elkies algorithm of complexity $O(l^2)$ field operations in $\mathbb{K}$.

VII. Ordinary isogeny graph

Now, the aim is to expand on the theoretical connection between the previous sections. This will lead in the end to the previously mentioned result of Jao et al., regarding the hardness of the DLP [13].

Throughout this section, let $\mathbf{E}$ be an ellliptic curve over a finite field $\mathbb{F}_q$ of characteristic p. The $\mathbb{F}_q$-isogeny class of $\mathbf{E}$ is the set of $\mathbb{F}_q$-isomorphism classes of elliptic curves over $\mathbb{F}_q$ that are isogenous to $\mathbf{E}$ over $\mathbb{F}_q$. We know from previous sections that

$$\mathbb{Z}[\pi_q] \subseteq End(\mathbf{E}) \subseteq \mathcal{O}_{\mathbb{K}}$$

where $\mathbb{K} = \mathbb{Q}[\sqrt{t^2 - 4q}]$.

We give a first definition of an isogeny graph.

Definition 6 ([7]): Let $S \subset \mathbb{N}$ be a finite set of primes. Define $X_{\mathbf{E},S}$ the (directed) graph with vertex set the $\mathbb{F}_q$-isogeny class of $\mathbf{E}$. Vertices are labeled as j-invariants and edges are labeled as $l \in S$, corresponding to an l degree isogeny from a vertex to the other one.

There is a bijection between the set of isomorphism classes of elliptic curves $\mathbf{E}/\mathbb{F}_q$ with the same endomorphism ring $\mathcal{O}$ and the set of ideal classes $Cl(\mathcal{O})$ [7], [18]. One associate to each invertible $\mathfrak{a} \in Cl(\mathcal{O})$ the elliptic curve $\mathbf{E} = \mathbb{C}/\mathfrak{a}$ over the complex numbers.

Equivalent ideals in $Cl(\mathcal{O})$ lead to isomorphic curves over $\mathbb{C}$. Let $\mathfrak{l} \subseteq \mathbb{C}$ be an invertible $\mathcal{O}$ ideal. Then the set $\mathbf{E}[\mathfrak{l}] = \{P \in \mathbf{E}(\mathbb{C}) \,|\, \phi(P) = \mathcal{O}_E, \forall \phi \in \mathfrak{l}\}$ is isomorphic to $\mathfrak{l}^{-1}\mathfrak{a}/\mathfrak{a}$. $\#\mathbf{E}[\mathfrak{l}] = N(\mathfrak{l})$ and there is an isogeny from $\mathbb{C}/\mathfrak{a} \to \mathbb{C}/\mathfrak{l}^{-1}\mathfrak{a}$ of kernel $\mathfrak{l}^{-1}\mathfrak{a}/\mathfrak{a}$. The theory over $\mathbb{C}$ can be reduced over finite fields and every isogeny is given by this method. If $\mathfrak{l} = (l)$, $l \in \mathbb{N}$, and if l splits in $\mathcal{O}$ as $(l) = \mathfrak{l}_1\mathfrak{l}_2$ then $\phi : \mathbf{E} \to \tilde{\mathbf{E}}$ corresponds to one of the ideal, and the dual to the other one.

In the case of the ring of integers, l splits in $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\alpha]$ iff the minimal polynomial of α factors modulo l in two different linear factors, condition equivalent to $(\frac{d_{\mathbb{K}}}{l}) = 1$. In the case of $\mathbf{E}/\mathbb{F}_q$ with $End(\mathbf{E}) = \mathcal{O} = \mathbb{Z}[\theta]$ of conductor $c_{\mathbf{E}}$, if $(l, c_{\mathbf{E}}) = 1$ there are $1 + (\frac{d_{\mathbb{K}}}{l})$ prime ideals $\mathfrak{l}$ above $l \in \mathbb{N}$ and therefore, the same number of isogenies of degree l. If $(\frac{d_{\mathbb{K}}}{l}) = 1$, then take $\mathfrak{l}_1 = (l, a + \theta)$ and $\mathfrak{l}_2 = (l, b + \theta)$ as the prime ideals and test which corresponds to the isogeny $\phi : \mathbf{E} \to \tilde{\mathbf{E}}$. This is possible when we have the j invariants of the isogenous curves and we can compute the kernel of ϕ via Elkies algorithm. Either $[a]P + \theta(P) = \mathcal{O}_{\tilde{\mathbf{E}}}$ or $[b]P + \theta(P) = \mathcal{O}_{\tilde{\mathbf{E}}}$, when $P \in Ker_{\phi}$.

Now, we make the connection between orders, ideals and the isogeny graph defined previously. We take $\mathbf{E}$ corresponding to a $\mathcal{O}$-ideal $\mathfrak{a}$ and a finite set $S \subset \mathbb{N}$ of primes coprime to the conductor of $\mathcal{O}$. Take the set S' of $\mathcal{O}$ invertible ideals above the primes in S and let $< S' >$ be the subgroup generated by S' in $Cl(\mathcal{O})$.

Then the isogeny graph can be identified with the graph of invertible $\mathcal{O}$ ideals that are in the coset $\mathfrak{a} < S' >$. For each $\mathfrak{b} \in \mathfrak{a} < S' >$ and each $\mathfrak{l} \in S'$, there is an edge denoted by $\mathfrak{l}$ between $\mathfrak{b}$ and $\mathfrak{l}^{-1}\mathfrak{b}$ corresponding to an isogeny.

Thus, the first problem is to determine the endomorphism ring of any elliptic curve $\mathbf{E}/\mathbb{F}_q$, meaning finding the conductor of the order in the quadratic field. A solution is given by Kohel in his thesis [14].

Definition 7 ([14]): Let l be a prime. An l-isogeny $\phi : \mathbf{E} \to \tilde{\mathbf{E}}$ is called horizontal (respectively ascending, descending) if $End(\mathbf{E}) \cong End(\tilde{\mathbf{E}})$ (respectively $[End(\tilde{\mathbf{E}}) : End(\mathbf{E})] = l$, $[End(\mathbf{E}) : End(\tilde{\mathbf{E}})] = l$).

If $End(\mathbf{E}) = \mathcal{O}_K$ we say that $\mathbf{E}$ is on the surface of the isogeny graph. If $End(\mathbf{E}) = \mathbb{Z}[\pi_p]$ then $\mathbf{E}$ is on the floor of the isogeny graph.

Theorem 4: [14] Let $\mathbf{E}$ be an ordinary elliptic curve over $\mathbb{F}_q$ and let $\mathcal{O} = End(\mathbf{E})$. Let $c = [\mathcal{O}_{\mathbb{K}} : \mathcal{O}]$ and let l be a prime. Every l-isogeny $\phi : E \to \tilde{E}$ arises from

- if $l \nmid c$ then there are exactly $1 + \left(\frac{t^2-4q}{l}\right)$ equivalence classes of horizontal l-isogenies over $\mathbb{F}_q$ from $\mathbf{E}$ to other elliptic curves
- If $l \mid c$ then there are no horizontal isogenies, and exactly 1 ascending isogeny from E to another curve
- if $l \mid [\mathcal{O} : \mathbb{Z}[\pi_q]]$ then there are $l + 1$ isogenies classes from E, where horizontal and ascending isogenies are as above
- if $l \nmid [\mathcal{O} : \mathbb{Z}[\pi_q]]$ then there are no descending l-isogenies

The above theory permits us to navigate on different levels in the isogeny graph. One application is the following algorithm

Kohel's Algorithm

a) : Input: An elliptic curve $\mathbf{E}/\mathbb{F}_q$ given by Weierstrass equation

Output: c the conductor of $End(\mathbf{E})$

Complexity: of order $O(c^3 \log q)$ operations in $\mathbb{F}_q$

Compute $\#\mathbf{E}(\mathbb{F}_q)$ and $t = p + 1 - \#\mathbf{E}(\mathbb{F}_q)$ with Schoof's algorithm of counting points on an elliptic curve [17]. Determine the conductor $c_{\mathbb{Z}[\pi_q]} = [\mathcal{O}_{\mathbb{K}} : \mathbb{Z}[\pi_q]]$. If it is 1 return $c = 1$. Otherwise factor it and compute the set of pairs $S = \{(l, n) : \ c_{\mathbb{Z}[\pi_q]} = \prod_l l^n, \ l \text{ prime}, n > 0\}$.

Let $c = 1$. Pick a pair $(l, n) \in S$. We have $n + 1$ levels of endomorphism rings, each levels correspond to l^i, with $i \in [0, n]$.

First step is to find the solutions of $\Phi_l(x, j_{\mathbf{E}})$. The number of possible solutions (together with multiplicity) could be 1 and $l+1$ as we do not consider $c_{\mathbb{Z}[\pi_q]} = 1 = c$. If there is only one solution, the curve is on the bottom, level corresponding to l^n and we compute $c = c \cdot l^n$. If there are $l + 1$ solutions, we either are on the surface or somewhere in between surface and floor.

First check if two of the isoenies could be horizontal isogenies, i.e. $(\frac{d_{\mathbb{K}}}{l}) = 1$. If not, we can only navigate either up or down. So, take two solutions j_1 and j_1' and construct two indexed sets, $V_1 = \{j_{\mathbf{E}}, j_1\}$ and $V_1' = \{j_{\mathbf{E}}, j_1'\}$. Repeat the factorization part using the two new j-invariants, but take only one solution out of all $l+1$ such that it is not the first element in the corresponding list. Update the indexed sets $V_2 = \{j_1, j_2\}$ and $V_2'\{j_1', j_2'\}$ and repeat this step until you find the first occurrence of a single solution for the modular polynomial. Do not compute the new list, but compute c. The exponent of l in the factorization of c is n minus the index of the sets.

Now, when having horizontal isogenies, the principle is similar. We need to avoid taking 2 possible paths on the surface so, we consider three indexed sets.

Afterwards remove the pair (l, n) from S and pick another arbitrary pair. Repeat the procedure until S is empty. Return c.

VIII. The Galbraith-Hess-Smart Algorithm

The second problem is given two vertices of the isogeny graph, corresponding to two curves $\mathbf{E}, \tilde{\mathbf{E}}$ defined over $\mathbb{F}_q$, compute an isogeny path in between them.

A first method is due to Galbraith [6]. We start with two sets $X_0 = \{j_{\mathbf{E}}\}$ and $Y_0 = \{j_{\tilde{\mathbf{E}}}\}$ representing the j invariants of the starting curves. Let S be a set of primes. At each step $i+1$ we have two sets X_i and Y_i of j invariants and for every prime $l \in S$, using the modular polynomial we compute all the j-invariants of the curves that are isogenous to the ones in X_i and Y_i and add the new values to X_i, Y_i and increase the index

to $i+1$. The algorithm stops when X_i and Y_i have a common element. Taking $l < 6(\log q)^2$, a condition implying that with large enough probability the isogeny graph is connected, the complexity of the running time is expected to be of order $O(q^{1/4})$ and the storage of order $O(q^{1/4}(\log q)^2)$.

The Galbraith-Hess-Smart Algorithm [8] proposes a new method of navigating in the isogeny graph.

The GHS Algorithm:

Input: $\mathbf{E}, \tilde{\mathbf{E}}$ over $\mathbb{F}_q$

Output: Isogeny $\phi : \mathbf{E} \to \tilde{E}$

1. Compute first the endomorphism rings of $\mathbf{E}$ and $\tilde{\mathbf{E}}$ via Kohel's algorithm. Find a chain of isogenies from $\mathbf{E}$ and $\tilde{\mathbf{E}}$ to two curves on the surface, $\mathbf{E}_1$ and $\mathbf{E}_2$ respectively. In case the conductor of $\mathbb{Z}[\pi_q]$ has a large prime factor, this stage is costly but this case mostly never happens in practice.
   Now, we restrict the problem to find a path between $\mathbf{E}_1$ and $\mathbf{E}_2$ with $End(\mathbf{E}_i) = \mathcal{O}_{\mathbb{K}}$, $i = 1, 2$.
2. Each vertex is a j-invariant of a curve and we construct a pseudorandom walk on the set of invariants. We consider pairs of the form $(j, \mathfrak{a})$, where j is a j-invariant of an elliptic curve isomorphism class and $\mathfrak{a}$ is an element in $Cl(\mathcal{O}_{\mathbb{K}})$. First pick a set F of primes that split in $\mathcal{O}_{\mathbb{K}}$ (we could include some primes that ramify) such that the set of prime ideals $\mathfrak{l}$ above F generates $Cl(\mathcal{O}_{\mathbb{K}})$ and $\#F$ is big enough for the walk to look random.
   We take the primes in F to be bounded by $B = 6(\log q)^2$ (in practice it works for $\#F$ at least 16). Similar to Pollard-rho [16], we take a partitioning function $f : \mathbb{F}_q \to F \times \{0, 1\}$ of approximately uniform distribution. Given a j-invariant, the function will link it in a deterministic way to the degree l of a modular polynomial and a bit 0 or 1. The factorization of the polynomial leads to two j-invariants corresponding to horizontal isogenies and one of them, lets say j', is picked deterministically according to the bit 0 or 1. Compute the ideal $\mathfrak{l}$ that corresponds to the isogeny and update the pair to $(j'$, Reduce$(\mathfrak{a} \cdot \mathfrak{l}))$.
   The goal is to reach a collision, the same j-invariant, and the number of steps is expected to be $O(\sqrt{h(\mathcal{O}_{\mathbb{K}})})$ due to the Birthday Paradox. Besides, since each step requires $O(B^2 \log q)$, the complexity of this stage is asymptotically of $O(q^{1/4+\epsilon})$.
   We can run this stage in parallel by resort to distinguished j-invariants and different starting j-invariants for each processor. If we do not reach a collision after a given maximal number of steps, one solution is to redefine the partitioning function f.
3. This step deals with replacing the ideal $\mathfrak{a}$ by a smooth ideal of bound B', using a method similar to index-calculus. Take F' the set of primes that are split in $\mathcal{O}_{\mathbb{K}}$ and bounded by B'. Find a smooth $\mathfrak{b} = \mathfrak{a} \cdot \prod_{l_i \in F'} \mathfrak{l}_i^{a_i}$ for random integers a_i, meaning there exist $b_i > 0$ such that $\mathfrak{b} = \prod_{l_i \in F'} \mathfrak{l}_i^{b_i}$. Then $\mathfrak{a} = \prod_{l_i \in F'} \mathfrak{l}_i^{b_i - a_i}$. The authors give an heuristic complexity of order $O(\sqrt{q^{1/4+\epsilon}})$.
4. Compute the isogeny path between $\mathbf{E}_1$ and $\mathbf{E}_2$.

Complexity: The number of steps is asymptotically of order $O(q^{1/4+\epsilon})$ but the mapping of points from one curve to another is done in polynomial time.

IX. Improved GHS algorithm

In a recent article [9], while looking to improve this algorithm, Galbraith and Stolbulnov proposes a method for solving a more generic problem, called the group action inverse problem (GAIP).

First lets introduce the problem. Take G a group, X a non-empty set and the left action of G on X: for all $g \in G$ and $x \in X$, $(g, x) \to g \star x$. The action is associative and the identity e of G is a stabilizer for X, meaning $e \in \{g \in G \mid g \star x = x\}$ for all $x \in X$. The orbit of $x \in X$ is $G \star x$ and is an equivalence class.

GAIP: Let G be a group acting on a set X. Given $x, y \in X$ compute $g \in G$ such that $y = g \star x$.

The authors solve the problem in case X is a principal homogenous space for a finite group G, i.e, X is finite, there is only one orbit and the stabilizer set is $\{e\}$ for each $x \in X$. These restrictions imply the existence of an unique solution for GAIP.

Now take X as the set of isomorphic classes of elliptic curves $\mathbf{E}$ over $\mathbb{F}_q$ with $End(\mathbf{E}) = \mathcal{O}$ and consider the ideal class group $Cl(\mathcal{O})$. Taking into account the theory from the previous sections, the group $Cl(\mathcal{O})$ acts on X in the natural way. For each ideal $\mathfrak{l} \in Cl(\mathcal{O})$ and class of isomorphic curves E consider $\mathfrak{l} \star E$ as the isomorphism class corresponding to the isogeny given by l and E.

Cl**-GAIP**: Let $\mathbf{E}, \tilde{\mathbf{E}}$ be two elliptic curves defined over $\mathbb{F}_q$ with the same endomorphism ring $\mathcal{O}$. Find $\mathfrak{l} \in Cl(\mathcal{O})$ such that $\mathfrak{l} \star \mathbf{E} \cong \tilde{\mathbf{E}}$.

Let H be a finite set of r $\mathcal{O}$-prime ideals, where r is a positive integer. In the isogeny graph obtained with this method, there is an edge between two vertexes iff there is an isogeny corresponding to an $\mathfrak{l} \in H$.

As in the previous paper, the authors use a partitioning function . The main difference is picking different probabilities for each partition, due to favoring the smallest primes in H. They also impose that only one element of $\mathfrak{l}, \mathfrak{l}^{-1}$ is in H.

The theoretical analysis of the running time is done by emplying a simpler model, where the case of cycles is not taken into account and the action is given by random permutations h_i of the elements in X. Theorem 1 proves that the number of steps is expected to be $\sqrt{\pi n/d} + 2/\theta + O(\ln^4(n))$, where $n = \#X$, p_i is the probability of picking a particular element $l_i \in H$, θ is the probability of a distinguished element and $d = 1 - (1 - \theta) \sum_{i=1}^{r} p_i^2$. If the probabilities are equal, $\theta \to 0$ as $n \to \infty$, then d tends to $\frac{r-1}{r}$, limit that agrees with the Pollard-rho running time given by an r-adding function.

The theoretical result is compared to an extensive set of experimental data, obtained by applying the algorithm for GAIP with $G = X$ of order up to 2^{80}, r integer in $[4, 16]$ and the probabilities in a geometric progression of ratio $w \in [1, 3/4, 1/2, 1/3, 1/4]$. They compute ω as the ratio between expected results in practice and the ones in theory. They notice that for r and w fixed, ω stabilizes in the interval $(1, 1.5)$ when the order of G increases and exceeds 2^{30}. Moreover they determine experimental running times for the

action of a prime ideal $\mathfrak{l}$ over an elliptic curve, meaning the second case of computing explicit isogenies that factorizes modular polynomials and implements Elkies algorithm. They also choose the set H of prime ideals that generate $Cl(\mathcal{O}_{\mathbb{K}})$, such that most of them are above the smallest possible primes that split in $\mathcal{O}$.

Finally, the estimated serial running time is given by

$$\omega E[L]\vec{p}\cdot\vec{t},$$

where ω is the same as before, $E[L]$ is the expected number of steps obtained applying Theorem 1, $\vec{p}$ is the probability vector and $\vec{t}$ is the time cost vector for the actions induced by the prime ideals in H. Taking the previous recommended parameters $r = 16$ and $w = 1$, one obtains the cost of the GHS algorithm for a random curve over a finite field of 160 bit size. The new version of GHS gives a speedup of 14 when $r = 9$ and $w = 1/3$. But asymptotically, the complexity is still of order $O(q^{1/4+\epsilon})$.

X. Towards cyclic isogenies between genus 2 curves

One could argue that computing an isogeny path is too costly to be useful in cryptanalysis. On the other hand, the best known attack on elliptic curves implemented in cryptographic applications is still the Pollard-rho exponential algorithm of complexity $O(q^{1/2})$. Having a vulnerable curve of the same endomorphism ring as our initial strong curve leads to computing the isogeny path in $O(q^{1/4+\epsilon})$ steps. Afterwards, transferring one hard DLP instance into the weak corresponding one is done in polynomial time, and thus, computing the isogeny decreases the hardness of the DLP by a significant factor. Finally, Jao, Miller and Venkatesen in [13] prove that the DLP is either hard or easy for "most" elliptic curves in an isogeny class, a result that answers the question if such a weak curve could be found or not.

Similar to the elliptic curve case, there is no subexponential algorithm for DLP on the Jacobian of a curve of genus 2 defined over a finite field. A genus 2 curve $\mathbf{C}$ over $\mathbb{F}_q$ has $\#J_C(\mathbb{F}_q) \approx q^2$. Hence, the same level of security is achieved when taking $\mathbf{C}$ over $\mathbb{F}_q = \mathbb{F}_{2^{80}}$ as opposed to when taking an elliptic curve $\mathbf{E}$ over $\mathbb{F}_q = \mathbb{F}_{2^{160}}$. On the other hand, when dealing with higher genus curves the arithmetic is costly and improving the existent method [10] is a first step in my research plan.

Regarding the isogeny graph, the endomorphism ring of $\mathbf{C}$ is an order in a quartic field. The vertexes do not represent curves with the same number of points, but represent curves whose Frobenius endomorphisms have the same characteristic polynomial (Tate's theorem). In the case of elliptic curve this statement of Tate's theorem is equivalent to the well known result regarding the number of points.

Currently, one can explicitly compute only a special class of isogenies, but not all isogenies are of this form and the graph may not be connected. The structure of the resulting graph proves to be a lattice [12] and not a vulcano like in the elliptic curves case. Therefore, the navigation in the isogeny graph proves to be harder. Bisson provided a subexponential algorithm [3] to locate the endomorphism ring of a curve on such lattices. Hence, another point of interest and subsequently future research is linking the vertexes in the genus 2 graph through isogenies of prime degree l, $l < poly(\log q)$. The next natural step is formulating the random self-reducibility argument to show that the DLP is equally hard on each genus 2 Jacobian with the same endomorphism ring.

The implementation of an explicit isogeny computation for genus 2 curves could be done in Sage or Magma. Sage has an extensive library related to elliptic curves and isogenies. It allowed me to determine the isogeny graph when implementing Kohel's algorithm for certain curves.

In the case of hyperelliptic curves of genus 2, there is a Magma package developed by Bisson, Cosset and Robert [4] for computing the current type of isogenies and which can be extended in order to explicitly compute prime degree isogenies, an isogeny path between vertexes and any future algorithm that transfers one instance of DLP to another one on a different curve.

References

[1] L. Adleman. A subexponential algorithm for the discrete logarithm problem with applications to cryptography. In *Proceedings of the 20th Annual Symposium on Foundations of Computer Science*, SFCS '79, pages 55–60, Washington, DC, USA, 1979. IEEE Computer Society.

[2] L. M. Adleman, J. DeMarrais, and M.-D. A. Huang. A subexponential algorithm for discrete logarithms over the rational subgroup of the jacobians of large genus hyperelliptic curves over finite fields. In *ANTS*, pages 28–40, 1994.

[3] G. Bisson. *Endomorphism Rings in Cryptography*. PhD thesis, Eindhoven University, July 2011.

[4] G. Bisson, R. Cosset, and D. Robert. *avIsogenies: a library for computing isogenies between abelian varieties*.

[5] D. A. Cox. *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication*. Wiley, New York, 1989.

[6] S. D. Galbraith. Constructing isogenies between elliptic curves over finite fields. *LMS J. Comput. Math*, 2:118–138, 1999.

[7] S. D. Galbraith. *Mathematics of Public Key Cryptography*. Cambridge University Press, UK, 2012.

[8] S. D. Galbraith, F. Hess, and N. P. Smart. Extending the ghs weil descent attack. In *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques: Advances in Cryptology*, EUROCRYPT '02, pages 29–44, London, UK, UK, 2002. Springer-Verlag.

[9] S. D. Galbraith and A. Stolbunov. Improved algorithm for the isogeny problem for ordinary elliptic curves. *CoRR*, abs/1105.6331, 2011.

[10] P. Gaudry. Fast genus 2 arithmetic based on Theta functions. *Journal of Mathematical Cryptology*, 1(3):243–265, 2007.

[11] P. Gaudry, F. Hess, and N. P. Smart. Constructive and destructive facets of weil descent on elliptic curves. *J. Cryptology*, 15(1):19–46, 2002.

[12] D. Gruenewald. *Explicit Algorithms for Humbert Surfaces*. PhD thesis, University of Sydney, December 2008.

[13] D. Jao, S. D. Miller, and R. Venkatesan. Do all elliptic curves of the same order have the same difficulty of discrete log? In *ASIACRYPT*, pages 21–40, 2005.

[14] D. Kohel. Endomorphism rings of elliptic curves over finite fields. *PhD Thesis*, 1996.

[15] D. A. Marcus. *Number Fields*. Springer-Verlag, Berlin, Heidelberg and New York, 1977.

[16] J. Pollard. Monte Carlo methods for index computation (mod p). *Mathematics of Computation*, 32:918–924, 1978.

[17] R. Schoof. Counting points on elliptic curves over finite fields. *J. Theorie des Nombres de Bordeaux*, 7:pp. 219–254, 1995.

[18] J. Silverman. *The Arithmetic of Elliptic Curves*. Graduate texts in mathematics. Springer-Verlag, 1986.

[19] B. Smith. Isogenies and the discrete logarithm problem in jacobians of genus 3 hyperelliptic curves. In *EUROCRYPT*, pages 163–180, 2008.