Random Self-reducibility of the Discrete Logarithm Problem for Genus 2 Curves

Cihangir Tezcan
LACAL, I&C, EPFL

***Abstract*—Known attacks on the elliptic curve discrete logarithm problem introduce constraints on elliptic curve parameters. A common cryptographic practice is to select an elliptic curve randomly, and keep it if its group order satisfies these constraints. But this process assumes that elliptic curves over the same finite field with the same number of points have the same difficulty of the discrete logarithm problem. It is shown in [14] that this assumption is true for almost all elliptic curves. Orders in imaginary quadratic fields [4, Section 7] play an important role in this result because the endomorphism ring of an ordinary curve is isomorphic to an order in an imaginary quadratic field.**

The same cryptographic practice is valid for hyperelliptic curves but the algorithms for calculating the number of points on these curves are not practical when the underlying finite field is large. However, [11] shows that this computation can be practical for special curves having real multiplication. Yet, it is an open problem if the discrete logarithm problem is equally hard for all hyperelliptic curves over the same finite field with the same number of points. We propose to study this problem for curves of genus 2.

***Index Terms*—discrete logarithm problem, isogenies, genus 2 curves, random self-reducibility, expander graphs, number fields, orders, point counting problem**

Proposal submitted to committee: September 13th, 2011; Candidacy exam date: September 20th, 2011; Candidacy exam committee: Serge Vaudenay, 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

The difficulty of the discrete logarithm problem (DLP) depends on the group on which the problem is defined. Public key cryptosystems based on the elliptic curve discrete logarithm problem [15], [22] is of critical importance in cryptography because there is no known subexponential algorithm to solve this problem in the group under addition of points of an elliptic curve E defined over a finite field $\mathbb{F}_q$.

Definition 1: 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 $Q \in \langle P \rangle$, finding the unique integer $m \in [0, \dots, r-1]$ such that $Q = [m]P$ is called the *elliptic curve discrete logarithm problem* (ECDLP).

Known attacks on the ECDLP force us to carefully select the elliptic curve parameters.

1) To avoid the Pohlig–Hellman [24] and Pollard's Rho [25], [35] attacks, r should be a large prime of at least 160 bits because these attacks have a time complexity of $O(\sqrt{r})$.
2) The MOV and Frey–Rück attacks [21], [8] reduce the ECDLP on $E(\mathbb{F}_q)$ to the DLP in $\mathbb{F}_{q^l}$, for some integer l, by using a Weil pairing on $E[r]$. When $\gcd(r, q) = 1$, the integer l is the smallest such that $q^l \equiv 1 \pmod{n}$. This reduction is polynomial in terms of the number of operations in $\mathbb{F}_{q^l}$. Therefore, to avoid the MOV attack, r should not divide $q^l - 1$ for each $1 \leq l \leq C$ where $C = 20$ is sufficient. This required property of r cannot be obtained when the curve is supersingular.
3) When q is prime, the elliptic curves whose trace of Frobenius t is 1 and $N = q$ are called anomalous curves. These curves resist the MOV attack. However, using q-adic elliptic logarithm [28], [33] or considering the q-primary part of the subgroup generated by P [31], one can give a linear time method to solve the ECDLP. To avoid these attacks, N should be different from q.

Therefore, in practice, we need ordinary, non-anomalous (i.e. $N \neq q$) elliptic curves with group orders divisible by a large prime number of at least 160 bits. In practice, an elliptic curve is selected randomly and kept if it satisfies these conditions. Thus, determining the order of the group $E(\mathbb{F}_q)$, which is also known as the *point counting problem*, is of critical importance in elliptic curve cryptography. Schoof's point counting algorithm [29], [30] solves this problem efficiently. Although working with random curves is not as efficient as working with special curves like Koblitz curves [17], it is practical. Therefore, it is a natural question to ask if the ECDLP is equally hard for every elliptic curve over the same finite field having the same number of points.

A function f is called *random self-reducible* if the evaluation of f at any given instance can be reduced in polynomial time to the evaluation of f at one or more random instances [6]. In [14], it is shown that almost all elliptic curves over the same finite field having the same number of points have the same difficulty of discrete logarithm by showing polynomial time random self-reducibility of the ECDLP among these curves. This result holds with the assumption of the Generalized Riemann Hypothesis. Orders in imaginary quadratic fields [4, Section 7] play an important role in this result because the endomorphism ring of an ordinary curve is isomorphic to an order in an imaginary quadratic field. For a fixed N and m, elliptic curves that are isomorphic to the same order in an imaginary quadratic field form the vertices of an isogeny graph (see Section III.B) and prime degree isogenies between them of degree less than m form the edges. The polynomial time random self-reducibility of the ECDLP is achieved by navigating this isogeny graph. Properties of imaginary quadratic fields and orders are summarized in Section II and the random self-reducibility of the ECDLP is summarized in Section III.

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 $\deg(f) = 2g + 1$.

This equation is called the *imaginary model* of the curve. In general, $\deg(h(x)) \leq g + 1$ and $\deg(f(x)) \leq 2g + 2$ and it is not possible to represent every hyperelliptic curve with this model. However, in this proposal we only consider the imaginary model because the remaining curves introduce some extra technicalities. The integer $g \geq 0$ is called the *genus* of the curve and elliptic curves correspond to the $g = 1$ case.

The group of *divisors* on C is obtained from the finite formal sums of points of C over $\mathbb{Z}$:

$$\mathrm{Div}(C) = \left\{ D = \sum_{P_i \in C} n_i P_i : \; n_i \in \mathbb{Z} \right\}.$$

The *degree* of a divisor D is the sum of its coefficients $\deg D = \sum n_i$ and we denote degree zero divisors by $\mathbf{D}^0$.

The *coordinate ring* $\mathbb{F}_q[C]$ *of* C *over* $\mathbb{F}_q$ is the quotient ring

$$\mathbb{F}_q[C] = \mathbb{F}_q[x, y]/(y^2 + h(x)y - f(x)).$$

And *the function field* $\mathbb{F}_q(C)$ of C over $\mathbb{F}_q$ is the field of fractions of $\mathbb{F}_q[C]$. Let φ be a non-zero rational function in $\mathbb{F}_q(C)$ and let $P \in C$. If $\varphi(P) = 0$, then φ is said to have a *zero* and the multiplicity of this zero is assigned to $\nu_P(\varphi)$. If φ is not defined at P, then φ is said to have a *pole* at P and the opposite of the multiplicity of this pole is assigned to $\nu_P(\varphi)$. Otherwise, we let $\nu_P(\varphi) = 0$.

The divisor of φ is defined as

$$\mathrm{div}(\varphi) = \sum_{P_i \in C} \nu_{P_i}(\varphi) P_i.$$

A non-zero function has finitely many zeros and poles. Thus, $\nu_{P_i}(\varphi) = 0$ for almost all the P_is and $\mathrm{div}(\varphi)$ is well defined. Such a divisor is called a *principal divisor*. The set of principal divisors $\mathbf{P}$ is a subset of $\mathbf{D}^0$. The quotient group $J_C = \mathbf{D}^0/\mathbf{P}$ is called the *Jacobian* of the curve C and it is an abelian variety of dimension g.

Koblitz showed in [16] that Jacobians of hyperelliptic curves over finite fields are good sources of cyclic groups for cryptographic use. Intuition of Koblitz [18] was that curves with higher genus provide better security. But this is another example of misjudgement in the history of cryptography for Adleman et al. [1] provided a subexponential algorithm for discrete logarithm over the rational subgroup of the Jacobians of large genus hyperelliptic curves over finite fields. Because of this attack, in practice only the hyperelliptic curves of genus 1, 2, and 3 are considered to be secure [18]. However, the security of genus 3 curves is questionable because the attack of [1] is faster than Pollard's Rho attack for these curves (but still exponential). Moreover, Smith [34] showed that explicit isogenies can transfer instances of the DLP on hyperelliptic curves of genus 3 to non-hyperelliptic curves of genus 3, where they are vulnerable to faster index calculus attacks. His analysis shows that around $\%18.57$ of hyperelliptic curves of genus 3 over a given finite field is susceptible to this attack.

In order for a hyperelliptic curve cryptosystem to have the same security level of an elliptic curve cryptosystem, the underlying finite field can be chosen relatively smaller. Moreover, there is no known subexponential algorithm to solve the DLP for hyperelliptic curves of small genus. As in the case of elliptic curve cryptosystems, the point counting problem is important for random hyperelliptic curve selection. Although there exist polynomial time algorithms for point counting, they are impractical. It is shown in [11] that for some special curves of genus 2, the complexity of the Schoof's algorithm can be reduced from $\tilde{O}((\log q)^8)$ to $\tilde{O}((\log q)^5)$ by making use of the real multiplication. By using this algorithm, the authors also compute the order of a Jacobian defined over a 512-bit prime field which should be compared to the previous record of 128-bit field. These results are provided in Section IV.

In the process of random elliptic curve selection, it is assumed that the ECDLP for two elliptic curves over the same finite field having the same number of points are equally hard. However, its correctness was not known until the formal justification of [14]. Now the same question should be asked for random genus 2 curve selection. In this research, our main aim is to show that the DLP is equally hard in a large class of genus 2 curves.

II. Orders in Quadratic Fields

Definition 3: A subfield K of the complex numbers $\mathbb{C}$ that has finite degree over $\mathbb{Q}$ is called a *number field*. The degree of K over $\mathbb{Q}$ is denoted $[K : \mathbb{Q}]$.

Definition 4: Let K be a number field. The set of all $\alpha \in K$ that are roots of a monic integer polynomial forms a ring called the *algebraic integers of* K or *ring of integers of* K and denoted $\mathcal{O}_K$.

Definition 5: A number field $K = \mathbb{Q}(\sqrt{n})$ where $n \neq 0, 1$ is a squarefree integer is called a *quadratic field*. K is called an *imaginary quadratic field* if $n < 0$ and it is called a *real quadratic field* otherwise. The *discriminant* d_K *of* K is defined to be n if $n \equiv 1 \pmod 4$, and $4n$ otherwise.

Proposition 1 ([4]): Let K be a number field.

(i) $\mathcal{O}_K$ is a subring of $\mathbb{C}$ whose field of fractions is K.
(ii) $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $[K:\mathbb{Q}]$.

Definition 6 ([4]): If K is a number field and $\mathfrak{a}$ is a nonzero ideal of $\mathcal{O}_K$, then the quotient ring $\mathcal{O}_K/\mathfrak{a}$ is finite and the *norm* of $\mathfrak{a}$ is defined to be $N(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|$.

If $K = \mathbb{Q}(\sqrt{n})$ where n is squarefree, then one can calculate

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

and by using the discriminant we obtain

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{d_K + \sqrt{d_K}}{2}\right].$$

A lattice $[a,b]$ is defined as the set $\{ma + nb : m,n \in \mathbb{Z}\}$ where $a,b \in \mathbb{C}$. Therefore, we can write the ring of integers in K as the lattice

$$\mathcal{O}_K = [1, w_K], \text{ where } w_K = \frac{d_K + \sqrt{d_K}}{2}.$$

Definition 7 ([4]): An *order* $\mathcal{O}$ in a quadratic field K is a subset $\mathcal{O} \subset K$ such that

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

Clearly, K is the field of fractions of $\mathcal{O}$ and $\mathcal{O}_K$ is always an order in K. Moreover, by definition we have $\mathcal{O} \subset \mathcal{O}_K$ which makes $\mathcal{O}_K$ the *maximal order* of K.

Lemma 1: An order $\mathcal{O}$ in a quadratic field K has finite index in $\mathcal{O}_K$ and if we set $f = [\mathcal{O}_K : \mathcal{O}]$, then $\mathcal{O} = \mathbb{Z} + f w_K$.

This finite index f of an order $\mathcal{O}$ in a quadratic field K is denoted $f = [\mathcal{O}_K : \mathcal{O}]$ and is called the *conductor* of the order. Let us denote $\mathcal{O}$ as the lattice $[\alpha, \beta]$ where $\alpha, \beta \in \mathbb{C}$ and let $a \mapsto a'$ be the nontrivial automorphism of 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 used and when we use the basis $\mathcal{O} = [1, f w_K]$, we obtain $D = f^2 d_K$.

Let $\mathfrak{a}$ be a nonzero ideal of $\mathcal{O}$, then $\mathcal{O}/\mathfrak{a}$ is finite and we define the norm of $\mathfrak{a}$ as $N(\mathfrak{a}) = |\mathcal{O}/\mathfrak{a}|$. An ideal $\mathfrak{a}$ is called a *proper ideal* when $\mathcal{O} = \{\beta \in K : \beta\mathfrak{a} \subset \mathfrak{a}\}$. And an ideal $\mathfrak{b}$ of $\mathcal{O}$ that is a nonzero finitely generated $\mathcal{O}$-module is called a *fractional ideal* and it is of the form $\alpha\mathfrak{c}$ where $\alpha \in K^*$ and $\mathfrak{c}$ is an $\mathcal{O}$-ideal. Moreover, a fractional $\mathcal{O}$-ideal $\mathfrak{a}$ is *invertible* if there exists another fractional $\mathcal{O}$-ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} = \mathcal{O}$. It turns out that notions of proper ideals and invertible ideals are identical for orders in quadratic fields:

Proposition 2: Let $\mathcal{O}$ be an order in a quadratic field K, and let $\mathfrak{a}$ be a fractional $\mathcal{O}$-ideal. Then $\mathfrak{a}$ is proper if and only if $\mathfrak{a}$ is invertible.

Thus, the set of proper fractional $\mathcal{O}$-ideals $I(\mathcal{O})$ have inverses and they form a group under multiplication. The ideals of the form $\alpha\mathcal{O}$ where $\alpha \in K^*$ are called *principal ideals* $P(\mathcal{O})$ and they are invertible. Hence, we have $P(\mathcal{O}) \subset I(\mathcal{O})$ and the quotient $Cl(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O})$ is called the *ideal class group of the order* $\mathcal{O}$. $Cl(\mathcal{O})$ is commonly referred as the Picard group.

III. Elliptic Curves Having the Same Number of Points over $\mathbb{F}_q$

A. Preliminaries

Definition 8: Two elliptic curves E_1 and E_2 over $\mathbb{F}_q$ are called *isogenous* if there exists a nontrivial algebraic group homomorphism $\phi : E_1 \to E_2$ between them over $\mathbb{F}_q$.

Theorem 1 (Tate's theorem): Let E_1 and E_2 be elliptic curves over $\mathbb{F}_q$. They are isogenous $\iff \#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$.

Hence, when an isogeny between two elliptic curves is known, the ECDLP on one elliptic curve can be reduced to the ECDLP on the other curve. However, constructing an isogeny between two specific curves is considered to be hard because there is no known polynomial time algorithm.

Definition 9: An *endomorphism* of E is an isogeny $\varphi : E \to E$ defined over the algebraic closure $\bar{\mathbb{F}}_q$ of $\mathbb{F}_q$. The set of endomorphisms of E together with the zero map forms a ring under the operations of pointwise addition and composition. This ring is called *endomorphism ring of* E and it is denoted by $End(E)$.

The *Frobenius endomorphism* is the isogeny $\pi : E \to E$ of degree q given by the equation $\pi(x,y) = (x^q, y^q)$ where E is defined over $\mathbb{F}_q$. It satisfies the equation

$$\pi^2 - [t]\pi + [q] = [0]$$

where $t = q + 1 - N$ is the *trace of Frobenius*. By Hasse's Theorem we have $|t| \leq 2\sqrt{q}$.

Definition 10: An elliptic curve E over $\mathbb{F}_q$ is called *supersingular* if the characteristic of the field divides the trace of Frobenius. Otherwise, it is called *ordinary*.

If E is supersingular, then the ring $End(E)$ is isomorphic to an order in a quaternion algebra and if E is ordinary, then $End(E)$ is isomorphic to an order in an imaginary quadratic field [32, p. 145].

Definition 11: An isogeny $\phi : E_1 \longrightarrow E_2$ over $\mathbb{F}_q$ is called an ℓ-isogeny if its kernel $ker(\phi)$ has size ℓ. The kernel of ϕ is determined by the polynomial

$$\psi(x) = \prod_{(x_0, \pm y_0) \in ker(\phi)} (x - x_0) \in \mathbb{F}_q.$$

We can represent every isogeny ϕ as a rational map of the form

$$\phi(x,y) = \left(\frac{\phi_1(x,y)}{\psi(x)^2}, \frac{\phi_2(x,y)}{\psi(x)^3}\right),$$

where ϕ_1 and ϕ_2 are polynomials over $\mathbb{F}_q$ and $\psi(x)$ is introduced in Definition 11. Hence, construction of an isogeny means the explicit computation of the polynomials ϕ_1, ϕ_2 and $\psi(x)$.

B. Isogeny Graphs

If an elliptic curve is ordinary, then its endomorphism ring $End(E)$ is an order in an imaginary quadratic field and if an elliptic curve E' is isogenous to E, then $End(E')$ is also an order in the same field. We denote the order generated by the Frobenius map π with $\mathbb{Z}[\pi]$ and the conductors of $End(E)$ and $\mathbb{Z}[\pi]$ are denoted by

$$[\mathcal{O}_K : End(E)] = c_E \text{ and } [\mathcal{O}_K : \mathbb{Z}[\pi]] = c_\pi.$$

Since the discriminant of $\mathbb{Z}[\pi]$ is $d_\pi = t^2 - 4q$, the conductor c_π is the largest integer such that $d_\pi/c_\pi^2 \equiv 0 \text{ or } 1 \pmod 4$. Equivalently, it is the unique integer for which d_π/c_π^2 is a fundamental discriminant. Thus, divisors of c_π are the only possibilities for c_E and therefore, we have finitely many possibilities for $End(E)$.

Proposition 3: [19, Proposition 21] Let E and E' be elliptic curves over the finite field $\mathbb{F}_q$. Let $\phi : E \to E'$ be an isogeny of prime degree ℓ different from the characteristic of the field. Then $\mathcal{O} = \mathrm{End}(E)$ contains $\mathcal{O}' = \mathrm{End}(E')$ or $\mathcal{O}'$ contains $\mathcal{O}$ in K and the index of one in the other divides ℓ.

Therefore, the orders can be uniquely identified by their conductors and they form a tower. Such a tower of 6 levels is shown in Figure 1 where the edges represent ascending/descending isogenies.

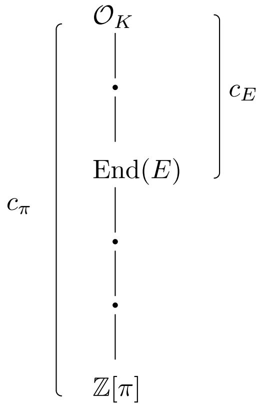

Fig. 1. Tower of endomorphism rings of elliptic curves

An ℓ-isogeny $\phi : E_1 \to E_2$ is called a *descending* ℓ-isogeny if $[\mathcal{O}_1 : \mathcal{O}_2] = \ell$, it is called *ascending* if $[\mathcal{O}_2 : \mathcal{O}_1] = \ell$ and it is called *horizontal* if $\mathcal{O}_1 = \mathcal{O}_2$. The possibilities for the rational ℓ-isogenies of E defined over $\mathbb{F}_q$ are given in [19, Proposition 23] and provided in Table I.

TABLE I
NUMBER AND TYPE OF THE ℓ-ISOGENIES

Case		Number and Type
$\ell \nmid c_E$	$\ell \nmid c_\pi/c_E$	$1 + \left(\frac{D}{\ell}\right)$ horizontal
	$\ell \mid c_\pi/c_E$	$1 + \left(\frac{D}{\ell}\right)$ horizontal $\ell - \left(\frac{D}{\ell}\right)$ descending
$\ell \mid c_E$	$\ell \nmid c_\pi/c_E$	1 ascending
	$\ell \mid c_\pi/c_E$	1 ascending ℓ descending

Let's denote by $S_{N,q}$ the set of elliptic curves defined over a given finite field $\mathbb{F}_q$, up to $\bar{\mathbb{F}}_q$-isomorphism that have the same number of points N over $\mathbb{F}_q$. We separate $S_{N,q}$ to levels depending on the endomorphism rings of the elliptic curves where the order with the smallest conductor form the top level and levels descend as the conductor value of the orders increase. Hence, two elliptic curves E_1 and E_2 in $S_{N,q}$ is on the same level if $End(E_1) = End(E_2)$. An elliptic curve E is at the top level if $End(E) = \mathcal{O}_K$ and it is at the bottom level if $End(E) = \mathbb{Z}[\pi]$. Hence, there are more elliptic curves at lower levels than higher levels. If we connect these curves with ℓ-isogenies, the obtained structure resembles a *volcano* where the horizontal ℓ-isogenies at the top level form the crater.

A level of a volcano is called an *isogeny graph* $\mathcal{G}$, where the curves in that level form the vertices and equivalence classes of ℓ-isogenies between these curves over $\mathbb{F}_q$ form the edges. We consider only the ℓ-isogenies where ℓ is prime and less than or equal to some specified bound m. We denote the common endomorphism ring of all of the elliptic curves in this level by $End(E) = \mathcal{O}$. To be able to navigate the isogeny graph, we need it to be connected and have rapid mixing properties. Hence, m must be large enough. On the other hand, in order to construct the isogenies, m must not be too large. In [14], it is shown that there exists a constant $\delta > 0$ so that these requirements are satisfied when $m = (\log q)^{2+\delta}$.

Definition 12: Let B be a group and T be a generating set. We assign a color col_t to each generator t of T and let us assign every element b of B to the vertices of a graph. For each $b \in B$ and $t \in T$, the vertices corresponding to b and bt are joined by a directed edge of color col_t. Such a graph is called a *Cayley graph*.

Let $\mathfrak{a}, \mathfrak{b} \subset \mathcal{O}$ be invertible ideals. By the theory of complex multiplication [4, Section 10-11], $\mathfrak{a}$ (viewed as a 2-dimensional $\mathbb{Z}$-lattice in $\mathbb{C}$) gives rise to an elliptic curve $\mathbb{C}/\mathfrak{a}$ over some number field $L \subset \mathbb{C}$ which has a complex multiplication by $\mathcal{O}$ and $\mathfrak{b}$ defines an isogeny $\mathbb{C}/\mathfrak{a} \to \mathbb{C}/\mathfrak{a}\mathfrak{b}^{-1}$ that has degree $N(\mathfrak{b})$. Let us denote by $\mathcal{H}$ the graph whose vertices are these elliptic curves $\mathbb{C}/\mathfrak{a}$ and edges are complex analytic isogenies represented by $\mathfrak{b} \subset \mathcal{O}$ where $N(\mathfrak{b}) \leq m$ for the same bound m. Then Deuring's theory of canonical lifting of endomorphisms from characteristic p to characteristic zero [20], [9, Section 3] shows that the isogeny graph $\mathcal{G}$ is isomorphic to $\mathcal{H}$. In [14], it is observed that nodes of $\mathcal{H}$ are ideal classes of $\mathcal{O}$ and two ideal classes $[\mathfrak{a}_1]$ and $[\mathfrak{a}_2]$ are connected by an edge if and only if there exists a prime ideal $\mathfrak{b}$ with $\mathfrak{b} \leq m$ such that $[\mathfrak{a}_1\mathfrak{b}] = [\mathfrak{a}_2]$. Thus, $\mathcal{H}$ is isomorphic to a Cayley graph of the group $Cl(\mathcal{O})$ with respect to the generators $[\mathfrak{b}] \in Cl(\mathcal{O})$ for every prime ideal $\mathfrak{b}$ with $N(\mathfrak{b}) \leq m$. Since $\mathcal{G}$ is isomorphic to $\mathcal{H}$, it is also isomorphic to this Cayley graph.

Remark 1 ([14]): We can pass from $\mathcal{H}$ to $\mathcal{G}$ by taking reductions modulo a prime ideal in L lying over p and we can pass from $\mathcal{G}$ to $\mathcal{H}$ by Deuring's Lifting Theorem [20], [9]. Known algorithms for computing the isomorphism between $\mathcal{G}$ and $\mathcal{H}$ are exponential time algorithms. However, we are not required to compute it since we are only interested in the graph-theoretic properties of $\mathcal{G}$.

Theorem 2: [32, Theorem III.6.1.] Let $\phi : E_1 \to E_2$ be an homomorphism of degree ℓ. Then there exists a unique isogeny $\hat{\phi} : E_2 \to E_1$ such that

$$\hat{\phi} \circ \phi = [\ell] : E_1 \to E_1,$$

and $\deg(\hat{\phi}) = \ell$.

This isogeny $\hat{\phi}$ is called the *dual* isogeny of ϕ.

Remark 2 ([14]): Since each isogeny $\phi : E_1 \to E_2$ has a unique dual isogeny $\hat{\phi} : E_2 \to E_1$ of the same degree, $\mathcal{G}$ is actually an undirected graph for ordinary elliptic curves.

C. Expander Graphs

Let $G = (\mathcal{V}, E)$ be a k-regular finite graph on vertices $\mathcal{V} = \{v_1, \ldots, v_h\}$ with undirected edges. We denote the adjacency matrix of G by the symmetric $h \times h$ matrix A where $A_{ij} = 1$ if there is an edge between v_i and v_j, and $A_{ij} = 0$ otherwise. Since A is symmetric, it has an orthonormal basis where the basis elements are eigenvectors with eigenvalues $\lambda_0, \ldots, \lambda_{h-1}$. Without loss of generality, let us assume that $\lambda_0 \geq \lambda_1 \geq \ldots, \lambda_{h-1}$. It is easy to see that a constant vector is an eigenvector of A with eigenvalue $\lambda_0 = k$ and all of the eigenvalues of A satisfy the bound $\lambda \leq k$.

Definition 13: A family of such graphs G with $h \to \infty$ is said to be a sequence of *expander graphs* if λ_1 is bounded away from $\lambda_0 = k$ by a fixed amount.

To obtain expanders from abelian Cayley graphs, the aim of [14] is to obtain a nontrivial exponent $\beta < 1$ such that $\lambda_1 = O(k^\beta)$.

Proposition 4 ([14]): Suppose that the eigenvalue λ of any non-constant eigenvector satisfies the bound $\lambda \leq c$ for some $c < k$. Let $S \subset \mathcal{V}$ and x be any vertex in G. Then a random walk of any length at least $\frac{\log 2h/|S|^{1/2}}{\log k/c}$ starting from x will land in S with probability at least $\frac{|S|}{2|\mathcal{V}|}$.

Note that if the endpoint of the walk were uniformly random, probability of a random walk that starts at x to land in S would be $\frac{|S|}{|\mathcal{V}|}$. Hence, the proposition means that this probability is halved in our case for the random walks of length longer than the specified bound. In [14], the values k, $\frac{k}{k-c}$ and $\frac{|\mathcal{V}|}{|S|}$ are all bounded by polynomials in $\log(h)$. Hence, polylog(h) many random walks starting from x with length polylog(h) will land in S at least once with probability at least $1/2$. This rapid mixing result is used for the polynomial time random self-reducibility.

By the prime number theorem, $\lambda_0 = k$ is roughly $\frac{\pi(m)}{e} \sim \frac{m}{e \log m}$ where e is the number of units in $\mathcal{O}$. For $\mathcal{G}$ to be an expander graph, we need to show that the separation between λ_0 and λ_1 is of size $1/\text{polylog}(q)$ but this requires the assumption of Generalized Riemann Hypothesis (GRH).

Lemma 2: [14, Lemma 4.1] (Assuming GRH) Let $D < 0$ and let $\mathcal{O}$ be the quadratic order of discriminant D. Then λ_1 is bounded by $O(m^{1/2} \log |mD|)$.

If we let q large and $p(x) = x^{2+\delta}$ where $\delta > 0$ is fixed, this lemma shows that if we choose $m = p(\log q)$, then $\lambda_1 = O(\lambda_0^\beta)$ for any $\beta > \frac{1}{2} + \frac{1}{\delta+2}$, since $|D| \leq 4q$ and $\lambda_0 \sim \frac{m}{e \log m}$. Hence, our isogeny graphs are expanders and this bound with Proposition 4 proves the following theorem.

Theorem 3 ([14]): (Assuming GRH) There exists a polynomial $p(x)$, independent of N and q, such that for $m = p(\log q)$ the isogeny graph $\mathcal{G}$ on each level is an expander graph, in the sense that any random walk on $\mathcal{G}$ will reach a subset of size h with probability at least $\frac{h}{2|\mathcal{G}|}$ after polylog(q) steps (where the implicit polynomial is again independent of N and q).

Thus, if we have an algorithm A that solves the ECDLP for some proportion of the curves in a fixed level, a random walk from any curve probabilistically reaches this proportion in at most polylog(q) steps. Since each step consists of a low degree isogeny, their composition can be computed in polylog(q) steps. Hence, we obtain the following corollary.

Corollary 1 ([14]): (Assuming GRH) The ECDLP is random self-reducible in the following sense: given any algorithm A that solves the ECDLP on some fixed positive proportion of curves in a fixed level, one can probabilistically solve the ECDLP on any given curve in that same level with polylog(q) expected queries to A with random inputs.

As it can be seen from the corollary, the ECDLP random self-reduction is provided only for a fixed level and theoretically it is not proven for all elliptic curves in $S_{N,q}$. To reduce the ECDLP on one level to another, one needs to construct vertical isogenies between these levels and the fastest known algorithm [19] has complexity $O(\ell^4)$ where ℓ is the largest prime dividing the conductor of one level and not the other. Hence, this can be done when c_π is polynomially smooth. On the other hand, for a randomly selected curve over $\mathbb{F}_q$, most of the time $S_{N,q}$ consists of only one level.

D. Navigating the Isogeny Graph

Definition 14: The *j-invariant* of a lattice L is defined to be the complex number

$$j(L) = 1728 \frac{g_2(L)^3}{g_2(L)^3 - 27 g_3(L)^2}$$

where

$$g_2(L) = 60 \sum_{w \in L - \{0\}} \frac{1}{\omega^4} \quad \text{and} \quad g_3(L) = 140 \sum_{w \in L - \{0\}} \frac{1}{\omega^6}.$$

Over an algebraically closed field, two elliptic curves are isomorphic if and only if they have the same j-invariant. For a given elliptic curve E, if an elliptic curve E' is m-isogenous to E, then $j(E')$ is a root of the modular equation $\Phi_m(j(E), Y) = 0$ and the modular equation is of the form

$$\Phi_m(X, Y) = X^{m+1} + Y^{m+1} + \sum_{a=0}^{m} \sum_{b=0}^{m} f_{ab} X^a Y^b$$

where $f_{ab} \in \mathbb{Z}$.

Since the isogeny graph $\mathcal{G}$ has exponentially many nodes, it is not possible to compute the whole graph or store it. However, for a given curve E and a prime ℓ, we can navigate the isogeny graph locally by computing the curves E' that are connected to E with an isogeny of degree ℓ. Idea is to compute the j-invariants of the curves E' by solving the modular polynomial relation $\Phi_\ell(j(E), j(E')) = 0$. The time complexity of this step is $O(\ell^3)$ field operations [5, Section 3]. Once the j-invariants are known, the isogenies can be computed by using the algorithm of Fouquet–Morain [7].

IV. Counting Points on Genus 2 Curves with Real Multiplication

A. Introduction

We denote the Frobenius endomorphism of J_C by π and the dual by $\hat{\pi}$ such that $\pi\hat{\pi} = [q]$. The characteristic polynomial of π is of the form

$$\chi(T) = T^4 - s_1T^3 + (s_2 + 2q)T^2 - qs_1T + q^2 \qquad (1)$$

where s_1 and s_2 are integers. Determining the values of s_1 and s_2 is identical to solving the point counting problem because $\#J_C(\mathbb{F}_q) = \chi(1)$. Weil bounds imply that $|s_1| \leq 4\sqrt{q}$ and $|s_2| \leq 4q$ and Rück [27] shows that the possible values belong to the subset such that

$$\{(s_1, s_2) : s_1^2 - 4s_2 \geq 0 \text{ and } s_2 + 4q \geq 2|s_1|\}.$$

We denote by $[\ell]$ the multiplication by ℓ on J_C and $J_C[\ell]$ denotes its kernel. Similarly, if ϕ is an endomorphism on J_C then $J_C[\phi] = \ker(\phi)$.

Definition 15 ([11]): Let $P \mapsto D_P$ be a fixed embedding of C in J_C. We say that an endomorphism ϕ of J_C is *explicit* if we can effectively compute polynomials d_0, d_1, d_2, e_0, e_1, and e_2 such that if $P = (x_P, y_P)$ is a generic point of C, then the Mumford representation of $\phi(D_P)$ is given by

$$\left(x^2 + \frac{d_1(x_P)}{d_2(x_P}x + \frac{d_0(x_P)}{d_2(X_P)}, y - y_p\left(\frac{e_1(x_P)}{e_2(x_P)}x + \frac{e_0(x_P)}{e_2(x_P)}\right)\right).$$

The d_0, d_1, d_2, e_0, e_1, and e_2 are called the ϕ-division polynomials.

Let D be a generic element of J_C, then its Mumford representation is $D = (x^2 + a_1x + a_0, y - (b_1x + b_0))$. We can compute with this generic element by reducing the coefficients modulo I_ϕ where I_ϕ is an ideal in $\mathbb{F}_q[a_1, a_0, b_1, b_0]$ that vanishes on the nonzero elements of $J_C[\phi]$. Complexity analysis of [12] shows that we can compute I_ϕ in $\tilde{O}(\delta^3)$ field operations where δ is the maximum among all the degrees of the ϕ-division polynomials.

The efficient point counting algorithms originate from Schoof's work [29] and they construct $\chi(T)$ by first computing the polynomials $\chi_\ell(T) = \chi(T) \pmod{\ell}$ for sufficiently many primes ℓ and then using the Chinese Remainder Theorem (CRT).

Let $\bar{q}$ denote q modulo ℓ. In order to compute $\chi_\ell(T)$, we first compute $(\pi^2 + [\bar{q}])^2(D)$, $(\pi^2 + [\bar{q}])\pi(D)$, and $\pi^2(D)$ for a generic element D of $J_C[\ell]$ and then search for $(\bar{s_1}, \bar{s_2})$ in $(\mathbb{Z}/\ell\mathbb{Z})^2$ such that

$$(\pi^2 + [\bar{q}])^2(D) - [\bar{s_1}](\pi^2 + [\bar{q}])\pi(D) + [\bar{s_2}]\pi^2(D) = 0. \quad (2)$$

In [23], Pila shows that the set of primes ℓ with $\ell < 21 \log q$ is sufficient to apply the CRT. So the number of primes we use is $O(\log q)$.

The complexity of the classical Schoof–Pila point counting algorithm is as follows. For a fixed ℓ, we first compute the ℓ-division polynomials [3] to compute $\chi_\ell(T)$ that have degrees in $O(\ell^2)$. Then we compute the ideal I_ℓ in $\mathbb{F}_q[a_1, a_0, b_1, b_0]$ and since ℓ-division polynomials have degrees in $O(\ell^2)$, this computation costs $\tilde{O}(\ell^6)$ field operations. To check the equality in (1), we compute Frobenius images of the generic element in $\tilde{O}(\ell^4 \log q)$ and find the matching $(\bar{s_1}, \bar{s_2})$ in $\tilde{O}(\ell^5)$. Thus, the total complexity of computing $\chi_\ell(T)$ is $\tilde{O}(\ell^4(\ell^2 + \log q))$ field operations. Since we repeat this process for $O(\log q)$ many ℓs and since each ℓ is bounded by $O(\log q)$, the total complexity of the point counting algorithm becomes $\tilde{O}((\log q)^8)$.

For large values of ℓ, this algorithm becomes infeasible and in practice it is run for small values of ℓ to obtain s_1 and s_2 modulo some integer M and then a baby-step giant-step (BSGS) algorithm is used. When $M < 8\sqrt{q}$, BSGS algorithm reduces the search space of (s_1, s_2) from $O(q^{3/2})$ to $O(q^{3/4}/M^2)$ and the time complexity becomes $\tilde{O}(q^{3/4}/M)$. Since $|s_1| < 4\sqrt{q}$, when we have $M \geq 8\sqrt{q}$, the value of s_1 is fully determined and the search space reduces to $O(q/M)$ for which the time complexity becomes $\tilde{O}(\sqrt{q/M})$.

B. Point Counting in Genus 2 with Real Multiplication

Definition 16 ([11]): An explicit endomorphism ϕ is said to be *efficiently computable* if the cost of evaluating ϕ at points of $J_C(\mathbb{F}_q)$ requires only $O(1)$ field operations. In practice, this means that the ϕ-division polynomials have small degree.

When J_C is ordinary and simple, $\chi(T)$ becomes an irreducible polynomial defining a quartic CM-field with real quadratic subfield $\mathbb{Q}(\sqrt{\Delta})$ and J_C is said to have *real multiplication* (RM) by $\mathbb{Q}(\sqrt{\Delta})$. For a randomly selected curve, we have $\Delta = O(q)$ but [11] considers only the curves that admit an explicit (see Definition 15) endomorphism ϕ such that

$$\mathbb{Z}[\phi] = \mathbb{Q}(\sqrt{\Delta}) \cap \mathrm{End}(J_C)$$

and $\mathrm{disc}(\mathbb{Z}[\phi]) = \Delta$ for small Δ. The authors also provide examples for $\Delta = 5$ and $\Delta = 8$. Moreover, it is assumed that the trace $Tr(\phi)$ and norm $N(\phi)$ are known and ϕ is efficient (see Definition 16).

Let $\psi = \pi + \hat{\pi}$. Then $\mathbb{Z}[\psi]$ is a subring of the real quadratic subring of $\mathrm{End}(J_C)$ with characteristic polynomial

$$\xi(T) = T^2 - s_1T + s_2$$

and

$$\mathrm{disc}(\mathbb{Z}[\psi]) = s_1^2 - 4s_2.$$

Since $\mathbb{Z}[\phi] = \mathbb{Q}(\sqrt{\Delta}) \cap \mathrm{End}(J_C)$, $\mathbb{Z}[\psi]$ is contained in $\mathbb{Z}[\phi]$. So there exist integers m and n such that $\psi = m + n\phi$. We can determine s_1 and s_2 by computing n and m because $s_1 = \mathrm{Tr}(\psi) = 2m + n\mathrm{Tr}(\phi)$ and $s_2 = \mathrm{N}(\psi) = (s_1^2 - n^2\Delta)/4$.

We note that the composition of $\psi = \pi + \hat{\pi}$ and π gives

$$\psi\pi = \pi^2 + [q] = m\pi + n\phi\pi.$$

Thus, we can compute m and n modulo ℓ by first computing $(\pi^2 + [\bar{q}])(D)$, $\pi(D)$, and $\phi\pi(D)$ for a generic element D of $J_C[\ell]$ and then by searching for $(\bar{m}, \bar{n})$ in $(\mathbb{Z}/\ell\mathbb{Z})^2$ such that

$$(\pi^2 + [\bar{q}])(D) - [\bar{m}]\pi(D) - [\bar{n}]\phi\pi(D) = 0. \qquad (3)$$

Replacing equation (2) with equation (3) (i.e., searching for (m, n) instead of (s_1, s_2)) provides the following advantages:

1) Equation (2) requires four Frobenius computations which are costly in practice. However, equation (3) requires two Frobenius computations.

2) We have $s_1 = O(\sqrt{q})$ and $s_2 = O(q)$. However, m and n are both in $O(\sqrt{q})$, so the search space of BSGS reduces to $O(\sqrt{q}/M^2)$ and this reduces the time complexity of BSGS to $O(\sqrt{q}/M)$.
3) The multiplication of m and n is also in $O(\sqrt{q})$ and this reduces the number of primes ℓ to be considered by half.

C. Split Primes in $\mathbb{Q}(\sqrt{\Delta})$

If a prime ℓ splits in an RM order $\mathbb{Z}[\phi]$ in $\mathbb{Q}(\phi) \cong \mathbb{Q}(\Delta)$ as $(\ell) = \mathfrak{p}_1\mathfrak{p}_2$, then $J_C[\ell]$ decomposes as $J_C[\ell] = J_C[\mathfrak{p}_1] \oplus J_C[\mathfrak{p}_2]$. Moreover, any point D in $J_C[\ell]$ can be uniquely expressed as a sum $D = D_1 + D_2$ where D_i is in $J_C[\mathfrak{p}_i]$.

If the order $\mathbb{Z}[\phi]$ has class number 1 (i.e., the number of elements of $Cl(\mathbb{Z}[\phi])$ is 1), then all of its ideals are principal. Hence, we can find a generator for each of the ideals $\mathfrak{p}_i$ and [11] shows that the coefficients of these generators are in $O(\sqrt{q})$ and the generators can be computed in $O(\ell)$ field operations.

Both $\psi(D_i)$ and $\phi(D_i)$ are elements of $\mathbb{Z}[\phi]/\mathfrak{p}_i \cong \mathbb{Z}/\ell\mathbb{Z}$. We know $\bar{x}_i = \phi \pmod{\mathfrak{p}_i}$, so we have

$$\psi(D_i) = [\bar{m} + \bar{n}\bar{x}_i](D_i) = [\bar{y}_i](D_i).$$

Th composition of both sides with π gives

$$(\pi^2 + [\bar{q}])(D_i) = [\bar{y}_i]\pi(D_i),$$

which is a discrete logarithm in the cyclic group $\langle D_i \rangle \cong \mathbb{Z}/\ell\mathbb{Z}$. We first compute $(\bar{y}_1, \bar{y}_2)$ and recover $\bar{y}$ in $\mathbb{Z}[\phi]/(\ell)$ by CRT. Then we solve for $(\bar{m}, \bar{n})$ such that $\bar{y} = \bar{m} + \bar{n}\phi \in \mathbb{Z}[\phi]/(\ell)$.

Asymptotically, half of the primes ℓ split in $\mathbb{Z}[\phi]$ by the Chebotarev density theorem [4, Theorem 8.17]. So it suffices to consider split primes in $O(\log q)$. The advantage of working with split primes is, the computations are modulo the ideal for $J_C[\mathfrak{p}_i]$ of degree in $O(\ell^2)$ instead of the ideal for $J_C[\ell]$ of degree in $O(\ell^4)$. This reduces the complexity of computing $\chi_\ell(T)$ from $\tilde{O}(\ell^4(\ell^2 + \log q))$ to $\tilde{O}(\ell^2(\ell + \log q))$. Thus, the complexity of the point counting algorithm reduces from $\tilde{O}((\log q)^8)$ to $\tilde{O}((\log q)^5)$.

The computation of the order of an RM Jacobian defined over a 512-bit prime field is provided in [11] to show the reduced complexity of the point counting problem that is obtained by using split primes. Note that the previous record of point counting in genus 2 was over a 128-bit field.

V. Research Proposal

For an elliptic curve to resist the known attacks on the ECDLP, its group order should satisfy some properties (see Section I). In practice, a randomly selected elliptic curve is kept if it satisfies these constraints. This common practice assumes that the discrete logarithm problems for two elliptic curves over the same finite field having the same number of points are equally hard. However, its correctness was not known until the formal justification of [14]. The attacks on the ECDLP mentioned in Section I have similar variants that are applicable to curves of higher genus. Therefore, random selection of curves of genera 2 and 3 should be justified, too.

Like the ECDLP, there is no known subexponential algorithm to solve the discrete logarithm problem on the Jacobians of a curve of small genus over a finite field. Moreover, a hyperelliptic curve C over the finite field $\mathbb{F}_q$ with genus g has $\#J_C(\mathbb{F}_q) \approx q^g$. Thus, when compared to an elliptic curve cryptosystem, we can choose a much smaller underlying finite field for a hyperelliptic curve cryptosystem to achieve the same security. For example, an elliptic curve cryptosystem defined by an ordinary elliptic curve over $\mathbb{F}_{2^{160}}$ has the same security as a hyperelliptic curve cryptosystem defined by a genus 2 curve over $\mathbb{F}_{2^{80}}$.

However, the attack of [1] provides a subexponential algorithm for the DLP on the Jacobians of large genus hyperelliptic curves. Although this attack becomes exponential for small genus, it is still faster than Pollard's Rho [7] attack when $g \geq 3$. Hence, only the genus 2 curves are unaffected by this attack and for this reason, we propose to investigate genus 2 curves in this research, with the main goal of showing that the DLP is equally hard in a large class of genus 2 curves.

As it is done for the random self-reducibility of the ECDLP in [14], our first goal is to show the random self-reducibility of the DLP for genus 2 curves having the same endomorphism ring. Then we will focus on constructing ascending/descending isogenies to provide random self-reducibility of the DLP for the curves having different endomorphism rings. However, moving from genus 1 to genus 2 curves introduces differences and new technical difficulties. First of all, two genus 2 curves having the same number of points are not necessarily isogenous. Indeed, Tate's isogeny theorem says that two abelian varieties A_1 and A_2 over $\mathbb{F}_q$ are isogenous if and only if their respective Frobenius endomorphisms have the same characteristic polynomial (in the case of elliptic curves, this is equivalent to having the same number of points). Thus, we restrict and study the random self-reducibility of the DLP for genus 2 curves whose Frobenius endomorphisms have the same characteristic polynomial.

On the other hand, genus 2 curves lack some of the efficient algorithms we have for elliptic curves. For example, as mentioned in Section IV, point counting algorithms become impractical when the underlying finite field is large. Furthermore, explicitly computing isogenies for genus 2 curves is not as efficient as constructing isogenies for genus 1 curves.

Definition 17: [13, Lemma 7.6] Let A be a principally polarized abelian surface and let R be a proper subgroup of $A[\ell]$. Then R is the kernel of an isogeny of principally polarized abelian surfaces $\varphi : A \longrightarrow B$ if and only if $R \cong (\mathbb{Z}/\ell\mathbb{Z})^2$ is a maximal isotropic subgroup with respect to the Weil pairing. Such a φ is called an (ℓ, ℓ)-isogeny.

A polynomial time algorithm for computing (ℓ, ℓ)-isogenies on Jacobians of genus 2 curves is provided in [26]. So we can construct (ℓ, ℓ)-isogenies when we are constructing our isogeny graphs but not every isogeny is of this form. Also, one has to carefully select the ℓ's according to their decomposition in the quartic field. Thus we will not be able to construct every isogeny. Another drawback is, as it is shown in [13], an isogeny graph that is drawn using (ℓ, ℓ)-isogenies does not have a volcano shape. These introduce extra difficulties for constructing and navigating the isogeny graphs.

Moreover, the arithmetic of higher genus curves is much more complex than the arithmetic of elliptic curves. Speeding up the arithmetic of genus 2 curves is also an area that we want to focus in this research and to the best of our knowledge, fastest genus 2 arithmetic is provided in [10] which is based on Theta functions.

In addition, ordinary elliptic curves over a finite field have complex multiplication in an imaginary quadratic field. In an imaginary quadratic field K, orders are uniquely identified by their index in $\mathcal{O}_K$ (i.e., by their conductors). Thus, the endomorphism rings generated by the ordinary elliptic curves over the same finite field having the same number of points form a tower (see Figure 1). However, all genus 2 curves over a finite field have complex multiplication in a quartic field and the endomorphism rings in this case form a lattice, instead of a tower. An example to lattice of orders is given in Figure 2 where the vertices represent orders and the edges indicate that the order below is contained in the order above. Therefore, it is harder to identify the endomorphism rings of the genus 2 curves and navigate between levels. Bisson provided a subexponential algorithm [2, Algorithm IV.I.4] to locate the endomorphism ring of a curve on such lattices.

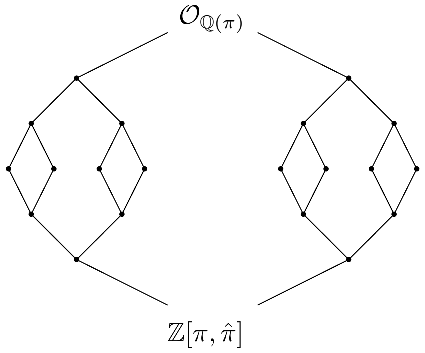

Fig. 2. Endomorphism rings of genus 2 curves

Unlike the elliptic curve case, in the genus 2 case isomorphism invariants of curves are Igusa invariants j_1, j_2, j_3 [13, Section 7.2.2]. In this case, one needs to know how to compute the Igusa invariants of (ℓ, ℓ)-isogenous curves.

In this research, we are also interested in the computational challenges such as the point counting problem and computation of explicit isogenis. We want to improve and implement algorithms related to these problems.

References

[1] 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.

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

[3] D. G. Cantor. On the analogue of the division polynomials for hyperelliptic curves. *J. Reine Angew. Math.*, 447:pp. 91–146, 1994.

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

[5] N. D. Elkies. Elliptic and modular curves over finite fields and related computational issues. In *Computational perspectives on number theory (Chicago, IL, 1995)*, volume 7 of *Studies in Advanced Mathematics*, pages 21–76, Providence, RI, 1998. AMS International Press.

[6] J. Feigenbaum and L. Fortnow. On the random-self-reducibility of complete sets. In *Structure in Complexity Theory Conference*, pages 124–132, 1991.

[7] M. Fouquet and F. Morain. Isogeny volcanoes and the SEA algorithm. In *ANTS*, pages 276–291, 2002.

[8] G. Frey and H.-G. Rück. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Math. Comput.*, 62:865–874, April 1994.

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

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

[11] P. Gaudry, D. Kohel, and B. Smith. Counting points on genus 2 curves with real multiplication. Cryptology ePrint Archive, Report 2011/295. To appear in ASIACRYPT 2011. Available from http://eprint.iacr.org/2011/295.

[12] P. Gaudry and É. Schost. Construction of secure random curves of genus 2 over prime fields. In *EUROCRYPT*, pages 239–256, 2004.

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

[14] 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.

[15] N. Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*, 48(177):pp. 203–209, 1987.

[16] N. Koblitz. Hyperelliptic cryptosystems. *J. Cryptology*, 1(3):pp. 139–150, 1989.

[17] N. Koblitz. CM-curves with good cryptographic properties. In *CRYPTO*, pages 279–287, 1991.

[18] N. Koblitz. Getting a few things right and many things wrong. In *INDOCRYPT*, page pp. 1, 2010.

[19] D. Kohel. *Endomorphism Rings of Elliptic Curves over Finite Fields*. PhD thesis, University of California, Berkeley, Fall 1996.

[20] S. Lang. *Elliptic Functions*. Graduate texts in mathematics. Springer-Verlag, 1987.

[21] A. Menezes, T. Okamoto, and S. A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Transactions on Information Theory*, 39(5):1639–1646, 1993.

[22] V. S. Miller. Use of elliptic curves in cryptography. In *CRYPTO*, pages 417–426, 1985.

[23] J. Pila. Frobenius maps of abelian varieties and finding roots of unity in finite fields. *Mathematics of Computation*, 55(192):pp. 745–763, 1990.

[24] S. Pohlig and M. Hellman. An improved algorithm for computing logarithms over GF(p) and its cryptographic significance (Corresp.). *Information Theory, IEEE Transactions on*, 24(1):106–110, 1978.

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

[26] D. Robert and R. Cosset. Computing (l,l)-isogenies in polynomial time on Jacobians of genus 2 curves. (unpublished), 2011.

[27] H.-G. Rück. Abelian surfaces and jacobian varieties over finite fields. *Compositio Mathematica*, 76(3):pp. 351–366, 1990.

[28] T. Satoh and K. Araki. Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves. *Commentarii Mathematici Universitatis Sancti Pauli*, 47:81–92, 1998.

[29] R. Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Math. Comp.*, 44:pp. 483–494, 1985.

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

[31] I. A. Semaev. Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p. *Math. Comput.*, 67:353–356, January 1998.

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

[33] N. P. Smart. The discrete logarithm problem on elliptic curves of trace one. *J. Cryptology*, 12(3):193–196, 1999.

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

[35] P. C. van Oorschot and M. J. Wiener. Parallel collision search with cryptanalytic applications. *J. Cryptology*, 12(1):1–28, 1999.