

HORIZONTAL ISOGENY GRAPHS OF ORDINARY ABELIAN VARIETIES AND THE DISCRETE LOGARITHM PROBLEM

DIMITAR JETCHEV AND BENJAMIN WESOLOWSKI

ABSTRACT. Fix an ordinary abelian variety defined over a finite field. The ideal class group of its endomorphism ring acts freely on the set of isogenous varieties with same endomorphism ring, by complex multiplication. Any subgroup of the class group, and generating set thereof, induces an isogeny graph on the orbit of the variety for this subgroup. We compute (under the Generalized Riemann Hypothesis) some bounds on the norms of prime ideals generating it, such that the associated graph has good expansion properties.

We use these graphs, together with a recent algorithm of Dudeanu, Jetchev and Robert for computing explicit isogenies in genus 2, to prove random self-reducibility of the discrete logarithm problem within the subclasses of principally polarizable ordinary abelian surfaces with fixed endomorphism ring. In addition, we remove the heuristics in the complexity analysis of an algorithm of Galbraith for explicitly computing isogenies between two elliptic curves in the same isogeny class, and extend it to a more general setting including genus 2.

1. INTRODUCTION

1.1. Motivation. Let \mathcal{C} be a hyperelliptic curve of genus g defined over a finite field \mathbf{F}_q and let $\mathcal{J} = \text{Jac}(\mathcal{C})$ be its Jacobian – a principally polarized abelian surface over \mathbf{F}_q . The discrete logarithm problem (or DLP) in genus g is the following: given $P \in \mathcal{J}(\mathbf{F}_q)$ and $Q = rP \in \mathcal{J}(\mathbf{F}_q)$ for some secret multiplier r , compute r . The problem for $g = 1$ is known as the elliptic curve discrete logarithm problem (or ECDLP); it is a central tool in public key cryptography, and has been extensively studied since its introduction in the 1980’s [Mil86, Kob87]. The case of $g = 2$ has been shown to be a promising alternative, allowing very efficient arithmetic [Gau07, BCHL16], but very little is known about the hardness of the corresponding version of the DLP. Apart from the question of the hardness of the problem on a particular Jacobian, one may ask how the difficulty of the problem compares on two distinct Jacobians. A natural way of transferring the problem from one Jacobian to another is via isogenies. It is thus of interest to study whether two Jacobians of genus 2 curves have the same difficulty of the problem, assuming that there exists an isogeny between them. Tate’s isogeny theorem [Tat66] implies that two abelian surfaces over a finite field are isogenous if and only if the characteristic polynomials of the Frobenius acting on their ℓ -adic Tate modules are the same. The latter can be computed efficiently, so it is easy to determine if two Jacobians are isogenous. It is however not clear how to explicitly compute an isogeny between two such Jacobians, which is actually needed to transfer the discrete logarithm problem.

Date: January 27, 2017.

Key words and phrases. Isogeny, expander graph, hyperelliptic curve cryptography, random self-reducibility, discrete logarithm.

The case of ordinary elliptic curves has been treated by Jao, Miller and Venkatesan [JMV05, JMV09] using random walks on isogeny graphs and rapid mixing arguments. A crucial ingredient in their analysis is that one can efficiently compute isogenies of small degrees, polylogarithmic in q . More precisely, one considers a graph with vertices the set of isomorphism classes of elliptic curves in the isogeny class that have a fixed endomorphism ring. These isomorphism classes correspond, by CM theory, to the ideal classes of that endomorphism ring. The edges of the graph correspond to *horizontal* isogenies, that is, α -transforms in the language of [ST61]. It turns out that it is connected for suitably chosen bounds on the ideal norms and, under GRH, it rapidly mixes random walks (i.e., behaves as an expander graph). Via random walks on this graph, one can show that it is possible to reduce the discrete logarithm problem from a given curve to the problem to a uniformly random curve in that class, thus obtaining random self-reducibility of the elliptic curve discrete logarithm problem within the class.

The similar problem in genus 2 is much more challenging since, unlike elliptic curves, abelian surfaces are not *a priori* principally polarized, so a quotient of a Jacobian by a finite subgroup need not be the Jacobian of a curve. Even if it is, there might be multiple non-equivalent principal polarizations giving rise to non-isomorphic curves¹. In addition, if one tries the straightforward analogy to [JMV05] of constructing isogeny graphs with vertices that are ideal classes in the class group of the endomorphism algebra (in this case, a quartic CM-field), one may get abelian surfaces that are not even principally polarizable and hence, unsuitable for transferring the discrete logarithm problem in practice. Finally, even if the target is principally polarizable, for the purpose of proving random self-reducibility, one does not need just one principal polarization on the target, but all of them, or at least the capability to sample one uniformly at random.

1.2. Main theorem. Jacobians of genus 2 hyperelliptic curves will be seen as a particular case of the following, more general situation. Let \mathcal{A} be an absolutely simple, ordinary abelian variety of dimension g over a finite field and let $K = \text{End}(\mathcal{A}) \otimes \mathbf{Q}$ be the corresponding CM field. The endomorphism ring $\text{End}(\mathcal{A})$ is isomorphic to an order \mathcal{O} of conductor \mathfrak{f} in K . The ideal class group $\text{Cl}(\mathcal{O})$ acts freely on the set of varieties isogenous to \mathcal{A} with same endomorphism ring \mathcal{O} , by complex multiplication. Let $H \subseteq \text{Cl}(\mathcal{O})$ be any subgroup and let $H(\mathcal{A})$ the H -orbit of \mathcal{A} . The choice of a set \mathcal{S} of invertible ideals in \mathcal{O} generating H induces a graph whose set of vertices is $H(\mathcal{A})$ and whose edges are labelled with isogenies between these abelian varieties. The norms of the ideals in \mathcal{S} are exactly the degrees of the induced isogenies. For any $B > 0$ and ideal \mathfrak{m} in \mathcal{O} , let \mathcal{S}_B be the set of ideals in \mathcal{O} of prime norm and coprime to \mathfrak{m} . Let \mathcal{G}_B be the induced isogeny graph, where all the degrees are bounded by B .

Theorem 1.1 (Rapid mixing for $H(\mathcal{A})$). *Assuming the Generalized Riemann Hypothesis, for any $\varepsilon > 0$, there exists a bound*

$$B = O\left((g[\text{Cl}(\mathcal{O}) : H] \ln(d_K N(\mathfrak{m})))^{2+\varepsilon}\right),$$

¹An example of this phenomenon has been given by Howe [How96]. More precisely, Howe showed that the curves $y^2 = x^5 + x^3 + x^2 - x - 1$ and $y^2 = x^5 - x^3 + x^2 - x - 1$ over \mathbf{F}_{11} are not isomorphic; yet, their Jacobians are absolutely simple and isomorphic as non-polarized abelian surfaces.

such that for any subset W of $H(\mathcal{A})$, any random walk in \mathcal{G}_B of length at least $\ln(2|H|/|W|^{1/2})$ starting from a given vertex will end in W with probability between $|W|/(2|H|)$ and $3|W|/(2|H|)$. In particular, the regular graph \mathcal{G}_B is connected and rapidly mixes random walks.

It is worth noticing that even the connectivity of the graph is new: the classical bounds for connectivity are derived from Bach's bounds [Bac90], which can only be applied when H is the full class group $\text{Cl}(\mathcal{O})$. We will prove Theorem 1.2 as a corollary of the following theorem. It constructs and proves that certain Cayley graphs for subgroups of more general ray class groups are expanders.

Theorem 1.2. *Let K be a number field of degree n and discriminant d_K , \mathfrak{m} an integral ideal of \mathcal{O}_K , G the narrow ray class group of K modulo \mathfrak{m} , and H a subgroup of G . For any ideal \mathfrak{l} of \mathcal{O}_K coprime to \mathfrak{m} , let $[\mathfrak{l}]$ denote its image in G . Let*

$$T_{H,\mathfrak{m}}(B) = \{\text{prime ideals } \mathfrak{l} \text{ of } \mathcal{O}_K \mid (\mathfrak{l}, \mathfrak{m}) = 1, N\mathfrak{l} \leq B \text{ is prime and } [\mathfrak{l}] \in H\}.$$

Let $T_{H,\mathfrak{m}}(B)$ be the multiset of its image in G . Let \mathcal{G}_B be the graph whose vertices are the elements of H and whose non-oriented edges are precisely (h, sh) for any $h \in H$ and $s \in T_{H,\mathfrak{m}}(B)$. Assuming the Generalized Riemann Hypothesis, for any character χ of H , the corresponding eigenvalue λ_χ of the Cayley graph \mathcal{G}_B satisfies

$$\lambda_\chi = \frac{\delta(\chi)}{[G:H]} \text{li}(B) + O\left(nB^{1/2} \ln(Bd_K N\mathfrak{m})\right),$$

where $\delta(\chi)$ is 1 if χ is trivial, and 0 otherwise. The implied constants are absolute.

Note that a similar result is proven in [JMV09], where H is the full narrow ray class group, rather than a subgroup. It was sufficient to study isogeny graphs of elliptic curves, which can be represented as Cayley graphs of class groups in imaginary quadratic fields. However, it is not strong enough for higher genus, where one needs to work on subgroups of class group of CM-fields, due to the extra condition of principal polarizability. Since properties of expander graphs do not transfer nicely to subgraphs in general, the refinement provided by Theorem 1.2 is crucial.

1.3. Applications of Theorem 1.1. Using the CM theory for polarized class groups, we will apply Theorem 1.1 to analyse isogeny graphs of Jacobians of hyperelliptic curves of genus 2. More precisely let \mathcal{A} be an absolutely simple, ordinary principally polarizable abelian surface. Let K be its quartic CM-field, and let K_0 be its real quadratic subfield, and let \mathcal{O} be the order in K isomorphic to $\text{End}(\mathcal{A})$. Let $\mathcal{P}(\mathcal{O}) \trianglelefteq \text{Cl}(\mathcal{O})$ be the image of the natural projection of the Shimura class group $\mathfrak{C}(\mathcal{O})$ on the ideal class group $\text{Cl}(\mathcal{O})$. As explained in Section 2.3.2, the orbit $\mathcal{P}(\mathcal{A})$ of the CM-action of $\mathcal{P}(\mathcal{O})$ on \mathcal{A} is a set of \mathbf{F}_q -isomorphism classes of principally polarizable abelian surfaces isogenous to \mathcal{A} and with same endomorphism ring \mathcal{O} . This orbit contains *all* such isomorphism classes when the CM-action is transitive, for instance when \mathcal{O} has maximal real multiplication (i.e., $\mathcal{O}_{K_0} \subset \mathcal{O}$). Let d_K be the discriminant of K . Applying Theorem 1.1 allows to construct isogeny graphs on $\mathcal{P}(\mathcal{A})$ that are expanders, and where all the isogenies are cyclic, with prime degrees bounded by $O([\text{Cl}(\mathcal{O}) : \mathcal{P}(\mathcal{O})] \ln d_K)^{2+\epsilon})$. When K is a primitive CM-field, the index $[\text{Cl}(\mathcal{O}) : \mathcal{P}(\mathcal{O})]$ is the narrow class number of $\mathcal{O} \cap K_0$.

This result is used for two major applications, concerning the discrete logarithm problem in genus 2 and the computation of explicit isogenies between two isogenous

principally polarized ordinary abelian surfaces. Aside from this, we remove certain heuristics from the complexity analysis of Galbraith’s algorithm for elliptic curves.

1.3.1. *Random self-reducibility of the discrete logarithm problem in genus 2.* We use the rapid mixing properties of isogeny graphs to prove that the discrete logarithm problem in genus 2 is random self-reducible in isogeny subclasses of ordinary Jacobians of genus 2 curves over a finite field, thus extending the similar result for elliptic curves proved in [JMV09, Th. 1.6].

Theorem 1.3 (Random self-reducibility in genus 2). *Let K be a primitive quartic CM-field, K_0 its maximal real subfield, and \mathcal{O} an order in K . Let \mathcal{J} be a Jacobian defined over \mathbf{F}_q of endomorphism ring isomorphic to \mathcal{O} . Let \mathcal{V} be the set of all \mathbf{F}_q -isomorphism classes of Jacobians defined over \mathbf{F}_q , isomorphic to \mathcal{J} and with endomorphism ring isomorphic to \mathcal{O} . Let G be a subgroup of $\mathcal{J}(\mathbf{F}_q)$ of order Q . Suppose that*

- (1) *there is a polynomial time (in $\log q$) algorithm \mathcal{A} that solves the DLP for a positive proportion $\mu > 0$ of the Jacobians in \mathcal{V} ,*
- (2) *$\mathcal{O} \cap K_0$ is the ring of integers of K_0 , and $[\mathcal{O} : \mathbf{Z}[\pi, \bar{\pi}]]$ is coprime to $2Q$.*

Then, assuming the Generalized Riemann Hypothesis, there is an absolute polynomial P in three variables such that the DLP can be solved on G by a probabilistic algorithm of expected runtime $P(\log q, h_{\mathcal{O}_0}^+, \text{Disc}(K_0))/\mu$, where $h_{\mathcal{O}_0}^+$ is the narrow class number of the order $\mathcal{O}_0 = \mathcal{O} \cap K_0$.

Remark 1. In most practical applications, since the CM method is currently the only viable method to generate cryptographic parameters, both the narrow class number $h_{\mathcal{O}_0}^+$ and the discriminant $\text{Disc}(K_0)$ are small (constant or at most polynomial in $\log q$), and the above algorithm yields a polynomial (in $\log q$) reduction and thus, justifies the common cryptographic belief that the security of these curves is governed only by the characteristic polynomial of Frobenius.

Remark 2. The conditions that $\mathcal{O} \cap K_0$ is the ring of integers of K_0 , and $[\mathcal{O} : \mathbf{Z}[\pi, \bar{\pi}]]$ is coprime to $2Q$ appear because they are required by the only currently known algorithm [DJR14, Dud16] to compute cyclic isogenies in genus 2.

1.3.2. *Explicit isogenies in genus 2.* In [Gal99], Galbraith considers the problem of computing an explicit isogeny between two isogenous ordinary elliptic curves E_1 and E_2 over \mathbf{F}_q . His approach is based on considering isogeny graphs and growing trees rooted at both E_1 and E_2 of small-degree computable isogenies until a collision is found. Galbraith’s original algorithm is proven to finish in probabilistic polynomial time (in $\log q$), finding a path of length $O(\ln h_K)$ from E_1 to E_2 , under GRH and a heuristic assumption claiming that the distribution of the new random points found in the process of growing the trees is close to uniform. In Section 5, we use the expander properties of isogeny graphs to construct and analyze an algorithm similar to the one from [Gal99]. This new algorithm improves upon Galbraith’s in two ways. Firstly, its analysis relies only on GRH, without any additional heuristics. Secondly, it works in a generalized framework which, in particular, encompasses the case of elliptic curves, and of Jacobians of genus 2 hyperelliptic curves.

1.4. **Organization of the paper.** Section 2 contains the necessary background on abelian varieties with complex multiplication, polarizations, and canonical lifting, and uses this theory to build the bridge between isogeny graphs and some Cayley

graphs. In Section 3 we prove Theorem 1.2 and use it to prove Theorem 1.1. In Section 4, we discuss the consequences of these results on isogeny graphs of principally polarized abelian surfaces over finite fields and deduce Theorem 1.3, the random self-reducibility. Finally, we present the generalization of Galbraith's algorithm as well as the new complexity analysis in Section 5.

2. ISOGENY GRAPHS OF ORDINARY ABELIAN VARIETIES

In this section, we describe the relation between our graphs of interest – graphs of horizontal isogenies between ordinary abelian varieties over finite fields – and class groups of certain number fields, or subgroups thereof.

2.1. Isogeny graphs over finite fields. Let \mathcal{A} be an absolutely simple, ordinary abelian variety of dimension g over a finite field \mathbf{F}_q . Its endomorphism algebra $K = \text{End}(\mathcal{A}) \otimes \mathbf{Q}$ is a CM-field, that is a totally imaginary quadratic extension of a totally real number field K_0 . The field K_0 is of degree g over \mathbf{Q} . The *Frobenius polynomial* is the characteristic polynomial of the Frobenius endomorphism π acting on the ℓ -adic Tate module $T_\ell \mathcal{A}$ for ℓ different from the characteristic of \mathbf{F}_q . This endomorphism generates the field $K = \mathbf{Q}(\pi)$, and a theorem due to Tate [Tat66] states that two abelian varieties defined over \mathbf{F}_q are isogenous if and only if they have the same Frobenius polynomial. This element π seen in $\overline{\mathbf{Q}}$ is a q -Weil number, and it uniquely determines the isogeny class of simple abelian varieties over \mathbf{F}_q with Frobenius π [Str10, Lemma IV.2.2]. The endomorphism ring of \mathcal{A} is an order $\mathcal{O} = \text{End}(\mathcal{A})$ in the CM-field K . We are interested in *horizontal* isogeny graphs, i.e., graphs whose vertices are abelian varieties with the same endomorphism ring \mathcal{O} and whose edges are labelled by certain isogenies between these varieties.

The abelian varieties arising in cryptography are constructed as Jacobians of some hyperelliptic curves (usually of genus 1 or 2), and are therefore principally polarized. The case of elliptic curves is well understood and the literature on their isogeny graphs is already extensive. The present work aims at generalizing some of that literature, dealing with horizontal isogeny graphs, to other families of abelian varieties. We put a particular focus on principally polarized abelian surfaces, where these new results combined with the algorithm of [DJR14, Dud16] give rise to some interesting applications, yet the framework we develop is much more general.

2.2. Class groups of orders. Class groups of orders in number fields are closely related to horizontal isogeny graphs, via the theory of complex multiplication, as will be recalled in Section 2.3. In this subsection, we fix the notations and recall some useful results on class groups.

Let K be a number field. Then, $\mathcal{I}(K)$ denotes the group of fractional ideals of \mathcal{O}_K . Fix a modulus \mathfrak{m} , that is a formal product of primes in K , finite or infinite. The finite part is an ideal \mathfrak{m}_0 in \mathcal{O}_K , and the infinite part is a subset \mathfrak{m}_∞ of the real embeddings of K . Let $\mathcal{I}_\mathfrak{m}(K)$ be the subgroup generated by ideals coprime to \mathfrak{m}_0 . Let $P_{K,1}^\mathfrak{m}$ be the subgroup of $\mathcal{I}_\mathfrak{m}(K)$ generated by principal ideals of the form $\alpha \mathcal{O}_K$ where $\text{ord}_\mathfrak{p}(\alpha - 1) \geq \text{ord}_\mathfrak{p}(\mathfrak{m}_0)$ for all primes \mathfrak{p} dividing \mathfrak{m}_0 , and $\iota(\alpha) > 0$ for all $\iota \in \mathfrak{m}_\infty$. The *ray class group* of K modulo \mathfrak{m} is the quotient group $\text{Cl}_\mathfrak{m}(K) = \mathcal{I}_\mathfrak{m}(K) / P_{K,1}^\mathfrak{m}$. The *narrow ray class group* modulo the ideal \mathfrak{m}_0 is $\text{Cl}_\mathfrak{m}(K)$ when \mathfrak{m}_∞ contains all the real embeddings.

Example 1. The subgroup $P_{K,1}^{\mathcal{O}_K}$ is generated by all the principal ideals, so $\text{Cl}_{\mathcal{O}_K}(K)$ is the usual ideal class group $\text{Cl}(K)$. Also, the narrow ray class group modulo \mathcal{O}_K is exactly the narrow class group $\text{Cl}^+(K)$.

Let \mathcal{O} be an order in K . The *conductor* of \mathcal{O} , defined as $\mathfrak{f} = \{x \in K \mid x\mathcal{O}_K \subset \mathcal{O}\}$, is an invariant of the order. It is the largest subset of K that is simultaneously an ideal in \mathcal{O} and in the maximal order \mathcal{O}_K . An ideal in \mathcal{O} is invertible if and only if it is coprime to the conductor \mathfrak{f} . Let $\mathcal{I}(\mathcal{O})$ denote the group of invertible ideals of \mathcal{O} , and $P(\mathcal{O})$ the subgroup generated by principal ideals. The class group of \mathcal{O} is the quotient $\text{Cl}(\mathcal{O}) = \mathcal{I}(\mathcal{O})/P(\mathcal{O})$. It can also be expressed as a quotient of $\mathcal{I}_{\mathfrak{f}}(K)$, as follows. Let $P_{K,\mathcal{O}}^{\mathfrak{f}}$ be the subgroup of $\mathcal{I}_{\mathfrak{f}}(K)$ generated by principal ideals $\alpha\mathcal{O}_K$ where $\alpha \in \mathcal{O}$ and $\alpha\mathcal{O} + \mathfrak{f} = \mathcal{O}$. From [LD15, Th. 3.8] and [LD15, Th. 3.11], the map sending any integral ideal \mathfrak{a} of \mathcal{O}_K to the ideal $\mathfrak{a} \cap \mathcal{O}$ of \mathcal{O} extends to a surjection $\mathcal{I}_{\mathfrak{f}}(K) \rightarrow \text{Cl}(\mathcal{O})$ with kernel $P_{K,\mathcal{O}}^{\mathfrak{f}}$. Therefore, it induces an isomorphism

$$\text{Cl}(\mathcal{O}) \cong \mathcal{I}_{\mathfrak{f}}(K)/P_{K,\mathcal{O}}^{\mathfrak{f}}.$$

From [LD15, Th. 4.2], there is a unique abelian extension $H(\mathcal{O})$ of K , the *ring class field* of \mathcal{O} , such that all primes of K ramified in $H(\mathcal{O})$ divide \mathfrak{f} , and the kernel of the Artin map

$$\varphi_{H(\mathcal{O})/K}^{\mathfrak{f}} : \mathcal{I}_{\mathfrak{f}}(K) \rightarrow \text{Gal}(H(\mathcal{O})/K)$$

is $P_{K,\mathcal{O}}^{\mathfrak{f}}$. This map then induces an isomorphism $\text{Cl}(\mathcal{O}) \cong \text{Gal}(H(\mathcal{O})/K)$. Similarly, there is a unique abelian extension $H^+(\mathcal{O})$, the *narrow ring class field* of \mathcal{O} , ramified only at primes dividing \mathfrak{f} and at infinite primes, such that $\text{Gal}(H^+(\mathcal{O})/K)$ is isomorphic to the narrow class group $\text{Cl}^+(\mathcal{O})$, through the Artin map.

2.3. Abelian varieties over \mathbf{C} with CM. A key tool for studying isogeny graphs is the theory of complex multiplication (henceforth, CM theory) The main reference for this section is [ST61]. Let $\mathcal{A}_{\mathbf{C}} = \mathbf{C}^g/\Lambda$ be an abelian variety of dimension g over \mathbf{C} , where Λ is a lattice, that has complex multiplication by a CM-field K and let K_0 be the real subfield of K of degree g .

2.3.1. CM-types. The field K has $2g$ embeddings in \mathbf{C} which we denote $\varphi_1, \dots, \varphi_{2g}$. An endomorphism of $\mathcal{A}_{\mathbf{C}}$ yields an endomorphism of \mathbf{C}^g and of Λ . We get an analytic representation $\rho_a : \text{End}(\mathcal{A}_{\mathbf{C}}) \rightarrow \text{End}_{\mathbf{C}}(\mathbf{C}^g)$ and a rational representation $\rho_r : \text{End}(\mathcal{A}_{\mathbf{C}}) \rightarrow \text{End}_{\mathbf{Z}}(\Lambda)$. We have $\rho_r \otimes \mathbf{C} \sim \rho_a \oplus \bar{\rho}_a$ and at the same time, $\rho_r \otimes \mathbf{C} \sim \varphi_1 \oplus \dots \oplus \varphi_{2g}$. It follows that, up to some reindexing, $\rho_a = \varphi_1 \oplus \dots \oplus \varphi_g$ where $\varphi_1, \dots, \varphi_g$ are not pairwise conjugate. We call $(K; \{\varphi_1, \dots, \varphi_g\})$ the CM-type of $\mathcal{A}_{\mathbf{C}}$. The abelian variety $\mathcal{A}_{\mathbf{C}}$ is simple if and only if its CM-type is *primitive*, which means that $(K; \Phi)$ is not a lift of a CM-type on a CM-subfield of K [ST61, §8.2].

Remark 3. If $g = 2$, the abelian surface $\mathcal{A}_{\mathbf{C}}$ is simple if and only if the field K is a primitive CM-field, i.e., K does not have any proper CM-subfield. This follows from [Str10, Lemma I.3.4].

Fix a CM-type $\Phi = \{\varphi_1, \dots, \varphi_g\}$ for K . Any abelian variety over \mathbf{C} of CM-type $(K; \Phi)$ is isomorphic to $\mathbf{C}^2/\Phi(\mathfrak{m})$ for some full-rank lattice \mathfrak{m} in K , where $\Phi : K \rightarrow \mathbf{C}^g$ is given by $x \mapsto (\varphi_1(x), \dots, \varphi_g(x))$. Let \mathcal{O} be the order of K isomorphic

to the endomorphism ring of the variety. Then, the lattice \mathfrak{m} is an \mathcal{O} -submodule of K , and \mathcal{O} coincides with the order $\mathcal{O}(\mathfrak{m})$ associated to the lattice,

$$\mathcal{O}(\mathfrak{m}) = \{\alpha \in K \mid \alpha\mathfrak{m} \subset \mathfrak{m}\}.$$

Given an ideal \mathfrak{a} in \mathcal{O} , the variety $\mathbf{C}^2/\Phi(\mathfrak{a}^{-1}\mathfrak{m})$ is isogenous to $\mathbf{C}^2/\Phi(\mathfrak{m})$, and its endomorphism ring is also \mathcal{O} . This isogenous variety is actually isomorphic if and only if \mathfrak{a} is principal. In fact, this construction induces a free action of the ideal class group $\text{Cl}(\mathcal{O})$ on the set of isomorphism classes of abelian varieties of CM-type $(K; \Phi)$ with endomorphism ring \mathcal{O} .

2.3.2. Polarizations and the Shimura class group. A polarization on an abelian variety X over a field k is an ample line bundle \mathcal{L}_X on X . Associated to such \mathcal{L}_X is the polarization isogeny $\varphi_{\mathcal{L}_X}: X \rightarrow X^\vee$, where X^\vee is the dual of X . A principal polarization is an ample line bundle of degree one (equivalently, the polarization isogeny is an isomorphism).

Example 2. If $\mathcal{A}_{\mathbf{C}}$ is a simple abelian surface, $\mathcal{A}_{\mathbf{C}}$ is principally polarizable if and only if it is the Jacobian of a genus 2 curve (see [Mil06, Prop. 3.13] and [DM02, Th. 4.1]).

In the remainder of this paragraph, we shall restrict to simple abelian varieties, or equivalently, to primitive CM-types $(K; \Phi)$. If $X = \mathcal{A}_{\mathbf{C}}$, a simple complex abelian variety with CM by an order \mathcal{O} in K , the theory of Taniyama and Shimura [ST61, §14] which we now briefly recall provides an explicit description of the polarizations on X in terms of the arithmetic of K . Indeed, by the theory of complex multiplication, there exists a full-rank lattice \mathfrak{m} in K such that $X(\mathbf{C}) \cong \mathbf{C}^2/\Phi(\mathfrak{m})$. The dual abelian variety of $\mathbf{C}^g/\Phi(\mathfrak{m})$ is $\mathbf{C}^g/\Phi(\mathfrak{m}^*)$ where $\mathfrak{m}^* = \{\beta \in K : \text{Tr}_{K/\mathbf{Q}}(\beta\bar{\mathfrak{m}}) \in \mathbf{Z}\}$. A polarization \mathcal{L} on $\mathbf{C}^g/\Phi(\mathfrak{m})$ induces an isogeny $\varphi_{\mathcal{L}}: \mathbf{C}^g/\Phi(\mathfrak{m}) \rightarrow \mathbf{C}^g/\Phi(\mathfrak{m}^*)$ that is given by $x \mapsto \rho_a(\xi)x$ for some purely imaginary element $\xi \in K$ that satisfies $\Phi(\xi) \in (i\mathbf{R}_{>0})^2$. The polarization is also described by the Riemann form $E(x, y) = \text{Tr}_{K/\mathbf{Q}}(\xi\bar{x}y)$. The polarization is principal if and only if $\varphi_{\mathcal{L}}(\Phi(\mathfrak{m})) = \Phi(\mathfrak{m}^*)$, i.e., if and only if $\xi\mathfrak{m} = \mathfrak{m}^*$. Thus, the CM-type $(K; \Phi)$ being fixed, the principally polarized abelian variety $(\mathcal{A}_{\mathbf{C}}, \mathcal{L})$ is determined by the pair (\mathfrak{m}, ξ) . The *Shimura class group* of \mathcal{O} , acts on such pairs. It is defined as

$$\mathfrak{C}(\mathcal{O}) = \{(\mathfrak{a}, \alpha) \mid \mathfrak{a} \in \mathcal{I}(\mathcal{O}) \text{ and } \mathfrak{a}\bar{\mathfrak{a}} = \alpha\mathcal{O}, \alpha \in K_0 \text{ totally positive}\} / \sim$$

with componentwise multiplication, where two pairs (\mathfrak{a}, α) and (\mathfrak{b}, β) are equivalent for the relation \sim if there exists an element $u \in K^\times$ such that $\mathfrak{b} = u\mathfrak{a}$ and $\beta = u\bar{u}\alpha$. For any $(\mathfrak{a}, \alpha) \in \mathfrak{C}(\mathcal{O})$ (up to equivalence), the pair $(\mathfrak{a}^{-1}\mathfrak{m}, \alpha\xi)$ corresponds to a principally polarized abelian variety isogenous to $\mathcal{A}_{\mathbf{C}}$ and with same endomorphism ring \mathcal{O} (up to isomorphism). This action of $\mathfrak{C}(\mathcal{O})$ is in fact free on the set of isomorphism classes of principally polarized abelian varieties isogenous to $\mathcal{A}_{\mathbf{C}}$ with same endomorphism ring [ST61, §17]. The structure of $\mathfrak{C}(\mathcal{O})$ and its relation to $\text{Cl}(\mathcal{O})$ is described by the exact sequence

$$1 \longrightarrow (\mathcal{O}_0^\times)^+ / N_{K/K_0}(\mathcal{O}^\times) \xrightarrow{u \mapsto (\mathcal{O}, u)} \mathfrak{C}(\mathcal{O}) \xrightarrow{(\mathfrak{a}, \alpha) \mapsto \mathfrak{a}} \text{Cl}(\mathcal{O}) \xrightarrow{N_{K/K_0}} \text{Cl}^+(\mathcal{O}_0),$$

where $\mathcal{O}_0 = \mathcal{O} \cap K_0$, $(\mathcal{O}_0^\times)^+$ is its subgroup of totally positive units, and $\text{Cl}^+(\mathcal{O}_0)$ its narrow class group. The image of the projection $\mathfrak{C}(\mathcal{O}) \rightarrow \text{Cl}(\mathcal{O})$, denoted $\mathcal{P}(\mathcal{O})$, is a subgroup of $\text{Cl}(\mathcal{O})$ that acts freely on the set of principally *polarizable* abelian

varieties isogenous to $\mathcal{A}_{\mathbf{C}}$ with endomorphism ring \mathcal{O} . Notice the crucial distinction between polarized and polarizable. The amount of information lost with the polarization is encoded in the group $(\mathcal{O}_0^\times)^+/N_{K/K_0}(\mathcal{O}^\times)$. For a maximal orders in quartic CM-fields, this group is either trivial, in which case $\mathfrak{C}(\mathcal{O})$ and $\mathcal{P}(\mathcal{O})$ are isomorphic and no information is lost, or it is of order two, in which case the abelian surfaces encoded in $\mathcal{P}(\mathcal{O})$ each have two possible polarizations. From the exactness of the sequence, the subgroup $\mathcal{P}(\mathcal{O})$ is also the kernel of N_{K/K_0} . The following lemma allows to extend the result of [BGL11, Th. 3.1] to higher dimensions, and non-maximal orders.

Lemma 2.1. *Let K be a CM-field and K_0 its maximal real subfield. Let \mathcal{O} be an order in K of conductor \mathfrak{f} , and $\mathcal{O}_0 = \mathcal{O} \cap K_0$. The index of the image of $\text{Cl}(\mathcal{O})$ through the norm map $N_{K/K_0} : \text{Cl}(\mathcal{O}) \rightarrow \text{Cl}^+(\mathcal{O}_0)$ is of index at most 2 in $\text{Cl}^+(\mathcal{O}_0)$. If there is a prime in K_0 that ramifies in K and does not divide \mathfrak{f} , the norm map N_{K/K_0} is surjective.*

Proof. We use the elements of class field theory recalled in Section 2.2. Let $H = H(\mathcal{O})$ and $H^+ = H^+(\mathcal{O}_0)$. The compositum KH^+ is a subfield of H , so we have a natural surjection $\text{Gal}(H/K) \rightarrow \text{Gal}(KH^+/K)$. From Galois theory, $\text{Gal}(KH^+/K)$ is isomorphic to $\text{Gal}(H^+/(K \cap H^+))$, which in turn is isomorphic to the quotient $\text{Gal}(H^+/K_0)/\text{Gal}((K \cap H^+)/K_0)$. Let $N = \text{Gal}((K \cap H^+)/K_0)$. Then,

$$\psi : \text{Gal}(H/K) \longrightarrow \text{Gal}(H^+/K_0)/N : \sigma \longmapsto \sigma|_{H^+} \pmod{N},$$

is the composition of these canonical maps, and is therefore is a surjection. Through the Artin map, the norm N_{K/K_0} commutes with ψ . We conclude that the image of $\text{Cl}(\mathcal{O})$ through N_{K/K_0} is a subgroup of $\text{Cl}^+(\mathcal{O}_0)$ of index at most $|N| \leq 2$. If there is a prime in K_0 that ramifies in K and does not divide \mathfrak{f} , then $K \cap H^+ = K_0$, so $|N| = 1$ and the map N_{K/K_0} is surjective. \square

In particular, this lemma implies that the index $[\text{Cl}(\mathcal{O}) : \mathcal{P}(\mathcal{O})]$ is either the narrow class number $h_{\mathcal{O}_0}^+ = |\text{Cl}^+(\mathcal{O}_0)|$, or $h_{\mathcal{O}_0}^+/2$. It is exactly $h_{\mathcal{O}_0}^+$ whenever there is a prime in the field K_0 that ramifies in K and does not divide \mathfrak{f} . As observed in [BGL11, Th. 3.1], there exists such a prime when \mathcal{O} is the maximal order in a primitive quartic CM-field.

2.4. Canonical lifting. Recall that our objects of primary interest are varieties defined over a finite field \mathbf{F}_q . The theory of canonical lifting of Serre and Tate [ST68] allows us to lift an ordinary abelian variety \mathcal{A}/\mathbf{F}_q to an abelian variety $\tilde{\mathcal{A}}$ over $W(\mathbf{F}_q)$, the ring of Witt vectors of \mathbf{F}_q in such a way that all endomorphisms of \mathcal{A} lift to endomorphisms of $\tilde{\mathcal{A}}$, and $\mathcal{A} \mapsto \tilde{\mathcal{A}}$ is functorial. To obtain lifts from abelian varieties over \mathbf{F}_q to abelian varieties over \mathbf{C} , we fix an embedding $\iota : W(\overline{\mathbf{F}}_q) \hookrightarrow \mathbf{C}$ and let $\mathcal{A}_{\mathbf{C}}$ be the complex abelian variety $\tilde{\mathcal{A}} \otimes_{\iota} \mathbf{C}$. If $T(\mathcal{A}) = H_1(\mathcal{A}_{\mathbf{C}}, \mathbf{Z})$ then $T(\mathcal{A})$ is a free \mathbf{Z} -module of rank $2 \cdot \dim(\mathcal{A})$. The correspondence $\mathcal{A} \mapsto T(\mathcal{A})$ is functorial and any isogeny $\varphi : \mathcal{A} \rightarrow \mathcal{B}$ over $\overline{\mathbf{F}}_q$ gives rise to a short exact sequence

$$0 \longrightarrow T(\mathcal{A}) \xrightarrow{T(\varphi)} T(\mathcal{B}) \longrightarrow \ker(\varphi) \longrightarrow 0.$$

A theorem of Deligne [Del69, Th.7] says that if π is the Frobenius endomorphism of \mathcal{A} over \mathbf{F}_q then the functor $\mathcal{A} \mapsto (T(\mathcal{A}), T(\pi))$ is an equivalence of categories between the category of ordinary abelian varieties over \mathbf{F}_q and the category of free \mathbf{Z} -modules T endowed with an endomorphism F satisfying

- (1) F is semi-simple, with eigenvalues of complex absolute value \sqrt{q} ,
- (2) At least half the roots in $\overline{\mathbf{Q}}_p$ of the characteristic polynomial of F are p -adic units,
- (3) There is an endomorphism V of T such that $FV = q$.

As discussed in [Del69, §8], any such (T, F) that is the image of a variety \mathcal{A} through this functor determines the complex abelian variety $\mathcal{A}_{\mathbf{C}}$ up to isomorphism as $\mathcal{A}_{\mathbf{C}} \cong (T \otimes \mathbf{R})/T$ (with a complex structure on $T \otimes \mathbf{R}$ such that F is \mathbf{C} -linear; the existence and uniqueness of the appropriate complex structure is established by a theorem of Serre [Del69, §8]). This means that up to isomorphism, we can write $\mathcal{A}_{\mathbf{C}} = \mathbf{C}^g/\Lambda$, for a lattice Λ in \mathbf{C}^2 and since lifting preserves the endomorphism ring $\mathcal{O} = \text{End}(\mathcal{A})$, we even have $\mathcal{A}_{\mathbf{C}} = \mathbf{C}^g/\Phi(\mathfrak{m})$ for some full-rank lattice \mathfrak{m} in K with order $\mathcal{O}(\mathfrak{m}) = \mathcal{O}$, where, as above, the map $\Phi: K \rightarrow \mathbf{C}^g$ is the CM-type of $\mathcal{A}_{\mathbf{C}}$. From the canonical identification between $\Phi(\mathfrak{m})$ and $H_1(\mathcal{A}_{\mathbf{C}}, \mathbf{Z})$ (see [BL04, §1.1]), the functor can be interpreted as $\mathcal{A} \mapsto (\Phi(\mathfrak{m}), \rho_r(\pi))$. This establishes a functorial map from the abelian varieties over \mathbf{F}_q of fixed endomorphism ring \mathcal{O} to the complex abelian varieties $\mathbf{C}^g/\Phi(\mathfrak{m})$ where \mathfrak{m} are lattices in K with order $\mathcal{O}(\mathfrak{m}) = \mathcal{O}$. Conversely, Deligne's theorem shows that any such $\mathbf{C}^g/\Phi(\mathfrak{m})$ is the lift of an abelian variety over \mathbf{F}_q with endomorphism ring \mathcal{O} : the variety corresponding to the pair $(\Phi(\mathfrak{m}), \rho_r(\pi))$, where $\rho_r(\pi)$ is the rational representation of π . Moreover, from [Del69, §3], the polarizations also lift properly, and in particular \mathcal{A} is principally polarizable if and only if $\mathcal{A}_{\mathbf{C}}$ is.

2.5. Horizontal isogeny graphs as Cayley graphs. Let π be a q -Weil number, and let $K = \mathbf{Q}(\pi)$ be the corresponding CM-field, with K_0 its maximal real subfield. Fix an order \mathcal{O} in K , and let $\mathcal{V}_{\pi, \mathcal{O}}$ be the set of all \mathbf{F}_q -isomorphism classes of abelian varieties defined over \mathbf{F}_q with endomorphism ring \mathcal{O} in the isogeny class characterised by π . Recall that the class group $\text{Cl}(\mathcal{O})$ acts freely on $\mathcal{V}_{\pi, \mathcal{O}}$. One can choose any reference variety \mathcal{A} in $\mathcal{V}_{\pi, \mathcal{O}}$ and any subgroup H in $\text{Cl}(\mathcal{O})$, and consider the orbit $H(\mathcal{A})$.

Combining the results of Deligne discussed in Section 2.4 with the theory of complex multiplication, there is an equivalence of categories between the category of objects $H(\mathcal{A})$ and morphisms the isogenies between them, and the category whose objects are the ideal classes in the subgroup H , and the sets of morphisms from $a \in H$ to $b \in H$ are the ideals of \mathcal{O} in the class $a^{-1}b$. The degree of an isogeny equals the norm of the corresponding ideal. Restricting the morphisms to a finite set of generators, the latter category can be seen as a Cayley (multi)graph.

Definition 2.2 (Cayley graph). Let G be a finite group and S a generating subset of G , with $S = S^{-1}$. The *Cayley graph* $\text{Cay}(G, S)$ is the finite $|S|$ -regular undirected graph with set of vertices G , and an edge between g and sg for any $g \in G$ and $s \in S$.

Remark 4. The edges of $\text{Cay}(G, S)$ can have multiplicities if S is a multiset. If S is a set of labels and $f: S \rightarrow S$ is a surjection, then f naturally induces a Cayley multigraph for the set of generators S whose edges are labelled by elements of S .

Let \mathcal{S} be a set of ideals of \mathcal{O} , and S its image in Cl_K , with $f: \mathcal{S} \rightarrow S$ the induced surjection. Let $\text{Cay}(H, S \cap H)$ be the induced labelled multigraph. Let T be the set of all isogenies between elements of $H(\mathcal{A})$ corresponding to the ideals of \mathcal{S} . We build the graph $\mathcal{G}_{\mathcal{S}}$ with set of vertices $H(\mathcal{A})$ by adding an edge between the vertices \mathcal{B} and \mathcal{C} for any isogeny $\mathcal{B} \rightarrow \mathcal{C}$ in T . Then, the equivalence of categories induces an isomorphism between the graphs $\mathcal{G}_{\mathcal{S}}$ and $\text{Cay}(H, S \cap H)$.

Example 3. If \mathcal{A} is a principally polarizable abelian variety and $H = \mathcal{P}(\mathcal{O})$, the orbit $H(\mathcal{A})$ (in this case also denoted $\mathcal{P}(\mathcal{A})$) is a set of isomorphism classes of principally polarizable abelian varieties isogenous to \mathcal{A} and with same endomorphism ring. Via the construction described above, any choice of a generating set of $\mathcal{P}(\mathcal{O})$ yields a graph of the set of vertices $\mathcal{P}(\mathcal{A})$. From [Wat69, Theorem 5.3] together with [Bla14, Theorem 4.5], the action of $\mathrm{Cl}(\mathcal{O})$ is transitive on the set of *all* abelian varieties isogenous to \mathcal{A} and with same endomorphism ring whenever \mathcal{A} has maximal real multiplication (i.e., $\mathcal{O}_{K_0} \subset \mathcal{O}$). We can conclude via [ST61, §17] that when \mathcal{A} has maximal real multiplication, the orbit $\mathcal{P}(\mathcal{A})$ is exactly the set of all isomorphism classes of principally polarizable abelian varieties isogenous to \mathcal{A} and with same endomorphism ring.

3. EXPANDER GRAPHS AND RAY CLASS GROUPS

In this section, we prove Theorem 1.2, and investigate its consequences on the structure of the Cayley graphs of interest.

3.1. Eigenvalues and Cayley graphs. Let \mathcal{G} be an undirected (multi)graph with set of vertices \mathcal{V} and set of edges \mathcal{E} . Suppose \mathcal{G} is finite and k -regular, i.e., each vertex has k incident edges. The *adjacency operator* A of \mathcal{G} is the operator defined for any function f from \mathcal{V} to \mathbf{C} by

$$Af(x) = \sum_{y \in \mathcal{N}_{\mathcal{G}}(x)} f(y),$$

for any $x \in \mathcal{V}$, where $\mathcal{N}_{\mathcal{G}}(x)$ denotes the (multi)set of neighbors of x in \mathcal{G} . This operator is represented by the adjacency matrix of \mathcal{G} with respect to the basis $\{\mathbf{1}_{\{x\}} : x \in \mathcal{V}\}$, where $\mathbf{1}_S$ denotes the characteristic function of a set S . It is a real symmetric matrix, so by the spectral theorem, A has $n = |\mathcal{V}|$ real eigenvalues $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n$. Since the graph is k -regular, the constant function $\mathbf{1}_{\mathcal{V}} : x \mapsto 1$ is an eigenvector with eigenvalue k . We call k the *trivial eigenvalue*, and denote it by λ_{triv} . This λ_{triv} is the largest eigenvalue in absolute value, i.e., $\lambda_1 = k$, and its multiplicity is the number of connected components of \mathcal{G} .

Definition 3.1 (Expander graph). Let $\delta > 0$. The k -regular graph \mathcal{G} is (*one-sided*) δ -*expander* if $\lambda_2 \leq (1 - \delta)\lambda_{\mathrm{triv}}$. It is a *two-sided* δ -*expander* if the stronger bound $|\lambda_2| \leq (1 - \delta)\lambda_{\mathrm{triv}}$ holds.

Observe that such a graph is connected whenever $\delta > 0$. The main reason for our interest in expander graphs is that they rapidly mix random walks. The following lemma is a classical result on expander graphs and can be found in, e.g., [JMV09].

Lemma 3.2. *Let \mathcal{G} be a finite k -regular graph for which the non-trivial eigenvalues λ of the adjacency operator A satisfy the bound $|\lambda| \leq c$, for some $c < k$. Let S be a subset of the vertices of \mathcal{G} , and v a vertex of \mathcal{G} . Any random walk from v of length at least $\frac{\ln(2|\mathcal{G}|/|S|^{1/2})}{\ln(k/c)}$ will end in S with probability between $\frac{1}{2} \frac{|S|}{|\mathcal{G}|}$ and $\frac{3}{2} \frac{|S|}{|\mathcal{G}|}$.*

For any finite group G with generating set S , observe that a character $\chi : G \rightarrow \mathbf{C}^*$ is an eigenvector for the adjacency operator A on $\mathrm{Cay}(G, S)$. Indeed,

$$A\chi(x) = \sum_{s \in S} \chi(sx) = \sum_{s \in S} \chi(s)\chi(x) = \lambda_{\chi}\chi(x), \text{ where } \lambda_{\chi} = \sum_{s \in S} \chi(s).$$

If G is abelian, these characters form a basis of the \mathbf{C} -vector space of functions of G . In particular, any eigenvalue is of the form λ_χ for some character χ . The trivial eigenvalue corresponds to the trivial character $\mathbf{1}_G$.

3.2. Proof of Theorem 1.2. Since G is abelian, any character χ of H can be extended to a character of G . Take any such extension and, by abuse of notation, also denote it by χ . Note that for any ideal \mathfrak{l} of \mathcal{O}_K coprime to \mathfrak{m} , we have

$$\sum_{\theta \in \widehat{G/H}} \theta([\mathfrak{l}]H) = \begin{cases} [G : H] & \text{if } [\mathfrak{l}] \in H, \\ 0 & \text{otherwise,} \end{cases}$$

where $\widehat{G/H} = \text{Hom}(G/H, \mathbf{C}^*)$ is the character group of the quotient G/H . Therefore this sum can be used to filter the condition that $[\mathfrak{l}] \in H$, and we can rewrite

$$\begin{aligned} \lambda_\chi &= \sum_{\mathfrak{l} \in \mathcal{T}_{H, \mathfrak{m}}(B)} \chi([\mathfrak{l}]) = \frac{1}{[G : H]} \sum_{\substack{\mathfrak{l}: N\mathfrak{l} < B \\ (\mathfrak{l}, \mathfrak{m})=1}} \chi([\mathfrak{l}]) \sum_{\theta \in \widehat{G/H}} \theta([\mathfrak{l}]H) \\ &= \frac{1}{[G : H]} \sum_{\theta \in \widehat{G/H}} \sum_{\substack{\mathfrak{l}: N\mathfrak{l} < B \\ (\mathfrak{l}, \mathfrak{m})=1}} \chi([\mathfrak{l}]) \theta([\mathfrak{l}]H). \end{aligned}$$

We are then left with estimating a character sum $\sum \chi([\mathfrak{l}]) \theta([\mathfrak{l}]H)$. Each of the summands of the latter defines a multiplicative function

$$\nu_{\chi, \theta}: \mathcal{I}_{\mathfrak{m}}(K) \longrightarrow \mathbf{C}^* : \mathfrak{l} \longmapsto \chi([\mathfrak{l}]) \theta([\mathfrak{l}]H)$$

where $\mathcal{I}_{\mathfrak{m}}(K)$ is the group of fractional ideals of K coprime to \mathfrak{m} . It extends to a function of $\mathcal{I}(K)$, the group of all the fractional ideals of K , by setting $\nu_{\chi, \theta}(\mathfrak{l}) = 0$ for all prime divisors \mathfrak{l} of \mathfrak{m} . The expression of λ_χ becomes

$$(3.1) \quad \lambda_\chi = \frac{1}{[G : H]} \sum_{\theta \in \widehat{G/H}} \sum_{\mathfrak{l}: N\mathfrak{l} < B} \nu_{\chi, \theta}(\mathfrak{l}).$$

From the classical estimate that can be found in [IK04, Th.5.15], we have

$$\sum_{\mathfrak{a}: N\mathfrak{a} < B} \Lambda(\mathfrak{a}) \nu_{\chi, \theta}(\mathfrak{a}) = \delta(\nu_{\chi, \theta}) B + O\left(n B^{1/2} \ln(B) \ln(B d_K N \mathfrak{m})\right),$$

where Λ is the von Mangoldt function (i.e., $\Lambda(\mathfrak{a})$ is $\ln N\mathfrak{l}$ if \mathfrak{a} is a power of a prime ideal \mathfrak{l} , and 0 otherwise), and $\delta(\nu_{\chi, \theta})$ is 1 if $\nu_{\chi, \theta}$ is principal, and 0 otherwise (a principal character is a character that only takes the values 1 or 0). Observe that if $\nu_{\chi, \theta}$ is principal, then χ must be the trivial character, so that $\delta(\nu_{\chi, \theta}) = \delta(\chi) \delta(\theta)$. Indeed, suppose that $\nu_{\chi, \theta}$ is principal, and let $[\mathfrak{l}] \in H$, for a prime \mathfrak{l} coprime to \mathfrak{m} . Then,

$$1 = \nu_{\chi, \theta}(\mathfrak{l}) = \chi([\mathfrak{l}]) \theta([\mathfrak{l}]H) = \chi([\mathfrak{l}]) \theta(\mathbf{1}_{G/H}) = \chi([\mathfrak{l}]),$$

so χ must be the trivial character of H .

We now want to replace each instance of $\Lambda(\mathfrak{a})$ in the above sum by $P(\mathfrak{a})$, where

$$P(\mathfrak{a}) = \begin{cases} \ln N\mathfrak{a} & \text{if } N\mathfrak{a} \text{ is prime,} \\ 0 & \text{otherwise.} \end{cases}$$

To do so, it is sufficient to prove that

$$(3.2) \quad \sum_{\mathfrak{a}: N\mathfrak{a} < B} \Lambda(\mathfrak{a})\nu_{\chi, \theta}(\mathfrak{a}) - \sum_{\mathfrak{a}: N\mathfrak{a} < B} P(\mathfrak{a})\nu_{\chi, \theta}(\mathfrak{a}) = O\left(nB^{1/2}\right).$$

The non-zero terms $(\Lambda(\mathfrak{a}) - P(\mathfrak{a}))\nu_{\chi, \theta}(\mathfrak{a})$ correspond to ideals \mathfrak{a} which are powers of a prime ideal \mathfrak{l} , and $N\mathfrak{a} = N\mathfrak{l}^k$ is not a prime number – but it is a power of a prime ℓ . Since K is of degree n , there are at most n different prime ideals \mathfrak{l} above any given prime number ℓ . Therefore the difference (3.2) is bounded in absolute value by

$$n \sum_{\substack{\ell^k < B \\ k \geq 2}} \ln \ell = n \sum_{\substack{\ell < B^{1/2} \\ 2 \leq k < \frac{\ln B}{\ln \ell}}} \ln \ell \leq n \sum_{\ell < B^{1/2}} \ln \ell \frac{\ln B}{\ln \ell} = n\pi(B^{1/2}) \ln B,$$

which, by the Prime Number Theorem, is $O(nB^{1/2})$. Therefore,

$$\sum_{\mathfrak{a}: N\mathfrak{a} < B} P(\mathfrak{a})\nu_{\chi, \theta}(\mathfrak{a}) = \delta(\nu_{\chi, \theta})B + O\left(nB^{1/2} \ln(B) \ln(Bd_K N\mathfrak{m})\right).$$

Applying the Abel partial summation formula, we derive that

$$\sum_{\mathfrak{l}: N\mathfrak{l} < B \text{ prime}} \nu_{\chi, \theta}(\mathfrak{l}) = \delta(\nu_{\chi, \theta})\text{li}(B) + O\left(nB^{1/2} \ln(Bd_K N\mathfrak{m})\right),$$

where li denotes the logarithmic integral. Replacing this into the expression (3.1) of λ_χ , we finally obtain

$$\lambda_\chi = \frac{\delta(\chi)}{[G : H]} \text{li}(B) + O\left(nB^{1/2} \ln(Bd_K N\mathfrak{m})\right),$$

which proves the theorem. \square

3.3. Spectral gaps for subgroups of ideal class groups. Let K be any number field of degree n , \mathcal{O} an order of conductor \mathfrak{f} in K , and H any subgroup of $\text{Cl}(\mathcal{O})$. Let $B > 0$, \mathfrak{m} an integral ideal of \mathcal{O}_K , and define the following set of ideals of \mathcal{O}_K ,

$$S_B = \{\mathfrak{l} \mid N\mathfrak{l} < B \text{ is prime, } (\mathfrak{l}, \mathfrak{f}\mathfrak{m}) = 1, \text{ and } [\mathfrak{l} \cap \mathcal{O}] \in H\},$$

where $[\mathfrak{l} \cap \mathcal{O}]$ is the class in $\text{Cl}(\mathcal{O})$. Let S_B be the multiset of its image in the class group. Using Theorem 1.2, one can bound the spectral gap of $\mathcal{G}_B = \text{Cay}(H, S_B)$.

Theorem 3.3. *For any character χ of H , the corresponding eigenvalue of \mathcal{G}_B is*

$$\lambda_\chi = \frac{\delta(\chi)}{[\text{Cl}(\mathcal{O}) : H]} \text{li}(B) + O(nB^{1/2} \ln(Bd_K N(\mathfrak{f}\mathfrak{m}))),$$

where $\delta(\chi)$ is 1 if χ is trivial, and 0 otherwise.

Proof. Using the notations from Section 2.2, the group $P_{K,1}^{\mathfrak{f}}$ is a subgroup of $P_{K,\mathcal{O}}^{\mathfrak{f}}$, so there is a natural surjection $\text{Cl}_{\mathfrak{f}}(K) \rightarrow \text{Cl}(\mathcal{O})$. Furthermore, the canonical injection of $\mathcal{S}_{\mathfrak{f}\mathfrak{m}}(K)$ in $\mathcal{S}_{\mathfrak{f}}(K)$ induces a surjection from $\text{Cl}_{\mathfrak{f}\mathfrak{m}}(K)$ to $\text{Cl}_{\mathfrak{f}}(K)$. Therefore we have a natural surjection $\pi : \text{Cl}_{\mathfrak{f}\mathfrak{m}}(K) \rightarrow \text{Cl}(\mathcal{O})$, which sends the class of any integral ideal \mathfrak{a} of \mathcal{O}_K to the class of $\mathfrak{a} \cap \mathcal{O}$. Consider the subgroup $\tilde{H} = \pi^{-1}(H)$ of $\text{Cl}_{\mathfrak{f}\mathfrak{m}}(K)$, and its Cayley graph $\tilde{\mathcal{G}}_B = \text{Cay}(\tilde{H}, T_{\tilde{H}, \mathfrak{f}\mathfrak{m}}(B))$ where $T_{\tilde{H}, \mathfrak{f}\mathfrak{m}}(B)$ is the multiset defined in the statement of Theorem 1.2. The Cayley graph \mathcal{G}_B on H is the image of the Cayley graph $\tilde{\mathcal{G}}_B$ on \tilde{H} via the projection π , taking into account the multiplicity of the edges. The eigenvalues of \mathcal{G}_B are exactly the eigenvalues λ_θ of $\tilde{\mathcal{G}}_B$

corresponding to characters θ of \tilde{H} that are trivial on the kernel of $\pi|_{\tilde{H}} : \tilde{H} \rightarrow H$. The result follows by applying Theorem 1.2 on $\tilde{\mathcal{G}}_B$. \square

Corollary 3.4. *For any $0 < \delta < 1$ and $\varepsilon > 0$, there is a function*

$$B_{\delta,\varepsilon}(H, \mathfrak{m}) = O\left((n[\text{Cl}(\mathcal{O}) : H] \ln(d_K N(\mathfrak{m})))^{2+\varepsilon}\right),$$

such that $\mathcal{G}_{B_{\delta,\varepsilon}(H, \mathfrak{m})}$ is a two-sided δ -expander.

Proof. Let $x > 0$, and write $k = [\text{Cl}(\mathcal{O}) : H]$. The graph \mathcal{G}_x is a two-sided δ -expander if $|\lambda_\chi| \leq (1 - \delta)\lambda_{\text{triv}}$ for any non-trivial character χ . From Theorem 3.3, and the fact that $\text{li}(x) \sim x/\ln(x)$ and $\text{li}(x) \geq x/\ln(x)$ for any $x \geq 4$, there are absolute constants C and D such that for any $x \geq C$, we have

$$\lambda_{\text{triv}} \geq \frac{x}{\ln(x)k} - Dnx^{1/2} \ln(xd_K N(\mathfrak{m})),$$

and $|\lambda| \leq Dnx^{1/2} \ln(xd_K N(\mathfrak{m}))$. So

$$\frac{\lambda_{\text{triv}}}{|\lambda|} \geq \frac{2x^{1/2}}{\ln^2(x)Dkn(\ln(d_K N(\mathfrak{m})) + 1)} - 1.$$

We have that $x^{1/(2+\varepsilon)} = O(x^{1/2}/\ln^2(x))$ for any $\varepsilon > 0$, so considering larger constants C and D if necessary, we have the inequality

$$\frac{\lambda_{\text{triv}}}{|\lambda|} \geq \frac{2x^{1/(2+\varepsilon)}}{Dkn(\ln(d_K N(\mathfrak{m})) + 1)} - 1.$$

The constants C and D are not absolute anymore but they only depend on ε . Let

$$B_{\delta,\varepsilon}(H, \mathfrak{m}) = \max\left(C, \left(\frac{1}{2} \left(\frac{1}{1-\delta} + 1\right) (Dkn(\ln(d_K N(\mathfrak{m})) + 1))\right)^{2+\varepsilon}\right).$$

Then, for $x = B_{\delta,\varepsilon}(H, \mathfrak{m})$, we have $\frac{\lambda_{\text{triv}}}{|\lambda|} \geq \frac{1}{1-\delta}$, so \mathcal{G}_x is δ -expander. \square

3.4. Proof of Theorem 1.1. Theorem 1.1 is now an easy combination of the graph isomorphism expounded in Section 2.5, together with Corollary 3.4 establishing that these graphs are expanders, and Lemma 3.2 on random walks on such graphs.

4. RANDOM WALKS ON ISOGENY GRAPHS OF JACOBIANS IN GENUS 2

Throughout this section, we will restrict to ordinary abelian surfaces that are Jacobians of genus 2 hyperelliptic curves over a finite field \mathbf{F}_q . Let $\mathcal{J} = \text{Jac}(\mathcal{C})$ be such a Jacobian with endomorphism algebra K and whose endomorphism ring is isomorphic to an order \mathcal{O} in K . Let $\mathcal{O}_0 = \mathcal{O} \cap K_0$ where K_0 is the real subfield of K . Let \mathcal{A} be the isomorphism class of \mathcal{J} as an abelian variety.

Consider the orbit $\mathcal{P}(\mathcal{A})$ of the action of $\mathcal{P}(\mathcal{O})$ on \mathcal{A} . The choice of any set of ideals generating $\mathcal{P}(\mathcal{O})$ yields an isogeny graph on the set of vertices $\mathcal{P}(\mathcal{A})$, as described in Example 3. Now, Theorem 1.1 provides generating sets \mathcal{S} with very convenient properties: (i) the corresponding isogeny graph rapidly mixes random walks, and (ii) every edge is an isogeny of small prime degree. In fact, all the occurring isogenies are computable in polynomial time by a recent algorithm of Dudeanu, Jetchev and Robert [DJR14, Dud16] (henceforth, the DJR algorithm).

4.1. Computing isogenies of small degree. More precisely, the DJR algorithm allows to compute any isogeny from \mathcal{J} , defined over \mathbf{F}_q and of odd prime degree ℓ (i.e., given a generator of the kernel, it finds an equation of a hyperelliptic curve \mathcal{C}' such that the target Jacobian is isomorphic to $\text{Jac}(\mathcal{C}')$) under the following conditions:

- (1) \mathcal{J} has maximal real multiplication, i.e., \mathcal{O}_0 is the maximal order of K_0 ,
- (2) the index $[\mathcal{O} : \mathbf{Z}[\pi, \bar{\pi}]$ is prime to 2ℓ , and
- (3) there exists a totally positive element $\beta \in \mathcal{O}_0$ of norm ℓ which annihilates the kernel of the isogeny (the isogeny is called β -cyclic, and the polarisation computed on the target curve depends on the choice of this β).

The cost of the algorithm is $O(\ell^2)$ operations in \mathbf{F}_q , assuming some precomputations of polynomial time in $\log q$ and ℓ (see [Dud16, Th. 4.8.2]).

Observe that Condition (3) exactly means that the isogeny corresponds to an ideal in the kernel $\mathcal{P}(\mathcal{O})$ of the map $N_{K/K_0} : \text{Cl}(\mathcal{O}) \rightarrow \text{Cl}^+(\mathcal{O}_0)$. Therefore this condition is, by construction, satisfied by all the isogenies of the graph. Also, we can choose the generating set \mathcal{S} so that it does not contain any ideal of norm dividing the index $[\mathcal{O} : \mathbf{Z}[\pi, \bar{\pi}]$, so the isogenies of the graph all satisfy Condition (2) if and only if $[\mathcal{O} : \mathbf{Z}[\pi, \bar{\pi}]$ is odd. Therefore, the conditions

- (1) \mathcal{J} has maximal real multiplication, and
- (2) the index $[\mathcal{O} : \mathbf{Z}[\pi, \bar{\pi}]$ is prime to 2,

are sufficient for constructing a graph whose edges can all be computed by the DJR algorithm. Before the work of Dudeanu, Jetchev and Robert, one was only able to compute (ℓ, ℓ) -isogenies [CR11] that were not sufficient to obtain a connected graph.

For the same computational cost, the DJR algorithm can compute the image of a point of order coprime to $2q$ $[\mathcal{O} : \mathbf{Z}[\pi, \bar{\pi}]$, given some additional precomputations of polynomial cost in $\text{Disc}(K_0)$.

4.2. Navigating in the graph with polarizations. The vertices of the graph represent principally *polarizable* (as opposed to *polarized*) abelian surfaces. As a consequence, two distinct Jacobians can represent the same vertex if they are isomorphic as abelian varieties, but have non-isomorphic polarizations. For computations, it is important to be able to determine whether two vertices of the graph are distinct or not, and to this end, the way the vertices are represented is crucial.

As explained in [CR11] and [DJR14], it is possible to distinguish between isomorphism classes of Jacobians as principally polarized abelian varieties by simply comparing the Rosenhain invariants². The DJR algorithm computes these explicitly for the target curve of an isogeny. Therefore, if $(\mathcal{O}_{K_0}^\times)^+ / N_{K/K_0}(\mathcal{O}_K^\times)$ is trivial, as discussed in Section 2.3.2, the map $\mathfrak{C}(\mathcal{O}) \rightarrow \mathcal{P}(\mathcal{O})$ forgetting the polarization is an isomorphism so the vertices of the graph can simply be represented as Jacobians, or their Rosenhain invariants.

But if $(\mathcal{O}_{K_0}^\times)^+ / N_{K/K_0}(\mathcal{O}_K^\times)$ is of order 2, more work is required. In this case, for any Jacobian \mathcal{J}_1 , there exists another Jacobian \mathcal{J}_2 which is isomorphic as a non-polarized abelian variety (and thus represents the same vertex in the graph), but not as a *principally polarized* abelian variety. To solve this issue, one can simply represent the vertices of the graph as pairs of Jacobians, isomorphic as

²Since the varieties are absolutely simple, ordinary, and over \mathbf{F}_q , two of them are \mathbf{F}_q -isomorphic if and only if they are $\bar{\mathbf{F}}_q$ -isomorphic (a consequence of [Wat69, Th. 7.2]; see [BJW16, Rem. 3.3]).

abelian varieties, but with non-isomorphic polarizations. It is still possible to use the DJR algorithm to navigate in this graph. Indeed, let $u \in (\mathcal{O}_{K_0}^\times)^+$ be a generator of $(\mathcal{O}_{K_0}^\times)^+/N_{K/K_0}(\mathcal{O}_K^\times)$. Starting from \mathcal{J} , given an appropriate kernel, the DJR algorithm chooses a β and computes the isogeny as a β -isogeny, resulting in a target Jacobian \mathcal{J}_1 . If β is replaced by $u\beta$, the DJR algorithm finds the Jacobian \mathcal{J}_2 which is isomorphic to \mathcal{J}_1 as an abelian variety, but with a different polarization. Therefore the representation of the vertex $\{\mathcal{J}_1, \mathcal{J}_2\}$ can be fully computed.

A last point must be addressed: given a Jacobian \mathcal{J} and a prime ℓ , the DJR algorithm allows to find isogenies of degree ℓ from that Jacobian, but it is unclear a priori which of these isogenies remain within the graph we constructed. Indeed, it could well be that some of these isogenies change the endomorphism order \mathcal{O} . Luckily, this is not a concern if only primes ℓ that cannot change the endomorphism order are picked. An isogeny over \mathbf{F}_q of degree ℓ can change the order only if ℓ divides the index $[\mathcal{O}_K : \mathbf{Z}[\pi, \bar{\pi}]]$ (see [BJW16, Prop. 3.4]). Therefore, in the generating set \mathcal{S} , we avoid the prime ideals dividing that index.

4.3. Proof of Theorem 1.3. Let $\mathcal{W} \subset \mathcal{V}$ be the subset of all isomorphism classes for which the algorithm \mathcal{A} solves the DLP. For any two polarised abelian varieties \mathcal{A} and \mathcal{B} , write $\mathcal{A} \sim \mathcal{B}$ if they are isomorphic as non-polarized abelian varieties. Recall that as discussed in Section 4.2, if \mathcal{A} can solve the DLP on one Jacobian $\mathcal{J} \in \mathcal{W}$, then it can solve the DLP on the other Jacobians $\mathcal{J}' \sim \mathcal{J}$. Let $V = \mathcal{V}/\sim$ and $W = \mathcal{W}/\sim$. Let π be a q -Weil number characterising the fixed isogeny class. From Example 3, the set V is naturally in bijection with $\mathcal{P}(\mathcal{A})$, the orbit for the CM-action of $\mathcal{P}(\mathcal{O})$. We can therefore apply Theorem 1.1 on the graph with set of vertices V induced by the set of invertible ideals in \mathcal{O} , coprime to $2[\mathcal{O}_K : \mathbf{Z}[\pi, \bar{\pi}]]$, of prime norm bounded by

$$B_\varepsilon(\mathcal{O}) = O\left(\left(h_{\mathcal{O}_0}^+ \ln(d_K N\mathfrak{f}[\mathcal{O}_K : \mathbf{Z}[\pi, \bar{\pi}]])\right)^{2+\varepsilon}\right) = O\left(\left(h_{\mathcal{O}_0}^+ \log q\right)^{2+\varepsilon}\right),$$

where \mathfrak{f} is the conductor of \mathcal{O} . Any path of length at least $\ln(2|V|/|W|^{1/2}) \leq \ln(2h_{\mathcal{O}})$ starting from any vertex will end in W with probability between $\mu/2$ and $3\mu/2$. So the strategy to solve DLP on $\mathcal{A} \in V$ is to build random paths from \mathcal{A} in $\mathcal{G}_{\mathcal{B}}$ of length $\ln(2h_{\mathcal{O}})$ until one of them ends in W , which happens with probability higher than $\mu/2$, so after an expected number of independent trials smaller than $2/\mu$. The length of each path is polynomial in $\ln(h_{\mathcal{O}})$, and the degree of each isogeny on the path is bounded by $B_\varepsilon(\mathcal{O})$. So the algorithm computes a polynomial (in $\log q$) number of isogenies, and each of them can be computed in polynomial time (in $\log q$, $h_{\mathcal{O}_0}^+$ and $\text{Disc}(K_0)$) by the DJR algorithm [DJR14, Dud16].

5. COMPUTING AN EXPLICIT ISOGENY BETWEEN TWO GIVEN JACOBIANS

Let \mathcal{C} and \mathcal{C}' be two hyperelliptic curves of genus 2, defined over the finite field \mathbf{F}_q . Let $\mathcal{A} = \text{Jac}(\mathcal{C})$ and $\mathcal{B} = \text{Jac}(\mathcal{C}')$ be their Jacobians. These are principally polarized abelian varieties of dimension 2, so by Tate's isogeny theorem [Tat66], \mathcal{A} and \mathcal{B} are isogenous over \mathbf{F}_q if and only if their Frobenius polynomials are the same. We know how to compute the latter (see [Pil90], or [GH00] for an efficient algorithm whose running time is $O((\log q)^9)$), and thereby decide whether or not there is an isogeny $\mathcal{A} \rightarrow \mathcal{B}$ defined over \mathbf{F}_q . Yet, once we know that \mathcal{A} and \mathcal{B} are isogenous, it is not clear how to explicitly compute an isogeny between them. In this section, the expander properties of horizontal isogeny graphs are used

to construct and analyse an algorithm similar to Galbraith’s algorithm [Gal99] to build an isogeny between two such varieties having the same endomorphism ring. The contribution of this new algorithm is two-fold. First, the analysis of Galbraith’s algorithm relies, in addition to GRH, on some heuristic assumptions on the growing rate of some trees built in the isogeny graph. Using expander properties of these graphs, our analysis relies solely on GRH. Second, while Galbraith’s algorithm constructs isogenies between elliptic curves, we provide a more general framework for large families of horizontal isogeny graphs. Precisely, we require

- (1) An order \mathcal{O} of conductor \mathfrak{f} in a CM-field K , and two isogenous abelian varieties \mathcal{A} and \mathcal{B} over a finite field \mathbf{F}_q with endomorphism ring \mathcal{O} ;
- (2) A set \mathcal{S} of ideals in \mathcal{O} generating a subgroup H of the class group $\text{Cl}(\mathcal{O})$, such that the orbits $H(\mathcal{A})$ and $H(\mathcal{B})$ coincide;
- (3) The isogeny graph \mathcal{G} induced by the action of H on $H(\mathcal{A})$ has the rapid mixing property, as described in Theorem 1.1;
- (4) The isogenies corresponding to the edges of the graph can be computed in time bounded by some $t_H > 0$.

For elliptic curves, one can choose $H = \text{Cl}(\mathcal{O})$, and \mathcal{S} the set of all ideals of prime norm bounded by a bound $B = O(\log(d_K N\mathfrak{f})^{2+\varepsilon}) = O((\log q)^{2+\varepsilon})$. All these isogenies can be computed in time t_H polynomial in $\log q$, and Theorem 1.1, or even the less general results of [JMV05, JMV09], shows that \mathcal{G} has the rapid mixing property. The smaller bound $O(\log(d_K N\mathfrak{f})^2)$ was used in Galbraith’s approach; the induced graph is then connected, but is not an expander, therefore some additional heuristic assumptions were required for the analysis.

For Jacobians of genus 2 curves, one can choose $H = \mathcal{P}(\mathcal{O})$, and \mathcal{S} to be a generating set of ideals of prime norms bounded by a bound $B = O((h_{\mathcal{O}_0}^+ \log q)^{2+\varepsilon})$, where $\mathcal{O}_0 = \mathcal{O} \cap K_0$. As seen in Section 4.1, the corresponding isogenies can then be computed using the DJR algorithm when \mathcal{O}_0 is maximal and $[\mathcal{O} : \mathbf{Z}[\pi, \bar{\pi}]]$ is odd.

Write $h = |H|$. The idea is to find $h^{1/2}$ varieties “close” to \mathcal{A} (in the sense that we know a path of polynomial length from these to \mathcal{A}), and then to build paths out of \mathcal{B} until one of the neighbors of \mathcal{A} is reached. In practice one could simply use the same tree-growing strategy as Galbraith [Gal99], but the analysis of our algorithm requires the various random paths to be independent in order to use the expanding properties (and this independence misses in the “tree” approach). The algorithm goes as follows, presented in the most general setting.

- Step 1** Build independent random paths in \mathcal{G} of length $\ln(2h)$ from \mathcal{A} until $h^{1/2}$ vertices are reached. Those are the *neighbors* of \mathcal{A} .
- Step 2** Build independent random paths of length $\ln(2h)$ from \mathcal{B} until a neighbor of \mathcal{A} is reached. There is now a short path between \mathcal{A} and \mathcal{B} .

Now, let us prove that the number of paths considered at each step is on average $O(h^{1/2})$. Let Y be a subset of the vertices of \mathcal{G} , smaller than $2h/3$. By a *trial*, we mean the computation of a random path of length $\ln(2h)$ from A , and a trial is a *success* if the path ends out of Y . Let us estimate the number N_Y of independent trials we need to obtain a success,

$$\mathbf{E}[N_Y] = \sum_{i=1}^{\infty} i \Pr[i - 1 \text{ failures and } 1 \text{ success}] \leq \sum_{i=1}^{\infty} i \left(\frac{3|Y|}{2h} \right)^{i-1},$$

and from the generating function $(1-x)^{-2} = \sum_{i=0}^{\infty} (i+1)x^i$, we obtain the inequality

$$\mathbf{E}[N_Y] \leq \left(1 - \frac{3|Y|}{2h}\right)^{-2} = \frac{4h^2}{(2h - 3|Y|)^2}.$$

Now consider the experiment consisting in a sequence of independent trials, and let Y_n be the first n distinct points obtained from the first experiments. The number M_n of trials required to find n distinct points can be estimated as

$$\mathbf{E}[M_n] = \sum_{i=1}^{n-1} \mathbf{E}[N_{Y_i}] \leq \sum_{i=1}^{n-1} \frac{4h^2}{(2h - 3i)^2} \leq \frac{4nh^2}{(2h - 3n)^2}.$$

In particular, to find $h^{1/2}$ neighbors of \mathcal{A} , the expected number of trials $\mathbf{E}[M_{h^{1/2}}]$ is at most $4h^{1/2}$, assuming that h is at least 9. Of course, in practice, we expect to need much less trials since we count here only the end point of each path. This proves that the expected number of paths we have to compute in Step 1 is $O(h^{1/2})$.

The expected number of paths considered in Step 2 can be found to be $O(h^{1/2})$ in a similar fashion. In total, we build $O(h^{1/2})$ paths of length $O(\ln h)$. So the algorithm needs to compute $O(h^{1/2} \ln h)$ isogenies, each of them being computable in time t_H , and finds a path of length $O(\ln h)$ between \mathcal{A} and \mathcal{B} .

ACKNOWLEDGEMENTS

We thank Emmanuel Kowalski, Philippe Michel, Ken Ribet and Damien Robert for useful conversations. The first author was supported by the Swiss National Science Foundation. The second author was supported by the Swiss National Science Foundation under grant number 200021-156420.

REFERENCES

- [Bac90] E. Bach, *Explicit bounds for primality testing and related problems*, Mathematics of Computation **55** (1990), no. 191, 355–380. MR 91m:11096
- [BCHL16] J. W. Bos, C. Costello, H. Hisil, and K. Lauter, *Fast cryptography in genus 2*, Journal of Cryptology **29** (2016), no. 1, 28–60.
- [BGL11] R. Bröker, D. Gruenewald, and K. Lauter, *Explicit CM theory for level 2-structures on abelian surfaces*, Algebra & Number Theory, **5–4** (2011), 495–528.
- [BJW16] E. H. Brooks, D. Jetchev, and B. Wesolowski, *Isogeny graphs of ordinary abelian varieties*, arXiv [abs/1609.09793](https://arxiv.org/abs/1609.09793) (2016).
- [BL04] C. Birkenhake and H. Lange, *Complex abelian varieties*, Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen, Springer, 2004.
- [Bla14] C. Blake, *A deuring criterion for abelian varieties*, Bulletin of the London Mathematical Society (2014), bdu079.
- [CR11] R. Cosset and D. Robert, *Computing (ℓ, ℓ) -isogenies in polynomial time on Jacobians of genus 2 curves*, preprint (2011).
- [Del69] P. Deligne, *Variétés abéliennes ordinaires sur un corps fini*, Invent. Math., vol. 8, Springer Berlin Heidelberg, 1969, pp. 238–243.
- [DJR14] A. Dudeanu, D. Jetchev, and D. Robert, *Computing cyclic isogenies in genus 2*, preprint (2014).
- [DM02] E. Nart D. Maisner, *Abelian surfaces over finite fields as jacobians*, Experiment. Math. **11** (2002), 321337.
- [Dud16] A. Dudeanu, *Computational aspects of jacobians of hyperelliptic curves*, Ph.D. thesis, EPFL, 2016.
- [Gal99] S. Galbraith, *Constructing isogenies between elliptic curves over finite fields*, LMS Journal of Computation and Mathematics **2** (1999), 118–138.
- [Gau07] P. Gaudry, *Fast genus 2 arithmetic based on theta functions*, J. of Math. Cryptology (2007), no. 1, 243–265.

- [GH00] P. Gaudry and R. Harley, *Counting points on hyperelliptic curves over finite fields.*, ANTS (Wieb Bosma, ed.), Lecture Notes in Computer Science, vol. 1838, Springer, 2000, pp. 313–332.
- [How96] E. Howe, *Constructing distinct curves with isomorphic Jacobians*, J. Number Theory **56** (1996), no. 2, 381–390.
- [IK04] H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications, no. v. 53, American Mathematical Society, 2004.
- [JMV05] D. Jao, S.D. Miller, and R. Venkatesan, *Do all elliptic curves of the same order have the same difficulty of discrete log?*, ASIACRYPT (B. Roy, ed.), Lecture Notes in Computer Science, vol. 3788, Springer, 2005, pp. 21–40.
- [JMV09] D. Jao, S. D. Miller, and R. Venkatesan, *Expander graphs based on GRH with an application to elliptic curve cryptography*, J. Number Theory **129** (2009), no. 6, 1491 – 1504.
- [Kob87] N. Koblitz, *Elliptic curve cryptosystems*, Mathematics of computation **48** (1987), no. 177, 203–209.
- [LD15] Chang Lv and YingPu Deng, *On orders in number fields: Picard groups, ring class fields and applications*, Science China Mathematics **58** (2015), no. 8, 1627–1638.
- [Mil86] V. S. Miller, *Use of elliptic curves in cryptography*, pp. 417–426, Springer Berlin Heidelberg, Berlin, Heidelberg, 1986.
- [Mil06] J. Milne, *Complex multiplication*, <http://www.jmilne.org/math/CourseNotes/CM.pdf> (2006).
- [Pil90] J. Pila, *Frobenius maps of abelian varieties and finding roots of unity in finite fields*, Math. Comp. **55** (1990), no. 192, 745–763.
- [ST61] G. Shimura and Y. Taniyama, *Complex multiplication of abelian varieties and its applications to number theory*, Publications of the Mathematical Society of Japan, vol. 6, The Mathematical Society of Japan, Tokyo, 1961.
- [ST68] J-P. Serre and J.T. Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517.
- [Str10] M. Streng, *Complex multiplication of abelian surfaces*, Ph.D. thesis, Universiteit Leiden, 2010.
- [Tat66] J. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144.
- [Wat69] W. Waterhouse, *Abelian varieties over finite fields*, Annales scientifiques de l'École Normale Supérieure **2** (1969), no. 4, 521–560 (eng).

E-mail address: `dimitar.jetchev@epfl.ch`

ECOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE, EPFL SB GR-JET, SWITZERLAND

E-mail address: `benjamin.wesolowski@epfl.ch`

ECOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE, , EPFL IC LACAL, SWITZERLAND