Commuting Ramanujan Graphs and the Random Self-Reducibility of Isogeny Problems

Youcef Mokrani* and David Jao[0000−0002−8073−1692]

Department of Combinatorics & Optimization, University of Waterloo
200 University Ave. W, Waterloo ON N2L 3G1, Canada
{ymokrani,djao}@uwaterloo.ca

Abstract. Recent attacks on SIDH have led to increased scrutiny of hardness assumptions for isogeny based cryptosystems, especially in the case of SIDH variants which mask some of the information disclosed by the original. One such piece of information which is potentially public in SIDH variants is the endomorphism ring of the domain of the secret isogeny. A possible way to mask this information is to use a random starting elliptic curve instead of a fixed one. This approach raises the question of whether doing so generates a new vulnerability, that is, whether the hardness assumptions corresponding to these new SIDH variants are randomly self-reducible.
In this paper, we study families of Ramanujan graphs whose adjacency matrices commute. We use results on these families of commuting matrices to prove the random self-reducibility of the hardness assumptions underlying the FESTA scheme, as well as for some SIDH-based proof of knowledge schemes.

1 Introduction

Isogeny based cryptography represents one of the possible candidate approaches to constructing post-quantum cryptosystems. All isogeny-based schemes derive their security from the hardness of the generic Supersingular Isogeny Problem (SIP), which entails constructing an isogeny between two given supersingular elliptic curves. To date, there is no known efficient quantum algorithm for solving this problem.

However, in practice, although the security of all isogeny-based cryptosystems is ultimately based on SIP, most such schemes actually require stronger assumptions, as one usually needs more information about a secret isogeny than just the endpoint curves in order to interact with it cryptographically. The most famous such scheme is SIDH [15], a key exchange scheme. In addition to providing the domain and codomain of the secret isogeny, SIDH also publishes its degree, its mapping on a fixed torsion subgroup and the endomorphism ring of the domain elliptic curve. The scheme had been conjectured post-quantum secure and was a Round 4 candidate in the NIST post-quantum standardization process until a series of papers by Castryk-Decru [7], Maino et al. [18] and Robert [22] proposed increasingly effective attacks on SIDH culminating in a classical break.

Since then, there have been multiple attempts at creating a secure SIDH variant by masking some of the leaked information. All such proposed variants mask the torsion point mapping information in order to be secure against known SIDH attacks. In fact, many proposals only mask the mapping, and continue to disclose the degree and domain endomorphism ring, for example M-SIDH [12], BinSIDH [5] and FESTA [6]. Some schemes, such as MD-SIDH [12] and Ter-SIDH [5], also mask the degree of the secret isogeny. Our focus here is on the third piece of aforementioned information, namely, the endomorphism ring of the starting curve for the isogeny. While such information is not necessary in Robert's version of the attack, it was needed in the original attack on SIDH by Castryk and Decru. Moreover, other attacks on SIDH and its variants also rely on the knowledge of the starting endomorphism ring, including Petit's [20] lollipop endomorphism attack, as well as Castryck and Vercauteren's recent adaptation of Petit's attack to M-SIDH and FESTA [8]. Therefore, there is good reason to avoid working with elliptic curves of known endomorphism ring if possible.

None of the cryptosystems mentioned above explicitly requires knowledge of the endomorphism ring of the starting curve of the isogeny in order to operate. However, there is no known straightforward way to select an elliptic curve of unknown endomorphism ring while also avoiding any possibility of backdoor knowledge of the endomorphism ring, although Basso et al. [3] have proposed a multiparty protocol to produce such a curve.

In this paper, we ask the question of whether using a random supersingular elliptic curve as opposed to a fixed one could introduce new vulnerabilities in these cryptosystems that we have yet to discover. In order words, for the various isogeny-based cryptosystems mentioned above, is the corresponding isogeny hardness assumption randomly self-reducible? While such a result is easy to prove for the generic Supersingular Isogeny Problem, the various concrete attacks on SIDH, each with different requirements, clearly demonstrate the potential for this result to fail for the actual assumptions that we use in isogeny-based schemes. To date, there are no known random self-reducibility results for the specific isogeny hardness assumptions appearing in SIDH variants that do not make use of orientations.

1.1 Contributions

The main mathematical result of this paper (Theorem 3.3) is a generalization of Sardari's theorem on the distance of vertices in a Ramanujan graph [24]. We generalize Sardari's result to families of Ramanujan graphs whose adjacency matrices commute, subject to some technical conditions on the graph degrees. Applying these results to various families of Ramanujan graphs arising from supersingular elliptic curves with level structure, we obtain sufficiency conditions for the random self-reducibility of isogeny problems linked to SIDH variants. Using eigenvalue results by Codogni and Lido [9], we apply these conditions to prove that, for some isogeny schemes such as FESTA and decisional SIDH-based zero-knowledge proofs [10,15,3], the problem of retrieving the secret key is randomly self-reducible assuming that the degree of the secret isogeny is large

enough and that the field characteristic is congruent to 1 mod 12. We also show that the congruence condition is unnecessary if the degree is a prime power.

In Section 2, we recall the background knowledge necessary for our theorems. These theorems are presented in Section 3, and their application to known isogeny problems is given in Section 4.

1.2 Related works

In the case of isogeny hardness problems involving orientations, such as CSIDH, prior random self-reducibility results do exist. Kawashima et al. [17] prove the random self-reducibilty of CISDH and propose an AKE scheme based on this property. However, their result makes use of the fact that CSIDH has an ideal class group structure, and these results do not carry over to SIDH variants.

The main mathematical result of this paper can be seen as generalization of Sardari [24]. In that paper, Sardari uses the eigenvalues of a single Ramanujan graph to compute a lower bound on the number of vertices that can be reached with a random non-backtracking walk of fixed prime length starting from any curve on the graph. This result can be applied to supersingular isogenies whose degree is a fixed prime power, as the supersingular isogeny graph is a Ramanujan graph. We generalize that theorem by working with families of Ramanujan graphs in order to be able to represent isogenies whose degree is not a prime power.

We make extensive use of recent work by Codogni and Lido [9] giving a full description of which level structures on supersingular elliptic curves generate a Ramanujan graph.

2 Background Knowledge

2.1 Elliptic Curves and Level Structures

In this paper, we are primarily interested with elliptic curves defined over $\mathbb{F}_{p^2}$, for some prime p, and therefore limit our elliptic curves to be defined only over these fields. When appropriate, we may also work in extensions of $\mathbb{F}_{p^2}$.

Level structures, introduced by Arpin [2] and further studied by De Feo et al. [11] and Codogni and Lido [9], provide a simple framework for categorizing isogeny problems corresponding to various SIDH variants.

Definition 2.1 (Level Structure). *Let E be a supersingular elliptic curve, let N be a positive integer and let H be a subgroup of $GL_2(\mathbb{Z}/N\mathbb{Z})$. For an ordered basis (P, Q) of $E[N]$ and for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in H$, we define the action of H on the set of ordered bases of $E[N]$ to be*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} (P, Q) := (aP + bQ, cP + dQ).$$

An H-level structure of E is an orbit of the above action.

Since we will often discuss the set of elliptic curves and level structure pairs, the following notation will be used throughout this paper.

Definition 2.2. *Let H be a subgroup of $GL_2(\mathbb{Z}/N\mathbb{Z})$. We define $\mathcal{E}_H$ to be the set of pairs (E, C) where E is a supersingular elliptic curve over $\mathbb{F}_{p^2}$ and C is an H-level structure in E.*

If $H = GL_2(\mathbb{Z}/N\mathbb{Z})$, there is a single orbit, which is the set of all ordered bases of $E[N]$. In this case we use the simplified notation $\mathcal{E}$ instead of $\mathcal{E}_H$.

2.2 Isogenies

Definition 2.3 (Isogeny). *An isogeny between two elliptic curves is a rational map between the curves which is also a group homomorphism.*

Note that constant isogenies are valid isogenies under our definition.

Definition 2.4 (Isomorphic elliptic curves [25]). *Let E_1 and E_2 be elliptic curves. We say that E_1 and E_2 are isomorphic, and write $E_1 \cong E_2$, if there are isogenies $\phi : E_1 \to E_2$ and $\psi : E_2 \to E_1$ such that $\psi \circ \phi$ and $\phi \circ \psi$ are the identity maps on E_1 and E_2, respectively. Such isogenies are called isomorphisms.*

Similarly to elliptic curves, isogenies can also be isomorphic.

Definition 2.5 (Isomorphic isogenies). *Let $\phi : E_1 \to E_2$ and $\psi : F_1 \to F_2$ be isogenies. We say that ϕ and ψ are isomorphic if there exist elliptic curve isomorphisms $\mu : E_1 \to F_1$ and $\rho : E_2 \to F_2$ such that $\rho \circ \phi = \psi \circ \mu$.*

We can extend the concept of level structure to isogenies by requiring the map to preserve level structures.

Definition 2.6 (Isogeny with level structure). *Let (E_1, C_1) and (E_2, C_2) be two elliptic curve / H-level structure pairs, and let $\phi\colon E_1 \to E_2$ be an isogeny. We say that $\phi\colon (E_1, C_1) \to (E_2, C_2)$ if $\phi(C_1) = C_2$.*

An important fact about isogenies, is the following result:

Theorem 2.7 ([25]). *A separable isogeny is uniquely defined up to isomorphism by its kernel.*

All isogenies in this paper are separable, and so Theorem 2.7 allows us to represent isogenies by their kernel, as well as to define pushforward isogenies.

Definition 2.8 (Pushforward Isogeny [4,23]). *Let E be a supersingular elliptic curve and let ϕ_1, ϕ_2 be isogenies on E of relatively prime degrees. We define the pushforward isogeny $[\phi_1]_*\phi_2$ to be the isogeny with kernel $\phi_1(\ker(\phi_2))$.*

In this paper, we rarely use a pushforward isogeny by itself, but instead compose it with the isogeny that was used to push it. As such, we define the following operation.

Definition 2.9. *We define* $\phi_2 \boxdot \phi_1 := ([\phi_1]_*\phi_2) \circ \phi_1$.

This operation as well as the following theorem form a key building block of most isogeny based schemes.

Theorem 2.10. *Up to isomorphism,* $\phi_2 \boxdot \phi_1$ *and* $\phi_1 \boxdot \phi_2$ *are equal.*

Proof. Since the kernel of both isogenies is $\ker(\phi_1)+\ker(\phi_2)$, Theorem 2.7 implies that the isogenies are equal. □

2.3 Isogeny Graphs

Mestre [19] introduced the idea of using graph-theoretic properties of the graph of supersingular elliptic curve isogenies to study arithmetic aspects of elliptic curves and modular curves.

Definition 2.11. *For a prime characteristic* p *and prime degree* ℓ*, the supersingular* ℓ*-isogeny graph* $\mathcal{G}_\ell$ *is the (directed) graph whose vertices are the supersingular elliptic curves over* $\mathbb{F}_{p^2}$*, up to isomorphism, and whose edges are isogenies of degree* ℓ *between such curves.*

The number of supersingular elliptic curves in characteristic p up to isomorphism is well known.

Lemma 2.12 ([25]). *The number of vertices of* $\mathcal{G}_\ell$ *is*

$$|V(\mathcal{G}_\ell)| = \left\lfloor \frac{p}{12} \right\rfloor + \epsilon$$

where

$$\epsilon = \begin{cases} 0 \text{ if } p \equiv 1 \bmod 12, \\ 1 \text{ if } p \equiv 5 \bmod 12, \\ 1 \text{ if } p \equiv 7 \bmod 12, \\ 2 \text{ if } p \equiv 11 \bmod 12. \end{cases}$$

Definition 2.13 (Ramanujan Graph). *A Ramanujan graph is a* k*-regular connected graph, for some positive integer* k*, whose largest eigenvalue is* k *and whose other eigenvalues have absolute value at most* $2\sqrt{k-1}$.

An important property of supersingular isogeny graphs is that they are Ramanujan. The following well known result was proved by Pizer.

Theorem 2.14 ([21]). $\mathcal{G}_\ell$ *is a* $(\ell+1)$*-regular Ramanujan Graph.*

While supersingular isogeny graphs always satisfy the Ramanujan eigenvalue bound, whether or not the graphs must be viewed as directed graphs is a subtler issue. For most isogenies, the dual isogeny goes in the reverse direction from the original isogeny (i.e. from the original codomain to the original domain), meaning that one can usually ignore the directed aspect of the edges by considering

isogenies together with their duals. However, this simplification breaks down when one of the two endpoint curves has more automorphisms than the other, since post-composition of an isomorphism to an isogeny always by definition produces an isomorphic isogeny, whereas pre-composition of an isomorphism does not always produce an isomorphic isogeny because a pre-isomorphism can potentially map the original kernel to a different subgroup. Therefore, in cases of unequal numbers of automorphisms, it is possible for two isogenies to be isomorphic when their duals are not. For characterstics $p > 3$, such a situation can only arise at j-invariants 0 and 1728, and these j-invariants are not supersingular if p is 1 mod 12, yielding the following result.

Theorem 2.15 ([21]). *If $p \equiv 1 \bmod 12$, then $\mathcal{G}_\ell$ is an undirected $(\ell+1)$-regular Ramanujan Graph.*

For the isogeny graph $\mathcal{G}_\ell$ itself (without level structure), the condition $p \equiv 1 \bmod 12$ is obligatory. In all other cases, the presence of extra automorphisms at the supersingular j-invariants at 0 and 1728 introduces asymmetries in the adjacency matrix of the isogeny graph which prevents consideration of this graph as an undirected graph. However, when we consider the isogeny graph $\mathcal{G}_{H,\ell}$ having level structure (Definition 2.18), in some cases the aforementioned asymmetries vanish because the extra automorphisms do not preserve the level structure and therefore no longer result in asymmetries (cf. Remark 2.19).

The reason we care about supersingular isogeny graphs being Ramanujan is that, in combination with the following theorem by De Feo, Jao and Plût, we can link the randomness of walks on supersingular isogeny graphs to the randomness of the final elliptic curve on said walks.

Theorem 2.16 ([16]). *Let G be a finite k-regular graph for which the non-trivial eigenvalues λ of the adjacency matrix are bounded by $|\lambda| \leq c$, for some $c < k$. Let S be any subset of the vertices of G, and v be any vertex of G. Then a random walk of length at least $\frac{\log\left(2|G|/\sqrt{|S|}\right)}{\log(k/c)}$ will end in S with probability between $\frac{|S|}{2|G|}$ and $\frac{3|S|}{2|G|}$.*

For the purposes of this paper, another important result is the following theorem by Sardari.

Theorem 2.17 ([24]). *Let G be a k-regular Ramanujan graph with n vertices and fix a vertex $x \in V(G)$. Let R be an integer such that $R > (1+\epsilon)\log_{k-1}(n)$. Define $M(x,R)$ to be the set of all vertices $y \in G$ such that there is no non-backtracking walk from x to y with length R. Then*

$$|M(x,R)| \leq n^{1-\epsilon}(1+R)^2.$$

The concept of level structure can be combined with supersingular isogeny graphs to obtain the following construction of isogeny graphs with level structure.

Definition 2.18. *For a field $\mathbb{F}_{p^k}$, a subgroup H of $GL_2(\mathbb{Z}/N\mathbb{Z})$, and an integer $\ell \nmid N$, the supersingular ℓ-isogeny graph with H-structure $\mathcal{G}_{H,\ell}$ is the graph whose vertices are the pairs (E, C) of supersingular elliptic curves E over $\mathbb{F}_{p^2}$ up to isomorphism and H-level structure C of E, and whose edges are the isogenies of degree ℓ between said pairs, also up to isomorphism.*

Remark 2.19. If $p \equiv 1 \bmod 12$, and ℓ belongs to H, the graph $\mathcal{G}_{H,\ell}$ is always undirected [9, Prop. 2.2.2]. In other cases, the graph may still be undirected, depending on the values of p, N, ℓ, and H. For example, when N is prime, the curve with $j = 1728$ is supersingular if and only if $p \equiv 3 \bmod 4$, in which case [2, Prop. 3.6] states that complex multiplication by i has no fixed points among the set of order N subgroups precisely when $N \equiv 3 \bmod 4$. In such cases, all vertices of the isogeny graph with level structure have the same number of automorphisms. Similarly, the curve $j = 0$ is supersingular if and only if $p \equiv 2 \bmod 3$, and complex multiplication by ζ_3 has no fixed points among the set of order N subgroups precisely when $N \equiv 2 \bmod 3$. We emphasize that uniformity of the number of automorphisms, by itself, is not sufficient to conclude that the adjacency matrix of the isogeny graph with level structure is symmetric. As shown in [9, Prop. 2.2.2], we also need ℓ to belong to H in order to ensure symmetry.

We need an upper bound on the size of this graph. A simple one to obtain is the following.

Lemma 2.20.

$$|\mathcal{E}_H| < \left(\frac{p}{12} + 2\right) \frac{|GL_2(\mathbb{Z}/N\mathbb{Z})|}{|H|}$$

Proof. From Lemma 2.12, we have that the number of supersingular curves, up to isomorphism, is less then $\frac{p}{12} + 2$. Since we are looking for an upper bound, we can ignore the possible isomorphism between two level structures of the same curve.

Let E be a supersingular elliptic curve, and let B be the set of ordered bases of $E[N]$. The number of level structures on E is the number of orbits of the group action of H on B. Since $E[N] \cong (\mathbb{Z}/N\mathbb{Z})^2$, $|B| = |GL_2(\mathbb{Z}/N\mathbb{Z})|$.

Since, for any ordered basis, the only matrix stabilizing it is the identity, we have that, by the orbit-stabilizer theorem, each orbit has size H. We can then combine Burnside's lemma with Lagrange's theorem to get that the number of orbits is $\frac{|B|}{|H|}$, leading to the desired inequality. □

The exact size of $GL_2(\mathbb{Z}/N\mathbb{Z})$ can be computed using the following theorem.

Theorem 2.21 ([13]). *Let $N = \prod_{k=1}^{t} \rho_k^{\alpha_k}$. Then*

$$|GL_2(\mathbb{Z}/N\mathbb{Z})| = \prod_{k=1}^{t} \rho_k^{4(\alpha_k - 1)} (\rho_k^2 - 1)(\rho_k^2 - \rho_k).$$

A recent paper, by Codogni and Lido, provides a generalization of Pizer's result to the case of added level structure.

Theorem 2.22 ([9]). *If every invertible multiple of the identity as well as a matrix of every determinant are in H, then $\mathcal{G}_{H,\ell}$ is an $(\ell+1)$-Ramanujan graph and its adjacency matrix is diagonalizable.*

Of course, the above conditions do not apply to every level structure, as we discuss in more detail in Section 4, but they do apply to some currently used primitives such as FESTA and the zero-knowledge proofs found in [10,15,3].

For a fixed value of p and H, the number of supersingular elliptic curves with H-level structure up to isomorphism is also fixed. As such, the dimensions of the adjacency matrix of $\mathcal{G}_\ell$ are the same for every value of ℓ. In fact, we also have that these matrices commute.

Lemma 2.23. *Let ℓ_1 and ℓ_2 be distinct primes and let A_1 and A_2 be the adjacency matrices of $\mathcal{G}_{H,\ell_1}$ and $\mathcal{G}_{H,\ell_2}$ respectively. We have that $A_1A_2 = A_2A_1$.*

Proof. For two elliptic curves E and F, $A_1(E,F)$ is the number of ℓ_1 isogenies from E to F. Similarly, $A_2A_1(E,F)$ is the number of isogenies from E to F that can be constructed as $\phi_2 \boxdot \phi_1$ where ϕ_2 is an isogeny of degree ℓ_2 and ϕ_1 is an isogeny of degree ℓ_1. By Theorem 2.10, each such isogeny can be written as $\phi_1 \boxdot \phi_2$. Therefore, $A_1A_2(E,F) \geq A_2A_1(E,F)$. Since this argument is symmetric, we can conclude that $A_1A_2(E,F) = A_2A_1(E,F)$. As this holds for any pair of elliptic curves, we have that $A_1A_2 = A_2A_1$. □

An important issue in this paper is the question of whether there exists an isogeny of fixed degree between two supersingular curves with level structure. As such, we use the following notation.

Definition 2.24. *Let $(E,C) \in \mathcal{E}_H$. We define $\Xi_{E,H,C,d}$ as*

$$\Xi_{E,H,C,d} = \{(F,D) \in \mathcal{E}_H \mid \exists\ \phi\colon E \to F,\ \phi(C) = D \text{ and } \deg(\phi) = d\}.$$

2.4 Linear Algebra

For the main result of this paper, we will require the following standard theorem from linear algebra.

Theorem 2.25 ([14, Thm. 1.3.21]). *If a family of diagonalizable matrices commutes, then there is an eigenvector basis that diagonalizes all of them at the same time (with possibly different eigenvalues).*

As our main result is somewhat a generalization of Sardari's result [24], we will also need to make use of Chebyshev polynomials of the second kind, which can be used to represent non-backtracking walks of regular graphs.

Definition 2.26 (Chebyshev polynomials of the second kind). *The family $\{U_n(x)\}_{n\in\mathbb{N}}$ of Chebyshev polynomials of the second kind is defined by the following recurrence relation:*

$$\begin{cases} U_0(x) = 1, \\ U_1(x) = 2x, \\ U_{n+1}(x) = 2xU_n(x) - U_{n-1}(x). \end{cases}$$

An important property of Chebyshev polynomials of the second kind is the following bound.

Theorem 2.27 ([1]). *For $-1 \leq x \leq 1$, we have that $-(n+1) \leq U_n(x) \leq (n+1)$.*

From elementary linear algebra, we also require the following standard results on diagonalizable matrices.

Theorem 2.28. *If A is a real symmetric matrix, then it is diagonalizable and its eigenvectors are orthonormal.*

Theorem 2.29. *If A is diagonalizable with eigenvalues $\lambda_1, \ldots, \lambda_n$ with associated eigenvectors $\phi_1, \ldots, \phi_n$, then*

$$A = \sum_{i=1}^{n} \lambda_i \phi_i^t \phi_i.$$

In addition, if p is a polynomial, then,

$$p(A) = \sum_{i=1}^{n} p(\lambda_i) \phi_i^t \phi_i.$$

2.5 Computational Problems

Definition 2.30. *We say that a problem is randomly self-reducible if every algorithm solving it for a non-negligible fraction of cases can be modified with a polynomial loss in efficiency to solve every case.*

When studying the possible random self-reducibility of problem associated with isogeny problems, we focus in this paper on the problems linked with the retrieval of the secret key, which is the secret isogeny. The most generic problem is of course SIP.

Problem 2.31 (Supersingular Isogeny Problem). Given two supersingular elliptic curves E and F over $\mathbb{F}_{p^2}$, compute an isogeny $\phi\colon E \to F$.

Note that every supersingular elliptic curve over $\mathbb{F}_{p^2}$ is isomorphic (possibly over an extension field) to a supersingular elliptic curve with exactly $(p+1)^2$ points. Additionally, Tate's isogeny theorem states that two curves over a finite field with the same number of points are isogenous. As such, by choosing such

curves as representatives of each isomorphism class, we can guarantee the existence of an isogeny between any two supersingular elliptic curves. As mentioned in the introduction, in most SIDH variants, the degree of the secret isogeny is known. Even in the cases where it is hidden, such as in MD-SIDH, a multiple of the degree is known, which leads us to the following problem.

Problem 2.32. Let d be a positive integer and let E and F be supersingular elliptic curves over $\mathbb{F}_{p^2}$. Given a guarantee that there exists a d-isogeny $\psi\colon E \to F$, compute an isogeny $\phi\colon E \to F$.

Note that finding an isogeny of degree other than d constitutes a valid solution to this problem. The reason we choose to work on this problem, rather than one where the degree of the outputted isogeny is specified is that, in practice, finding such an isogeny is enough to break most isogeny based encryption schemes.

Of course, the most substantial information that is typically made available, be it in the original SIDH, its new variants like M-SIDH, or even more distinct schemes like FESTA, is the mapping of the isogeny on a chosen level structure. Hence, the most important problem we want to be randomly self-reducible is the following.

Problem 2.33 (Known Level Structure Supersingular Isogeny Problem). Let d and N be relatively prime positive integers, and let $H < GL_2(\mathbb{Z}/N\mathbb{Z})$. Let (E, C) and (F, D) be supersingular elliptic curves-H-level structure pairs over $\mathbb{F}_{p^2}$. Given a guarantee that there is a d-isogeny $\psi\colon (E, C) \to (F, D)$, compute an isogeny $\phi\colon E \to F$ such that $\phi(C) = D$.

Problem 2.32 can be seen as a special case of Problem 2.33 where $H = GL_2(\mathbb{Z}/N\mathbb{Z})$. As such, our results focus on Problem 2.33 and we discuss how they apply to Problem 2.32 in Section 4.

3 Main Result

In this section, we will prove that some isogeny based problems are randomly self-reducible. As mentioned previously, the generic Supersingular Isogeny Problem is easily proven to be random self-reducible, as follows.

Theorem 3.1. *Problem 2.31 is randomly self-reducible.*

Proof. Let ℓ be any small prime number (e.g., 2) and consider E and F as vertices on the graph $\mathcal{G}_\ell$. Let $\mathcal{A}$ be an algorithm solving Problem 2.31 for a non-negligible fraction ϵ of pairs (E, F). Let T_E be the set of values of F such that $\mathcal{A}$ solves Problem 2.31 for (E, F). Let T' be the set of values of E for which the size of T_E is a non-negligible fraction of $|\mathcal{E}|$, and let ε be the smallest such fraction. Since the number of pairs (E, F) for which $\mathcal{A}$ solves Problem 2.31 is equal to $\sum_{E\in\mathcal{E}} |T_E|$, we have that $\frac{|T'|}{|\mathcal{E}|}$ is a non-negligible fraction δ. Consider the following algorithm, denoted REDU1.

1: **function** REDU1(ℓ,p, E, F)
2: Evaluate $\lambda = \frac{\log(2|\mathcal{E}|)}{\log\left((\ell+1)/(2\sqrt{\ell})\right)}$
3: Let $\phi_1 : E \to E'$ be a ℓ^λ-isogeny generated by a random walk on the ℓ-isogeny graph from E
4: Let $\phi_2 : F \to F'$ be a ℓ^λ-isogeny generated by a random walk on the ℓ-isogeny graph from F
5: Use $\mathcal{A}$ to evaluate an isogeny $\psi\colon E' \to F'$
6: **return** $\hat{\phi_2}\psi\phi_1$
7: **end function**

Since ℓ is small and λ is polynomial, the evaluation of isogenies and duals can be done in polynomial time. Let α be the probability of success of $\mathcal{A}$ on the pairs that it can solve. By Theorem 2.16, the probability that we have $E' \in T'$ is at least $\frac{\delta}{2}$, and the probability that $F' \in T_E$ is at least $\frac{\varepsilon}{2}$. Hence, the probability of success of REDU1 is at least $\frac{\alpha\delta\varepsilon}{4}$, which is non-negligible. □

Since Problem 2.33 can be seen as a generalization of Problem 2.32, we only need to find sufficient conditions for the former to be randomly self-reducible and then show that the latter respects these conditions.

Theorem 3.2. *If $\frac{|\Xi_{E,H,C,d}|}{|\mathcal{E}_H|}$ is non-negligible for all $(E, C) \in \mathcal{E}_H$, then Problem 2.33 is randomly self-reducible.*

Proof. Let ℓ be a small prime number not dividing N.

Let $\mathcal{B}$ be an algorithm that can solve Problem 2.33 for a non-negligible fraction of pairs $((E, C), (F, D))$ with $(F, D) \in \Xi_{E,H,C,d}$.

For any given pair $((E, C), (F, D))$ and any secret d-isogeny $\psi\colon (E, C) \to (F, D)$, we can use the following reduction algorithm:

1: **function** REDU2(ℓ,p, (E, C), (F, D))
2: Evaluate $\lambda = \frac{\log(2|\mathcal{E}_H|)}{\log\left((\ell+1)/(2\sqrt{\ell})\right)}$
3: Let $\phi_1\colon (E, C) \to (E', C')$ be a ℓ^λ-isogeny generated by a random walk on the ℓ-isogeny graph from (E, C)
4: Let $\phi_2\colon (F, D) \to (F', D')$ be a ℓ^λ-isogeny generated by a random walk on the ℓ-isogeny graph from (F, D)
5: Use $\mathcal{B}$ to evaluate an isogeny $\psi'\colon (E', C') \to (F', D')$
6: **return** $\hat{\phi_2}\psi'\phi_1$
7: **end function**

We only need to check that the probability of success in non-negligible. Let $T_{(E,C)}$ be the set of values of (F, D) such that $\mathcal{B}$ solves Problem 2.33 for $((E, C), (F, D))$. Let T' be the set of values of (E, C) for which the size of $T_{(E,C)}$

is a non-negligible fraction of $|\Xi_{E,C,H,d}|$ and let ε be the smallest such fraction. Since the number of pairs $((E,C),(F,D))$ for which $\mathcal{B}$ solves Problem 2.33 is equal to $\sum_{(E,C)\in\mathcal{E}_H}\left|T_{(E,C)}\right|$, we have that $\frac{|T'|}{|\Xi_{E,C,H,d}|}$ is a non-negligible fraction. Because $\frac{|\Xi_{E,C,H,d}|}{|\mathcal{E}_H|}$ is also non-negligible, $\frac{|T'|}{|\mathcal{E}_H|}$ is a non-negligible fraction δ. Since $\frac{|\Xi_{E,C,H,d}|}{|\mathcal{E}_H|}$ is non-negligible for all $(E,C)\in\mathcal{E}_H$, it follows that (F',D') has a non-negligible probability to be in $\Xi_{E',C',H,d}$. Hence, $\mathcal{B}$ has a non-negligible probability to succeed. □

In order to use the above theorem, we require a way to compute a lower bound for $\frac{|\Xi_{E,H,C,d}|}{|\mathcal{E}_H|}$. To do that, we generalize a theorem by Sardari [24].

Theorem 3.3. *Let $G_1,\ldots,G_k$ be a family of Ramanujan graphs with same common vertex set V, of size n, such that the following properties hold:*

1. *G_i is a (ℓ_i+1)-regular graph with a diagonalizable adjacency matrix, for some positive integer ℓ_i. (While not necessary for this theorem, ℓ_i is prime for our applications.)*
2. *G_i is undirected, so that its adjacency matrix is symmetric.*
3. *$\gcd(\ell_i,\ell_j)=1$ for $i\neq j$.*
4. *The adjacency matrices A_i and A_j of each pair of graphs G_i and G_j commute.*

Let $\boldsymbol{e}=(e_1,\ldots,e_k)$ be a vector of non-negative integers. Let $x\in V$ and let $\Xi_{\boldsymbol{e}}(x)$ be the set of vertices we can arrive at using the following algorithm.

1. *Let $x_0=x$.*
2. *For $1\leq i\leq k$, take a random non-backtracking walk in G_i of length e_i starting at x_{i-1} and let the final point be x_i.*
3. *Return x_k.*

Then

$$|\Xi_{\boldsymbol{e}}(x)|\geq n\left(1-\frac{n}{\prod_{i=1}^{k}\ell_i^{e_i}}\prod_{i=1}^{k}(e_i+1)^2\right).$$

Remark 3.4. When $p\equiv 1 \bmod 12$, G_i is taken to be the supersingular isogeny graph $\mathcal{G}_{\ell_i}$ over $\mathbb{F}_{p^2}$. Properties 1 and 2 come from Theorem 2.15, Property 3 is due to the fact that distinct supersingular isogeny graph use distinct prime values of ℓ and Property 4 comes from Lemma 2.23. As mentioned in Remark 2.19, when N is prime and the level structure is non-trivial ($H\neq GL_2(\mathbb{Z}/N\mathbb{Z})$), we have more cases where the isogeny graph is undirected and where this theorem applies. Namely, if $p\equiv 7 \bmod 12$ and ℓ belongs to H, Theorem 3.3 still applies if $N\equiv 3 \bmod 4$. Similarly, if $p\equiv 5 \bmod 12$ and ℓ belongs to H, then our theorem applies when $N\equiv 2 \bmod 3$, and if $p\equiv 11 \bmod 12$ then it applies when $N\equiv 11 \bmod 12$.

Proof. Since the adjacency matrices commute and are diagonalizable, Theorem 2.25 implies that there is a common basis of eigenvectors. Denote these (normalized) eigenvectors by ϕ_j, where ϕ_1 is the constant eigenvector (which exists since we are dealing with regular graphs).

Let $\lambda_{i,j}$ be the eigenvalue associated with ϕ_j for A_i. Since the G_i are Ramanujan graphs, we have that $\lambda_{i,1} = \ell_i + 1$ and $\lambda_{i,j} \leq 2\sqrt{\ell_i}$ for $j \geq 2$. Let

$$S_i(R) = \begin{cases} I \text{ if } R = 0, \\ A_i \text{ if } R = 1, \\ A_i S_i(R-1) - \ell_i S_i(R-2) \text{ otherwise.} \end{cases}$$

Here, $S_i(R)$ is the adjacency matrix of the graph whose edges are the walks of length R on G_i with no backtracking. From the above recurrence, we have

$$S_i(R) = (\ell_i)^{\frac{R}{2}} U_R\left(\frac{A_i}{2\sqrt{\ell_i}}\right)$$

where U_R is the Chebyshev of polynomial of the second kind defined in Definition 2.26. Observe that, since A_i is diagonalizable, we can write it as

$$\sum_{j=1}^{n} \lambda_{i,j} \phi_j^t \phi_j.$$

Since for any fixed R, $S_i(R)$ is a polynomial in A_i, we can use Theorem 2.29 to obtain

$$S_i(R) = \sum_{j=1}^{n} (\ell_i)^{\frac{R}{2}} U_R\left(\frac{\lambda_{i,j}}{2\sqrt{\ell_i}}\right) \phi_j^t \phi_j.$$

With multiplicity, the set of non-backtracking $\mathbf{e}$-walks is represented by

$$\begin{aligned} \prod_{i=1}^{k} S_i(e_i) &= \prod_{i=1}^{k} \sum_{j=1}^{n} (\ell_i)^{\frac{e_i}{2}} U_{e_i}\left(\frac{\lambda_{i,j}}{2\sqrt{\ell_i}}\right) \phi_j^t \phi_j \\ &= \sum_{1 \leq j_1, \ldots, j_k \leq n} \prod_{i=1}^{k} \left((\ell_i)^{\frac{e_i}{2}} U_{e_i}\left(\frac{\lambda_{i,j_i}}{2\sqrt{\ell_i}}\right) \phi_{j_i}^t \phi_{j_i} \right) \\ &= \sum_{1 \leq j_1, \ldots, j_k \leq n} \prod_{i=1}^{k} \left((\ell_i)^{\frac{e_i}{2}} U_{e_i}\left(\frac{\lambda_{i,j_i}}{2\sqrt{\ell_i}}\right) \right) \prod_{i=1}^{k} \left(\phi_{j_i}^t \phi_{j_i} \right). \end{aligned}$$

Since the set of ϕ_j consists of eigenvectors of real symmetric matrices, said vectors are orthonormal. Hence, $\prod_{i=1}^{k} \left(\phi_{j_i}^t \phi_{j_i} \right)$ is equal to 1 if all j_i's are equal and 0 otherwise, so

$$\prod_{i=1}^{k} S_i(e_i) = \sum_{j=1}^{n} \phi_j^t \phi_j \prod_{i=1}^{k} (\ell_i)^{\frac{e_i}{2}} U_{e_i}\left(\frac{\lambda_{i,j}}{2\sqrt{\ell_i}}\right).$$

For any two vertices x and y of V,

$$\prod_{i=1}^{k} S_i(e_i)(x,y) = \sum_{j=1}^{n} \phi_j(x)\phi_j(y) \prod_{i=1}^{k} (\ell_i)^{\frac{e_i}{2}} U_{e_i}\left(\frac{\lambda_{i,j}}{2\sqrt{\ell_i}}\right)$$

is equal to the number of $\mathbf{e}$-walks from x to y. Let x be a fixed vertex of V, and let y be a uniformly distributed random vertex of G. Since the total number of $\mathbf{e}$-walks is constant regardless of the choice of x (because the graphs are regular), we have that

$$E_y[\prod_{i=1}^{k} S_i(e_i)(x,y)] = \frac{\prod_{i=1}^{k} \left(\ell_i^{e_i-1}(\ell_i+1)\right)}{n}.$$

We also want to evaluate

$$\mathrm{Var}_y\left[\prod_{i=1}^{k} S_i(e_i)(x,y)\right] = \mathrm{Var}_y\left[\sum_{j=1}^{n} \phi_j(x)\phi_j(y) \prod_{i=1}^{k} (\ell_i)^{\frac{e_i}{2}} U_{e_i}\left(\frac{\lambda_{i,j}}{2\sqrt{\ell_i}}\right)\right].$$

Note ϕ_1 is the constant eigenvector, which implies that

$$\phi_1(x)\phi_1(y) \prod_{i=1}^{k} (\ell_i)^{\frac{e_i}{2}} U_{e_i}\left(\frac{\lambda_{i,1}}{2\sqrt{\ell_i}}\right)$$

does not depend on y and can be ignored when evaluating the variance.

$$\begin{aligned}
\mathrm{Var}_y\left[\prod_{i=1}^{k} S_i(e_i)(x,y)\right] &= \mathrm{Var}_y\left[\sum_{j=2}^{n} \phi_j(x)\phi_j(y) \prod_{i=1}^{k} (\ell_i)^{\frac{e_i}{2}} U_{e_i}\left(\frac{\lambda_{i,j}}{2\sqrt{\ell_i}}\right)\right] \\
&= E_y\left[\left(\sum_{j=2}^{n} \phi_j(x)\phi_j(y) \prod_{i=1}^{k} (\ell_i)^{\frac{e_i}{2}} U_{e_i}\left(\frac{\lambda_{i,j}}{2\sqrt{\ell_i}}\right)\right)^2\right] \\
&\quad - E_y\left[\sum_{j=2}^{n} \phi_j(x)\phi_j(y) \prod_{i=1}^{k} (\ell_i)^{\frac{e_i}{2}} U_{e_i}\left(\frac{\lambda_{i,j}}{2\sqrt{\ell_i}}\right)\right]^2 \\
&\leq E_y\left[\left(\sum_{j=2}^{n} \phi_j(x)\phi_j(y) \prod_{i=1}^{k} (\ell_i)^{\frac{e_i}{2}} U_{e_i}\left(\frac{\lambda_{i,j}}{2\sqrt{\ell_i}}\right)\right)^2\right] \\
&= \frac{1}{n}\sum_{y\in\Gamma}\left(\sum_{j=2}^{n} \phi_j(x)\phi_j(y) \prod_{i=1}^{k} (\ell_i)^{\frac{e_i}{2}} U_{e_i}\left(\frac{\lambda_{i,j}}{2\sqrt{\ell_i}}\right)\right)^2 \\
&= \frac{1}{n}\sum_{y\in\Gamma}\sum_{j_1=2}^{n}\sum_{j_2=2}^{n} \phi_{j_1}(x)\phi_{j_2}(x)\phi_{j_1}(y)\phi_{j_2}(y) \\
&\qquad \left(\prod_{i=1}^{k} (\ell_i)^{\frac{e_i}{2}} U_{e_i}\left(\frac{\lambda_{i,j_1}}{2\sqrt{\ell_i}}\right)\right)\left(\prod_{i=1}^{k} (\ell_i)^{\frac{e_i}{2}} U_{e_i}\left(\frac{\lambda_{i,j_2}}{2\sqrt{\ell_i}}\right)\right).
\end{aligned}$$

Since the ϕ_j's are orthonormal, we have that

$$\operatorname{Var}_y\left[\prod_{i=1}^{k} S_i(e_i)(x,y)\right] \leq \frac{1}{n}\sum_{j_1=2}^{n}\sum_{j_2=2}^{n}\phi_{j_1}(x)\phi_{j_2}(x)\left(\prod_{i=1}^{k}(\ell_i)^{\frac{e_i}{2}}U_{e_i}\left(\frac{\lambda_{i,j_1}}{2\sqrt{\ell_i}}\right)\right)$$
$$\left(\prod_{i=1}^{k}(\ell_i)^{\frac{e_i}{2}}U_{e_i}\left(\frac{\lambda_{i,j_2}}{2\sqrt{\ell_i}}\right)\right)\sum_{y\in\Gamma}\phi_{j_1}(y)\phi_{j_2}(y)$$

$$= \frac{1}{n}\sum_{j_1=2}^{n}\sum_{j_2=2}^{n}\phi_{j_1}(x)\phi_{j_2}(x)\left(\prod_{i=1}^{k}(\ell_i)^{\frac{e_i}{2}}U_{e_i}\left(\frac{\lambda_{i,j_1}}{2\sqrt{\ell_i}}\right)\right)$$
$$\left(\prod_{i=1}^{k}(\ell_i)^{\frac{e_i}{2}}U_{e_i}\left(\frac{\lambda_{i,j_2}}{2\sqrt{\ell_i}}\right)\right)\langle\phi_{j_1},\phi_{j_2}\rangle$$
$$= \frac{1}{n}\sum_{j=2}^{n}\phi_j(x)^2\left(\prod_{i=1}^{k}(\ell_i)^{e_i}U_{e_i}\left(\frac{\lambda_{i,j}}{2\sqrt{\ell_i}}\right)^2\right).$$

When $j \geq 2$, we have $\lambda_{i,j} \leq 2\sqrt{\ell_i}$ since G_i is Ramanujan. Hence $-1 \leq \frac{\lambda_{i,j}}{2\sqrt{\ell_i}} \leq 1$. Theorem 2.27 therefore implies that

$$-(e_i+1) \leq U_{e_i}\left(\frac{\lambda_{i,j}}{2\sqrt{\ell_i}}\right) \leq e_i+1.$$

Hence

$$\operatorname{Var}_y\left[\prod_{i=1}^{k} S_i(e_i)(x,y)\right] \leq \frac{1}{n}\sum_{j=2}^{n}\phi_j(x)^2\left(\prod_{i=1}^{k}(\ell_i)^{e_i}U_{e_i}\left(\frac{\lambda_{i,j}}{2\sqrt{\ell_i}}\right)^2\right)$$
$$= \frac{\prod_{i=1}^{k}(\ell_i)^{e_i}}{n}\sum_{j=2}^{n}\phi_j(x)^2\prod_{i=1}^{k}U_{e_i}\left(\frac{\lambda_{i,j}}{2\sqrt{\ell_i}}\right)^2$$
$$\leq \frac{\prod_{i=1}^{k}(\ell_i)^{e_i}(e_i+1)^2}{n}\sum_{j=2}^{n}\phi_j(x)^2$$
$$< \frac{\prod_{i=1}^{k}(\ell_i)^{e_i}(e_i+1)^2}{n}.$$

since $\sum_{j=2}^{n} \phi_j(x)^2 < 1$ as the ϕ_j's form an orthonormal basis missing one vector. We now use Chebyshev's inequality:

$$\begin{aligned}
&\Pr\left[\prod_{i=1}^{k} S_i(e_i)(x,y) = 0\right] \\
&\leq \Pr\left[\left|\prod_{i=1}^{k} S_i(e_i)(x,y) - E_y[\prod_{i=1}^{k} S_i(e_i)(x,y)]\right| \geq E_y[\prod_{i=1}^{k} S_i(e_i)(x,y)]\right] \\
&\leq \frac{\mathrm{Var}_y\left[\prod_{i=1}^{k} S_i(e_i)(x,y)\right]}{E_y[\prod_{i=1}^{k} S_i(e_i)(x,y)]^2}
\end{aligned}$$

$$\begin{aligned}
&< n\frac{\prod_{i=1}^{k}(\ell_i)^{e_i}(e_i+1)^2}{\prod_{i=1}^{k}\left(\ell_i^{e_i-1}(\ell_i+1)\right)^2} \\
&< n\frac{\prod_{i=1}^{k}(e_i+1)^2}{\prod_{i=1}^{k}\ell_i^{e_i}}.
\end{aligned}$$

Therefore

$$\left|\{y \in \Gamma : \prod_{i=1}^{k} S_i(e_i)(x,y) = 0\}\right| < n^2\frac{\prod_{i=1}^{k}(e_i+1)^2}{\prod_{i=1}^{k}\ell_i^{e_i}} = \frac{n^2}{d}\prod_{i=1}^{k}(e_i+1)^2,$$

so that

$$\begin{aligned}
|\Xi_{\mathbf{e}}(x)| &= \left|\{y \in \Gamma : \prod_{i=1}^{k} S_i(e_i)(x,y) > 0\}\right| \\
&= n - \left|\{y \in \Gamma : \prod_{i=1}^{k} S_i(e_i)(x,y) = 0\}\right| \\
&\geq n - \frac{n^2}{d}\prod_{i=1}^{k}(e_i+1)^2 \\
&\geq n(1 - \frac{n}{\prod_{i=1}^{k}\ell_i^{e_i}}\prod_{i=1}^{k}(e_i+1)^2).
\end{aligned}$$

which is the desired inequality. □

Combining Theorem 3.2 and Theorem 3.3, we obtain:

Corollary 3.5. *Let $d = \prod_{i=1}^{k}\ell_i^{e_i}$ be the factorization of the degree of the secret isogeny in Problem 2.33. If $p \equiv 1 \bmod 12$, and*

$$\frac{d}{|\mathcal{E}_H|\prod_{i=1}^{k}(e_i+1)^2}$$

is non-negligible, and H contains every scalar matrix in $GL_2(\mathbb{Z}/N\mathbb{Z})$, and the set $\det(H)$ is all of $(\mathbb{Z}/N\mathbb{Z})^\times$, then Problem 2.33 in randomly self-reducible.

Remark 3.6. This result still applies when $p \not\equiv 1 \bmod 12$, if N is prime and the conditions discussed in Remark 3.4 are respected.

Proof. Let c be the smallest positive integer such that

$$1 - \frac{n}{\ell_1^{e_1+c}\prod_{i=2}^{k}\ell_i^{e_i}}(e_1+c)\prod_{i=2}^{k}(e_i+1)^2 = 1 - \left(\frac{d}{|\mathcal{E}_H|\prod_{i=1}^{k}(e_i+1)^2}\right)^{-1}\frac{(e_1+c)}{e_1\ell_1^c}$$

is positive and non-negligible. By hypothesis, $\left(\frac{d}{|\mathcal{E}_H|\prod_{i=1}^{k}(e_i+1)^2}\right)^{-1}$ can be upper bounded by a polynomial in terms of the input size. Therefore, a value of ℓ_1^c respecting the desired conditions exists and is also of polynomial size. As a direct result of Theorems 3.2 and 3.3, we have that Problem 2.33 is randomly self-reducible when the degree of the secret isogeny is $\ell_1^c d$.

We remark that Problem 2.33 for a secret isogeny of degree d is polynomially equivalent to the same problem for a secret isogeny of degree $\ell_1^c d$. This is because, in the latter case, we can write the secret isogeny as $\phi_1\phi_2$ where ϕ_1 has degree d and ϕ_2 has degree ℓ_1^c. Since ℓ_1^c is polynomial, we can simply guess ϕ_2 and reduce the problem to an instance where the secret isogeny has degree d.

Hence, Problem 2.33 is also randomly self-reducible for the cases where the secret isogeny is of degree d. □

If $p \not\equiv 1 \bmod 12$, we can still prove random self-reducibility when the secret degree is a prime power (i.e. $k = 1$), by running through the proof of Corollary 3.5 and applying Theorem 2.17 instead of Theorem 3.3.

Corollary 3.7. *In the case where d is a prime power, let $d = \ell_1^{e_1}$ be the factorization of the degree of the secret isogeny in Problem 2.33. If*

$$\frac{\ell_1^{e_1}}{|\mathcal{E}_H|(e_1+1)^2}$$

is non-negligible, and H contains every scalar matrix in $GL_2(\mathbb{Z}/N\mathbb{Z})$, and the set $\det(H)$ is all of $(\mathbb{Z}/N\mathbb{Z})^\times$, then Problem 2.33 in randomly self-reducible.

4 Applications to Isogeny Problems

Using the results of the previous section, we can now explore which choices of H make Problem 2.33 potentially randomly-self reducible. In such cases, we give an upper bound for the required secret isogeny degree.

When studying these cases, we assume that N is smooth and that one of the following cases applies:

1. $p \equiv 1 \bmod 12$,

2. the secret isogeny degree is a prime power,
3. N is prime and one of the following subconditions applies:
   (a) $p \equiv 5 \bmod 12$ and $N \equiv 2 \bmod 3$,
   (b) $p \equiv 7 \bmod 12$ and $N \equiv 3 \bmod 4$,
   (c) $p \equiv 11 \bmod 12$ and $N \equiv 11 \bmod 12$.

Not that the third case asks for N to be both smooth and prime at the same time. This forces N to be small, which limits the applications of this case.

4.1 $H = GL_2(\mathbb{Z}/N\mathbb{Z})$

As mentioned in Subsection 2.5, this case is equivalent to Problem 2.32. In the generic level structure case, the necessary conditions for Corollary 3.5 hold and $|\mathcal{E}_H| = |\mathcal{E}| \sim \frac{p}{12}$. Problem 2.33 is therefore randomly self-reducible as long as

$$\frac{12d}{p\prod_{i=1}^{k}(e_i+1)^2}$$

is non-negligible.

4.2 $H = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$

When $N^2 > d$, the full level structure case can be attacked in polynomial time, as shown by the SIDH attacks [7,18,22], making it trivially randomly self-reducible. This inequality holds for most key exchanges based on SIDH since the values of N and d for one party are the flipped for the other, making the attack work against at least one party.

If one was to somehow use parameters such that the attacks do not hold, our results would not apply in this case since H does not contain every scalar matrix. According to Codogni and Lido [9], the isogeny graph in this case is connected if and only if ℓ generates $(\mathbb{Z}/N\mathbb{Z})^\times$, and walks on the graph will not reach every vertex when the graph is not connected. When the isogeny graph is not connected, we cannot apply Theorem 3.3 since the graph is not Ramanujan. Imagine a degenerate algorithm that could perfectly solve the problem on half the connected components but would always fail on the others. A random walk could not be used to reduce a solution on a successful component to a solution of a failure component. It is worth noting that the graph components are known to be isomorphic [9, Cor. 2.3.7]. If the isomorphism is efficiently computable, then one could use the isomorphism to obtain an equivalence of problems across components. However, if an isomorphism is not efficiently computable, then a reduction is not guaranteed. Of course, this does not necessarily mean that the problem is not randomly self reducible, only that if it was, the reduction would require different techniques.

Even in the cases where the isogeny graph is connected, our results would not apply as is, because, according to [9], the isogeny graph contains non-real

eigenvalues. This does not respect Condition 2 of Theorem 3.3 since non-real eigenvalues would imply that the adjacency matrix is not symmetric. The proof of Theorem 3.3 relies on the fact that every eigenvalue is real, in order to use a known upper bound on Chebyshev polynomials of the second kind. It might be possible to generalize our results to apply here by first proving an upper bound for Chebyshev polynomials in the complex disk of radius 1.

4.3 $H = \left\{ \begin{pmatrix} \mathbf{1} & \mathbf{*} \\ \mathbf{0} & \mathbf{1} \end{pmatrix} \right\}$

As shown by De Feo, Fouotsa and Panny [11], the single torsion point level structure case can be reduced to SIDH, making it also solvable in polynomial time when N is square and $N > d$. In these cases, the problem is trivially randomly self-reducible.

Similarly to the SIDH case, if the parameters are chosen so that no polynomial attack is known, our results do not apply since H does not contain every scalar matrix. According to Codogni and Lido [9], when $H = \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \right\}$, the isogeny graph is connected if and only if ℓ generates $(\mathbb{Z}/N\mathbb{Z})^\times$, but the eigenvalues are not all real. This leads to the same issues as the previous case, with similar avenues for further research.

4.4 $H = \left\{ \begin{pmatrix} \boldsymbol{\lambda} & \mathbf{0} \\ \mathbf{0} & \boldsymbol{\lambda} \end{pmatrix} \right\}$

Unfortunately, the results in this paper do not apply to M-SIDH (and MD-SIDH) since H does not contain matrices of non-square determinant. By [9, Thm. 1.6], if ℓ is a square in $(\mathbb{Z}/N\mathbb{Z})^\times$, then the isogeny graph is not connected and we run into the same issues as in the previous subsections. On the other hand, if ℓ is relatively prime to N and not a square in $(\mathbb{Z}/N\mathbb{Z})^\times$, then the isogeny graph is connected and all of its eigenvalues are real. However, for these values of ℓ, the isogeny graphs have both $(\ell + 1)$ and $-(\ell + 1)$ as eigenvalues. This does not respect the necessary conditions for Theorem 3.3 to apply since the isogeny graph is not Ramanujan when it has this extra trivial eigenvalue. For the proof of Theorem 3.3 to work, we require every eigenvalue, except for the trivial eigenvalue $(\ell + 1)$ having multiplicity one, to be at most $2\sqrt{\ell}$ in absolute value. This is because, when computing the variance in the proof of Theorem 3.3, the largest eigenvalue can be ignored as its eigenvector is the constant eigenvector and therefore has no influence on said variance. This trick does not work with any other eigenvalue and we then have to use upper bounds on Chebyshev's polynomials of the second kind. For the eigenvalue $-(\ell + 1)$, we currently have no usable upper bound, and this causes us similar issues as when the eigenvalues are non-real. While this argument does not prove that the problem is not random self-reducible, it does provide intuition for why M-SIDH might not be randomly self-reducible. For further research, one could find a good upper bound to the Chebyshev polynomial when the eigenvalue is large. Alternatively, one could use

the properties of the eigenvector associated to $-(\ell+1)$ in order to find a trick similar to the one we use to eliminate $(\ell+1)$.

4.5 $\boldsymbol{H = \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}}$

As mentioned in [11], this case is the Borel level structure case. We work with all upper (or lower) triangular matrices. This level structure mainly applies to protocols for zero-knowledge proofs using SIDH squares, for example [10,15,3]. Here H contains every scalar matrix, and there is a matrix for every possible determinant. Therefore, our results apply.

We have that $|H| = N\varphi(N)^2$. Let $N = \prod_{k=1}^{t} \rho_k^{\alpha_k}$ and $d = \prod_{i=1}^{k} \ell_i^{e_i}$. Applying our results, we find that Problem 2.33 is randomly self-reducible as long as

$$\frac{12dN\varphi(N)^2}{p\left(\prod_{k=1}^{t} \rho_k^{4(\alpha_k-1)}(\rho_k^2-1)(\rho_k^2-\rho_k)\right)\prod_{i=1}^{k}(e_i+1)^2}$$

is not negligible.

To get an idea of the size of the above fraction for current scheme, take for example the zero-knowledge proof found in the paper by Basso et al. [3]. One of the parameter sets used in the paper is the one from SIKE434. In this case, we have that $p = 2^{216} \times 3^{137} - 1$, $N = 2^{216}$ and $d = 3^{137}$. The formula becomes:

$$\frac{12 \times 2^{216} \times 3^{137} 2^{2\times 216-2}}{(2^{216} \times 3^{137} - 1)\left(2^{4(216-1)}(2^2-1)(2^2-2)\right)(137+1)^2} \approx 3.79 \times 10^{-134}.$$

Sadly, this is much too small to be useful. However, the zero-knowledge proof in [3] could be modified so that the d-isogeny is longer. For an example of parameter set for which the formula is useful, let $p = 2^a 3^b - 1$, $d = 3^{3b}$ and $N = 2^a$. The formula becomes:

$$\frac{12 \times 3^{3b} 2^{3a-2}}{(2^a 3^b - 1)\left(2^{4(a-1)}(2^2-1)(2^2-2)\right)(b+1)^2} \approx \frac{3^{2b}}{2^{2a}}$$

If $2^a \approx 3^b$, then the problem is randomly self-reducible. Using the same prime as before, a valid parameter set would be $p = 2^{216} \times 3^{137} - 1$, $N = 2^{216}$ and $d = 3^{411}$. In this case, the formula is equal to approximately 2.29×10^{-4}. As this is clearly non-negligible, this parameter set leads us to a randomly self-reducible problem. Of course this is a lower bound on the probability of success of the reduction algorithm and not on the length of the algorithm itself. As such, it is possible for the reduction to be more efficient in practice, in which case we could use smaller parameters. Still, with the above choice of parameters, we would need to compute isogeny chains of three times the length as those used in SIDH. While there is a required loss of efficient if one desired using our results in order to obtain random self-reducibility, it is only by a small factor.

4.6 $H = \left\{ \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \right\}$

As mentioned in [11], this case is the split Cartan level structure case. Here H contains every scalar matrix, and there is a matrix for every possible determinant. This level structure applies to FESTA [6]. Therefore, we can apply our results.

We have that $|H| = \varphi(N)^2$. Let $N = \prod_{k=1}^{t} \rho_k^{\alpha_k}$ and $d = \prod_{i=1}^{k} \ell_i^{e_i}$. Applying our results, we have that Problem 2.33 is randomly self-reducible as long as

$$\frac{12d\varphi(N)^2}{p\left(\prod_{k=1}^{t} \rho_k^{4(\alpha_k-1)}(\rho_k^2-1)(\rho_k^2-\rho_k)\right)\prod_{i=1}^{k}(e_i+1)^2}$$

is not negligible.

Similarly to the case in Subsection 4.5, the above formula is too small to be applicable to current FESTA parameters. As a rough estimate, in order to get a clean random self-reduction, the degree d of the secret isogeny should be around four times larger than N. For an example of parameter set for which the formula is useful, let $p = 2^a 3^b - 1$, $d = 3^{4b}$ and $N = 2^a$. The formula becomes:

$$\frac{12 \times 3^{4b} 2^{2a-2}}{(2^a 3^b - 1)\left(2^{4(a-1)}(2^2-1)(2^2-2)\right)(b+1)^2} \approx \frac{3^{3b}}{2^{3a}}$$

If $2^a \approx 3^b$, then the problem is randomly self-reducible. This is similar to the previous case, with a efficiency loss factor of about 4 instead of 3. For example, we could choose $p = 2^{216} \times 3^{137} - 1$, $N = 2^{216}$ and $d = 3^{548}$. In this case, the formula above is approximately equal to 2.84×10^{-4}. Hence, the problem is randomly self-reducible for this parameter set.

5 Conclusion

Using the results in this paper, we find that there are families of SIDH variants for which the problem of recovering the secret key can be shown to be randomly self-reducible, providing support for the strategy of choosing a random starting curve for these schemes. In particular, our results hold for Borel and Cartan level structures, linked to zero-knowledge proofs (such as [10,15,3]) and FESTA respectively.

In cases where our theorems do not imply random self-reducibility, such as for M-SIDH, we have some plausibility arguments for why random self-reducibility might not hold, since the associated isogeny graphs are either not connected, or have an extra trivial eigenvalue and eigenvector. Of course, this conclusion does not rule out the possibility of finding a reduction using another method.

The most direct avenue for future work would be to remove the conditions on p and N modulo 12. In practice, for any supersingular isogeny graph, there are at most two vertices that do not act like an undetected graph. As it is an exponentially small fraction of the total number of vertices in the graph, it

would be surprising if they alone could affect the random self-reducibility of the problem. Another direction for future work would be to improve the efficiency of our reduction. For our results, we only use the fact that the graphs we are working with are Ramanujan, giving us an upper bound on the second largest eigenvalue. One could, in theory, obtain better reductions by finding smaller upper bounds on some eigenvalues and applying them in the proof of Theorem 3.3.

Acknowledgments. The authors acknowledge support of the NSERC Alliance Consortia Quantum Grant ALLRP 578463–2022, the NSERC Discovery Grant program, the Institut Henri Poincaré (UAR 839 CNRS-Sorbonne Université), and LabEx CARMIN (ANR-10-LABX-59-01)

References

1. Abramowitz, M., Stegun, I.A.: Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables. Dover, New York, ninth dover printing, tenth gpo printing edn. (1964)
2. Arpin, S.: Adding level structure to supersingular elliptic curve isogeny graphs (2024), https://arxiv.org/abs/2203.03531
3. Basso, A., Codogni, G., Connolly, D., De Feo, L., Fouotsa, T.B., Lido, G.M., Morrison, T., Panny, L., Patranabis, S., Wesolowski, B.: Supersingular curves you can trust. In: Hazay, C., Stam, M. (eds.) Advances in Cryptology — EUROCRYPT 2023. pp. 405–437. Springer Nature Switzerland, Cham (2023)
4. Basso, A., Dartois, P., Feo, L.D., Leroux, A., Maino, L., Pope, G., Robert, D., Wesolowski, B.: Sqisign2d–west. In: Chung, K.M., Sasaki, Y. (eds.) Advances in Cryptology – ASIACRYPT 2024. pp. 339–370. Springer Nature Singapore, Singapore (2025)
5. Basso, A., Fouotsa, T.B.: New SIDH countermeasures for a more efficient key exchange. In: Guo, J., Steinfeld, R. (eds.) Advances in Cryptology — ASIACRYPT 2023. pp. 208–233. Springer Nature Singapore, Singapore (2023)
6. Basso, A., Maino, L., Pope, G.: FESTA: Fast encryption from supersingular torsion attacks. In: Guo, J., Steinfeld, R. (eds.) Advances in Cryptology — ASIACRYPT 2023. pp. 98–126. Springer Nature Singapore, Singapore (2023)
7. Castryck, W., Decru, T.: An efficient key recovery attack on SIDH. In: Hazay, C., Stam, M. (eds.) Advances in Cryptology — EUROCRYPT 2023. pp. 423–447. Springer Nature Switzerland, Cham (2023)
8. Castryck, W., Vercauteren, F.: A polynomial time attack on instances of M-SIDH and FESTA. In: Guo, J., Steinfeld, R. (eds.) Advances in Cryptology — ASIACRYPT 2023. pp. 127–156. Springer Nature Singapore, Singapore (2023)
9. Codogni, G., Lido, G.: Spectral theory of isogeny graphs (2024), https://arxiv.org/abs/2308.13913
10. De Feo, L., Dobson, S., Galbraith, S.D., Zobernig, L.: SIDH proof of knowledge. In: Advances in Cryptology – ASIACRYPT 2022: 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5–9, 2022, Proceedings, Part II. p. 310–339. Springer-Verlag, Berlin, Heidelberg (2023). https://doi.org/10.1007/978-3-031-22966-4_11
11. De Feo, L., Fouotsa, T.B., Panny, L.: Isogeny problems with level structure. In: Joye, M., Leander, G. (eds.) Advances in Cryptology — EUROCRYPT 2024. pp. 181–204. Springer Nature Switzerland, Cham (2024)

12. Fouotsa, T.B., Moriya, T., Petit, C.: M-SIDH and MD-SIDH: Countering sidh attacks by masking information. In: Hazay, C., Stam, M. (eds.) Advances in Cryptology — EUROCRYPT 2023. pp. 282–309. Springer Nature Switzerland, Cham (2023)
13. Han, J.: The general linear group over a ring. Bulletin of the Korean Mathematical Society **43** (08 2006). https://doi.org/10.4134/BKMS.2006.43.3.619
14. Horn, R., Johnson, C.: Matrix Analysis. Cambridge University Press (2012), https://books.google.ca/books?id=O7sgAwAAQBAJ
15. Jao, D., De Feo, L.: Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In: Yang, B.Y. (ed.) Post-Quantum Cryptography. pp. 19–34. Springer Berlin Heidelberg, Berlin, Heidelberg (2011)
16. Jao, D., Miller, S.D., Venkatesan, R.: Expander graphs based on GRH with an application to elliptic curve cryptography. Journal of Number Theory **129**(6), 1491–1504 (Jun 2009). https://doi.org/10.1016/j.jnt.2008.11.006
17. Kawashima, T., Takashima, K., Aikawa, Y., Takagi, T.: An efficient authenticated key exchange from random self-reducibility on CSIDH. In: Information Security and Cryptology – ICISC 2020: 23rd International Conference, Seoul, South Korea, December 2–4, 2020, Proceedings. p. 58–84. Springer-Verlag, Berlin, Heidelberg (2020). https://doi.org/10.1007/978-3-030-68890-5_4
18. Maino, L., Martindale, C., Panny, L., Pope, G., Wesolowski, B.: A direct key recovery attack on SIDH. In: Hazay, C., Stam, M. (eds.) Advances in Cryptology — EUROCRYPT 2023. pp. 448–471. Springer Nature Switzerland, Cham (2023)
19. Mestre, J.F.: La méthode des graphes. exemples et applications. Proceedings of the international conference on class numbers and fundamental units of algebraic number fields pp. 217–242 (1986)
20. Petit, C.: Faster algorithms for isogeny problems using torsion point images. In: Takagi, T., Peyrin, T. (eds.) Advances in Cryptology — ASIACRYPT 2017. pp. 330–353. Springer International Publishing, Cham (2017)
21. Pizer, A.K.: Ramanujan graphs and Hecke operators. Bulletin (New Series) of the American Mathematical Society **23**(1), 127–137 (1990). https://doi.org/bams/1183555725, https://doi.org/
22. Robert, D.: Breaking SIDH in polynomial time. In: Hazay, C., Stam, M. (eds.) Advances in Cryptology — EUROCRYPT 2023. pp. 472–503. Springer Nature Switzerland, Cham (2023)
23. Robert, D.: On the efficient representation of isogenies (a survey). Cryptology ePrint Archive, Paper 2024/1071 (2024), https://eprint.iacr.org/2024/1071
24. Sardari, N.T.: Diameter of Ramanujan graphs and random Cayley graphs. Combinatorica **39**, 427–446 (2015)
25. Silverman, J.H.: The Arithmetic of Elliptic Curves. Graduate texts in mathematics, Springer, Dordrecht (2009). https://doi.org/10.1007/978-0-387-09494-6