Genus Two Isogeny Cryptography

E.V. Flynn[1] and Yan Bo Ti[2]

[1] Mathematical Institute, Oxford University, UK. flynn@maths.ox.ac.uk
[2] Mathematics Department, University of Auckland, NZ. yanbo.ti@gmail.com

Abstract. We study (ℓ, ℓ)-isogeny graphs of principally polarised supersingular abelian surfaces (PPSSAS). The (ℓ, ℓ)-isogeny graph has cycles of small length that can be used to break the collision resistance assumption of the genus two isogeny hash function suggested by Takashima. Algorithms for computing $(2, 2)$-isogenies on the level of Jacobians and $(3, 3)$-isogenies on the level of Kummers are used to develop a genus two version of the supersingular isogeny Diffie–Hellman protocol of Jao and de Feo. The genus two isogeny Diffie–Hellman protocol achieves the same level of security as SIDH but uses a prime with a third of the bit length.

Keywords: Post-quantum cryptography · Isogeny-based cryptography · Cryptanalysis · Key exchange · Hash function

1 Introduction

Isogeny-based cryptography involves the study of isogenies between abelian varieties. The first proposal was an unpublished manuscript of Couveignes [6] that outlined a key-exchange algorithm set in the isogeny graph of elliptic curves. This was rediscovered by Rostovtsev and Stolbunov [18]. A hash function was developed by Charles, Goren and Lauter [4] that uses the input to the hash to generate a path in the isogeny graph and outputs the end point of the path. Next in the line of invention is the Jao–de Feo cryptosystem [12] which relies on the difficulty of finding isogenies with a given degree between supersingular elliptic curves. A key exchange protocol, called the Supersingular Isogeny Diffie–Hellman key exchange (SIDH), based on this hard problem, was proposed in the same paper. The authors proposed working with 2-isogenies and 3-isogenies for efficiency.

Elliptic curves are principally polarised abelian varieties of dimension one, hence we can turn to principally polarised abelian varieties of higher dimension when looking to generalise isogeny-based cryptosystems. As noted by Takashima elliptic curves have three 2-isogenies but abelian surfaces (abelian varieties of dimension 2) have fifteen $(2, 2)$-isogenies. Hence, this motivates the use of abelian surfaces for use in these cryptosystems.

In this work, we will focus on principally polarised supersingular abelian varieties of dimension two, which we call principally polarised supersingular abelian surfaces (PPSSAS) and consider their application to cryptography. The two challenges before us are: to understand the isogeny graphs of PPSSAS, and to have efficient algorithms to compute isogenies between principally polarised abelian surfaces (PPAS) in general.

In this work, we will examine the structure of the (ℓ, ℓ)-isogeny graph of PPSSAS and show that the genus two hash mentioned above is no longer collision resistant. This will be presented in §2. The realisation of the genus two version of SIDH will make up §3 and we will examine its security in §4.

Due to space restrictions, we will assume knowledge of abelian varieties and some of their properties. Assiduous readers can refer to [16] and [15] for definitions and background.

Acknowledgements

The authors would like to thank Steven Galbraith, Lukas Zobernig, Chloe Martindale, Luca de Feo and David Kohel for enlightening discussions. In particular, we thank Steven for the idea of the cryptanalysis of the hash function. We also thank the reviewers for suggesting improvements to the paper, most of which we have tried to include.

2 PPSSAS Graph

Let p and ℓ be distinct primes. In this section, we will examine the structure of the graph $\mathcal{G}_{p,\ell}$, where the vertices are isomorphism classes of PPSSAS over $\overline{\mathbb{F}}_p$, and edges are present between two vertices if they are (ℓ, ℓ)-isogenous. We will see that the PPSSAS graph has a regular and repeating substructure that we can identify. This can be seen explicitly in the subgraphs of the full isogeny graph presented in Appendix A.

2.1 Morphisms to Subgroups

One of the key tools in studying isogenies between abelian varieties is the correspondence between subgroups and isogenies. This subsection explains the properties a subgroup needs to have in order to correspond to an appropriate isogeny.

The first result allows us to restrict our attention to Jacobians of hyperelliptic curves of genus two or some reducible product of two elliptic curves.

Theorem 1. *If $A/\overline{\mathbb{F}}_p$ is a PPAS, then $A \cong J_H$ for some smooth (hyperelliptic) genus two curve H, or $A \cong E_1 \times E_2$ where E_i are elliptic curves.*

Proof. Use [11, Theorem 3.1] which says that A is isomorphic over $\mathbb{F}_{p^n}$ (for some n) to the two cases in the theorem, or to the restriction of scalars of a polarized elliptic curve over a quadratic extension of $\mathbb{F}_{p^n}$. Since we are working over $\overline{\mathbb{F}}_p$, the latter case is absorbed into the second case. □

Given an abelian variety A, the *dual variety* $A^\vee$ exists and is unique up to isomorphism. An ample divisor $\mathcal{L}$ of A defines an isogeny $\phi_{\mathcal{L}} : A \to A^\vee$ known as the *polarisation* of A. If the polarisation is an isomorphism, then we say that it is *principal*.

There is a non-degenerate alternating pairing, known as the *Weil pairing*, on an abelian variety A over k

$$e_m : A[m](\overline{k}) \times A^\vee[m](\overline{k}) \to \overline{k}^* ,$$

where $A[m]$ is the m-torsion subgroup of A.

Being non-degenerate, the Weil pairing is non-trivial on the entire torsion subgroup. But there are subgroups in the torsion subgroup onto which the Weil pairing acts trivially when restricted. We give them a special name:

Definition 1. *A subgroup S of $A[m]$ is* proper *if $A[n] \nsubseteq S$ for any $1 < n \leq m$.*

Let A be an abelian variety over $\overline{\mathbb{F}}_p$, and let m be a positive integer co-prime with p. We say a proper subgroup S of $A[m]$ is maximal m-isotropic *if*

(1) the m-Weil pairing on $A[m]$ restricts trivially to S, and
(2) S is not properly contained in any other subgroup of $A[m]$ satisfying (1).

We call the first condition the *isotropic condition.* Note that the definition for a maximal isotropic subgroup does not include kernels of isogenies that factor through the multiplication-by-n map.

The following result then illustrates the preservation of principal polarisations under isogenies whose kernels are isotropic.

Proposition 1. *Let H be a hyperelliptic curve of genus two over $\mathbb{F}_q$. Let K be a finite, proper, $\mathbb{F}_q$-rational subgroup of $J_H(\mathbb{F}_q)$. There exists a PPAS A over $\mathbb{F}_q$, and an isogeny $\phi : J_H \to A$ with kernel K, if and only if K is a maximal m-isotropic subgroup of $J_H[m]$ for some positive integer m.*

Proof. The quotient $J_H \to J_H/K$ always exists as an isogeny between abelian varieties [19, III.3.12]. Since J_H is the Jacobian of a hyperelliptic curve, it has a principal polarisation λ. Now consider the polarisation $\mu = [\deg \phi] \circ \lambda$ on J_H, then we certainly have $K = \ker \phi \subseteq \ker \mu$, and since K is isotropic, we use [15, Theorem 16.8] to get a polarisation λ' on J_H/K. Using [15, Remark 16.9], we have that $\deg \lambda' = 1$ and so J_H/K is a PPAS.

Furthermore, by Theorem 1, we have that A is the Jacobian of a hyperelliptic curve of genus two or a product of two elliptic curves. □

Using the results above, we can focus on the type of subgroups of the torsion group that correspond to the isogenies we would like to investigate. We will denote by C_n the cyclic group of order n.

Lemma 1. *Let A be a PPAS. If K is a maximal ℓ^n-isotropic subgroup, then it cannot be cyclic.*

Proof. Suppose that K is cyclic, then K is trivial on the pairing from the alternating property. It can then be shown that K is contained in $C_{\ell^n}^2$, which is also isotropic and so K cannot be maximal. □

Proposition 2. *Let A be a PPAS. Then the maximal ℓ^n-isotropic subgroups of $A[\ell^n]$ are isomorphic to*

$$C_{\ell^n} \times C_{\ell^n} \quad \text{or} \quad C_{\ell^n} \times C_{\ell^{n-k}} \times C_{\ell^k}$$

where $1 \leq k \leq \lfloor n/2 \rfloor$.

Proof. We see, from Lemma 1 and the fact that maximal isotropic subgroups must be proper, that K must have rank 2 or 3. Suppose that K has rank 2, then it can be shown that to be maximal, K must have the structure $C_{\ell^n} \times C_{\ell^n}$ by repeated inclusion.

Let $C_{\ell^a} \times C_{\ell^b} \times C_{\ell^c} \times C_{\ell^d}$ be a subgroup of $A[\ell^n]$. To simplify notation, we write this as $[a, b, c, d]$. Without loss of generality, we can take $a \geq b \geq c \geq d$. Then we have that the dual is $[n-a, n-b, n-c, n-d]$ (since the composition with the original isogeny is multiplication-by-ℓ^n) and $n - a \leq n - b \leq n - c \leq n - d$. Hence to get the symmetry as specified by [16, pg. 143, Thm. 1], we must have that $n - a = d$ and $n - b = c$. Since we must have that one of the indices is zero, we take $d = 0$ and the result follows. □

This result narrows down the subgroups that we need to study in order to study sequences of (ℓ, ℓ)-isogenies between PPAS.

2.2 Number of neighbours in an (ℓ, ℓ)-isogeny graph

In this section, we will consider the structure of an (ℓ, ℓ)-isogeny graph, $\mathcal{G}_{p,\ell}$. We do so by computing the number of neighbours that each vertex is connected to. Also, we will see that the number of paths between each vertex can vary according to the structure of the kernel.

We approach this question by choosing an arbitrary PPAS and considering isogenies emanating from this surface. Then the nascent isogeny graph is a rooted graph at the chosen surface. The first result counts the number of elements n steps from the root.

Theorem 2. *Let A be a PPAS, ℓ be a prime different from p and $n > 2$. Then the number of ℓ^n-maximal isotropic subgroup of $A[\ell^n]$ is*

$$\ell^{2n-3}(\ell^2 + 1)(\ell + 1)\left(\ell^n + \ell\frac{\ell^{n-2} - 1}{\ell - 1} + 1\right)$$

if n is even, and

$$\ell^{2n-3}(\ell^2 + 1)(\ell + 1)\left(\ell^n + \frac{\ell^{n-1} - 1}{\ell - 1}\right)$$

if n is odd.

The proof of the theorem follows by summing the number of maximal isotropic subgroups which is given in the following proposition.

Proposition 3. *Let A be a PPAS. Let $N(a,b,c)$ be the number of maximal isotropic subgroups of A isomorphic to $C_{\ell^a} \times C_{\ell^b} \times C_{\ell^c}$. Then*

1. $N(n, n-a, a) = \ell^{3n-2a-4}(\ell^2+1)(\ell+1)^2$*, where* $1 \leq a < n/2$*;*
2. $N(n,n,0) = \ell^{3n-3}(\ell^2+1)(\ell+1)$*;*
3. $N(2k,k,k) = \ell^{4k-3}(\ell^2+1)(\ell+1)$*.*

Proof. We will prove this for the second case. Note that this is equivalent to finding a subgroup isomorphic to $C_{\ell^n}^2$ in $A[\ell^n] \cong C_{\ell^n}^4$ which satisfies the isotropic condition.

So we need to find 2 elements in $C_{\ell^n}^4$ that have full order, are isotropic under the Weil pairing and generate subgroups with trivial intersection. To make things concrete, let $\langle P_1, \ldots, P_4 \rangle = C_{\ell^n}^4$. Let us pick the first element $A \in C_{\ell^n}^4$. This involves picking a full order element in $C_{\ell^n}^4$ for which we have $\ell^{4n} - \ell^{4n-4}$ choices. Let $A = \sum [a_i] P_i$.

To pick the second element $B \in C_{\ell^n}^4$, we need to pick a full order element but also ensure that B is isotropic to A under the Weil pairing. If we write $B = \sum [b_i] P_i$, then we require that

$$\begin{aligned} e_\ell(A,B) &= e_\ell(P_1,P_2)^{a_1b_2 - a_2b_1} \cdot e_\ell(P_1,P_3)^{a_1b_3-a_3b_1} \cdot e_\ell(P_1,P_4)^{a_1b_4-a_4b_1} \\ &\quad \cdot e_\ell(P_2,P_3)^{a_2b_3-a_3b_2} \cdot e_\ell(P_2,P_4)^{a_2b_4-a_4b_2} \cdot e_\ell(P_3,P_4)^{a_3b_4-a_4b_3} \\ &= 1\,. \end{aligned}$$

But this is a linear condition on the selection of the b_i's. Thus this gives us $\ell^{3n} - \ell^{3n-3}$ choices[1]. But we need to pick B such that $B \notin \langle A \rangle$. Given that B has full order, we need to avoid $(\ell-1)\ell^{3(n-1)}$ elements. Hence the total number of choices for B is

$$\ell^{3n} - \ell^{3(n-1)} - (\ell-1)\ell^{3(n-1)}\,.$$

Now, we need to divide the choices we have for A and B by the number of generating pairs in a subgroup $C_{\ell^n}^2$. The total number of generating pairs is $(\ell^{2n} - \ell^{2(n-1)})(\ell^{2n} - \ell^{2(n-1)} - (\ell-1)\ell^{2(n-1)})$. Hence the total number of maximal isotropic $C_{\ell^n}^2$ subgroups of $C_{\ell^n}^4$ is

$$\frac{(\ell^{4n} - \ell^{4n-4})(\ell^{3n} - \ell^{3(n-1)} - (\ell-1)\ell^{3(n-1)})}{(\ell^{2n} - \ell^{2(n-1)})(\ell^{2n} - \ell^{2(n-1)} - (\ell-1)\ell^{2(n-1)})} = \ell^{3n-3}(\ell^2+1)(\ell+1)\,.$$

The other two cases are proved similarly. □

[1] To see this, note that each $e_\ell(P_i,P_j) = \mu^{\alpha_{i,j}}$, where μ is an ℓ-root of unity and $\alpha_{i,j}$ is some non-zero integer. We can express the isotropic condition as

$$b_4(\alpha_{1,4}a_1 + \alpha_{2,4}a_2 + \alpha_{3,4}a_3) \equiv \begin{array}{l} \alpha_{1,2}(a_2b_1 - a_1b_2) + \alpha_{1,3}(a_3b_1 - a_1b_3) \\ +\alpha_{2,3}(a_3b_2 - a_2b_3) + \alpha_{1,4}a_4b_1 \\ +\alpha_{2,4}a_4b_2 + \alpha_{3,4}a_4b_3 \end{array} \pmod{\ell}\,.$$

In the case where $(\alpha_{1,4}a_1 + \alpha_{2,4}a_2 + \alpha_{3,4}a_3 \not\equiv 0$, we have free choices for b_1, b_2, b_3 (not all divisible by ℓ) and so have $\ell^{3n} - \ell^{3n-3}$ choices.

Now, suppose we have an isogeny which has a maximal isotropic kernel K with order ℓ^{2n}, then we can decompose this isogeny into a sequence of n (ℓ, ℓ)-isogenies:

$$A_0 \xrightarrow{\phi_1} A_1 \xrightarrow{\phi_2} A_2 \xrightarrow{\phi_3} \dots \xrightarrow{\phi_n} A_0/K\,.$$

As mentioned in the introduction, this decomposition of isogenies is non-unique. This arises from kernels whose structure allows for more than one subgroup isomorphic to $C_\ell \times C_\ell$. The key observation is that these subgroups form the kernels of ϕ_1. In that spirit, the next two lemmata will give properties for the kernels of the first isogeny.

Lemma 2. *Let A be a PPAS. Let K be a maximal isotropic subgroup of $A[\ell^n]$ which is isomorphic to $C_{\ell^n} \times C_{\ell^{n-a}} \times C_{\ell^a}$ for some $a \geq 0$. Let $\langle P, Q, R\rangle = K$ such that P, Q, R have orders $\ell^n, \ell^{n-a}, \ell^a$ respectively.*

(1) Let $P_i, Q_i, R_i \in A_i$ be elements mapped from $P = P_0, Q = Q_0, R = R_0$. Then $[\ell^{n-i-1}]P_i \in \ker \phi_{i+1}$ for all $i \geq 0$.

(2) The first (ℓ, ℓ)-isogeny must have kernel

$$\langle [\ell^{n-1}]P, [\ell^{n-a-1}]Q + [k][\ell^{a-1}]R\rangle \quad \text{for } 0 \leq k \leq \ell-1, \quad \text{or} \quad \langle [\ell^{n-1}]P, [\ell^{a-1}]R\rangle\,.$$

Proof. (1) One can show by contradiction that if there is a kernel not containing P_i, then we will have cyclic kernels, which cannot be a kernel of a (ℓ, ℓ)-isogeny by Lemma 1.

Next, let $P' \in \langle P_i\rangle$, $Q' \in \langle Q_i\rangle$, and $R' \in \langle R_i\rangle$ such that P', Q', R' all have order ℓ. Then kernels cannot be of the form $P' + Q', P' + R', Q' + R'$. Indeed, it can be shown by examining the pairing $e_\ell(P' + Q', P' + R')$ to see that one either obtains a cyclic kernel, or that the subgroup above is not isotropic.

(2) We have from the first part that $[\ell^{n-1}]P$ must be a generator of the group. The second generator must be chosen from the remaining points of order ℓ. By the isotropic condition of K, we have that they are all isotropic on the pairing as well.

□

Lemma 3. *Let $G \cong C_{\ell^n} \times C_{\ell^{n-a}} \times C_{\ell^a}$ and H be abelian groups. Let*

$$\langle P\rangle \cong C_{\ell^n}, \quad \langle Q\rangle \cong C_{\ell^{n-a}}, \quad \langle R\rangle \cong C_{\ell^a}$$

be subgroups of G with trivial intersections. If $\phi : G \to H$ is a group homomorphism, with

$$\ker \phi = \left\langle [\ell^{n-1}]P, [\ell^{n-a-1}]Q + [k][\ell^{a-1}]R\right\rangle$$

for $1 \leq k \leq \ell - 1$ and $a \leq n/2$, then $H \cong C_{\ell^{n-1}} \times C_{\ell^{n-a}} \times C_{\ell^{a-1}}$.

Proof. We have that $\phi(P)$ has order ℓ^{n-1} and Q has order ℓ^{n-a}, since $[\ell^{n-a-1}]Q \notin \ker \phi$. Since the order of the kernel is ℓ^2, we must have that $H \cong C_{\ell^{n-1}} \times C_{\ell^{n-a}} \times C_{\ell^{a-1}}$. □

We can now study the different isogenies that exist between two vertices on the graph. In particular, we will be counting the number of different paths between any two vertices on the graph.

We will examine the base cases first, where there is only one path between two vertices, or where two vertices are separated by two (ℓ, ℓ)-isogenies.

Proposition 4. *Let A be a PPAS, and let $K \cong (C_{\ell^n} \times C_{\ell^{n-a}} \times C_{\ell^a})$. Let $P(n, a)$ be the number of paths from A to A/K. Then*

1. $P(n, 0) = 1$ *for all* n;
2. $P(2, 1) = \ell + 1$.

Proof. 1. Since kernels of (ℓ, ℓ)-isogenies cannot be cyclic, the only possible subgroup of order ℓ^2 of $C_{\ell^n} \times C_{\ell^n}$ is $C_\ell \times C_\ell$, and there is only one choice for this subgroup.

2. Let $K = C_{\ell^2} \times C_\ell \times C_\ell$. Then from Lemma 2 (and using its notation) we must have that the first isogeny has kernel

$$\langle [\ell]P, Q + [k]R \rangle \quad \text{for } 0 \leq k \leq \ell - 1, \quad \text{or} \quad \langle [\ell]P, R \rangle .$$

There are $\ell+1$ choices for the first kernel. Thereafter, there is only one choice for the second kernel and so we have a total of $\ell + 1$ paths.

□

Now, we can prove the general case.

Proposition 5. *Using the notation above, where $P(n, a)$ is the number of paths in a $(C_{\ell^n} \times C_{\ell^{n-a}} \times C_{\ell^a})$-isogeny. Then $P(n, a)$ satisfies the following recursive equation:*

$$P(n, a) = 2P(n - 1, a - 1) + (\ell - 1)P(n - 1, a) ,$$

where $1 \leq a < n/2$, and with the following boundary conditions:

$$P(n, 0) = 1, \quad P(2, 1) = \ell + 1 .$$

Proof. We will prove this by induction. The base cases of the induction steps are easy and the boundary conditions follow from Proposition 4. We will show the induction step.

Let us suppose that the recursive formula holds for $P(n-1, a-1)$ and $P(n-1, a)$. Now, suppose that our kernel is isomorphic to $C_{\ell^n} \times C_{\ell^{n-a}} \times C_{\ell^a}$. Since each (ℓ, ℓ)-isogeny has a kernel of the form $C_\ell \times C_\ell$, we have, from Lemma 2(2), that the first isogeny must have a kernel of the form

$$\langle [\ell^{n-1}]P, [\ell^{n-a-1}]Q + [k][\ell^{a-1}]R \rangle \quad \text{for } 0 \leq k \leq \ell - 1, \quad \text{or} \quad \langle [\ell^{n-1}]P, [\ell^{a-1}]R \rangle .$$

It is clear that if the kernel is given by

$$\langle [\ell^{n-1}]P, [\ell^{n-a-1}]Q \rangle \quad \text{or} \quad \langle [\ell^{n-1}]P, [\ell^{a-1}]R \rangle ,$$

then the residual kernel will be of the form

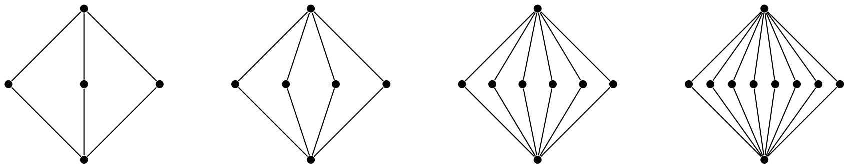
$$C_{\ell^{n-1}} \times C_{\ell^{n-a-1}} \times C_{\ell^a} \text{ or } C_{\ell^{n-1}} \times C_{\ell^{n-a}} \times C_{\ell^{a-1}}$$

respectively. Otherwise, if the first kernel has the form

$$\langle [\ell^{n-1}]P, [\ell^{n-a-1}]Q + [k][\ell^{a-1}]R \rangle \quad \text{for } 1 \leq k \leq \ell - 1,$$

the residual kernel will be of the form $C_{\ell^{n-1}} \times C_{\ell^{n-a}} \times C_{\ell^{a-1}}$ by Lemma 3. Hence we are done. □

Proposition 4 actually shows us the different paths that can exist between vertices in the graph. In particular, for kernels with rank 2, there can only be a single path between the domain and codomain. However, for kernels with rank 3, there can be a multitude of paths that exist between the domain and codomain. It can be seen that the following shapes (diamonds) are the basic paths drawn out by kernels with group structure $C_{\ell^2} \times C_\ell \times C_\ell$ for different ℓ's.



$\ell = 2$ $\ell = 3$ $\ell = 5$ $\ell = 7$

The non-uniqueness of these paths can be seen more explicitly in the example in Appendix A, where the kernel has order 256. Also in Appendix A, we will see how the diamonds fit together in the isogeny graph.

2.3 Cryptanalysis of the Isogeny-based Hash Functions

The CGL hash function performs a random walk on the supersingular elliptic curve 2-isogeny graph. From each supersingular elliptic curve, there are three 2-isogenies emanating from that curve. The algorithm receives a binary string as input and returns an $\mathbb{F}_{p^2}$ value as output. It does so by taking a fixed base curve, discards one of the three isogenies (how this is done will not be of consequence in this discussion), and uses the first bit of the input as a choice between the remaining two isogenies. In the subsequent step, the algorithm uses the second bit to choose between the only two isogenies that does not lead back to the base curve (this is termed "no back-tracking"). Note that in this discussion, we have not mentioned how one can deterministically choose one isogeny over the other given a fixed bit, but there is a variety of ways one can "order" the isogenies. Readers are encouraged to refer to the original paper for more details.

In the genus two case of the hash function, due to the additional isogenies available to a single vertex (15 as opposed to 3), it is hoped that one can achieve a higher security level with a smaller number of steps. In [21] Takashima outlined an algorithm for obtaining a sequence of $(2,2)$-isogenies without backtracking. He also implicitly suggested the generalisation of the above hash function to genus two. The genus two version of the CGL hash uses the input bits to traverse the $(2,2)$-isogeny graph of PPSSAS. The algorithm begins at a pre-chosen PPSSAS and begins a walk based on the binary input to the algorithm. The walk on the graph is similar to the original CGL hash with a difference of an increased number of paths at each iteration.

Genus Two Hash Collisions One of the main results of [4] is the proof that the CGL hash function is collision resistant. The vague intuition for this is that the supersingular elliptic curve isogeny graph is locally tree-like, i.e. there are no small cycles in a small enough subgraph. This assumption fails in the genus two case as pictured above, any diamond configuration leads to a collision in the hash. An attacker can find two pairs of bits so that the walks collide. Using the diamond of $\ell = 2$ as an example, where a hash is performed by walking along the left-most path. An attacker, with the knowledge that the hash has traversed through a diamond, will be able to choose either the middle path or the right-most path to achieve a collision.

In terms of endomorphisms, the collision resistance in the CGL hash is achieved by the lack of endomorphisms of degree 2^k, where k is small, in the graph. However, as we have seen in the previous section, we might be able to find endomorphism of degree 16 (or cycles of length 4) after 2 iterations of the genus two hash.

3 Genus Two SIDH Cryptosystem

In this section, we will construct the key exchange protocol for genus two. The scheme presented here follows the original scheme closely. Before presenting the scheme, we will review two algorithms used to select a base PPSSAS and select a key from the keyspace. We will also look briefly at the isogeny algorithms employed in the scheme.

We note that the `MAGMA` implementation of the scheme is extremely slow. An example is presented in Appendix B.

3.1 Selecting a Base Hyperelliptic Curve

Similar to the SIDH case, we pick primes of the form $p = 2^n \cdot 3^m \cdot f - 1$.

We consider a base hyperelliptic curve given by

$$H : y^2 = x^6 + 1\,.$$

It can be shown that the Jacobian of H is supersingular since it is the double cover of the supersingular elliptic curve $y^2 = x^3 + 1$, which is supersingular over $\mathbb{F}_p$, since $p \equiv 2 \pmod 3$. We then take a random sequence of Richelot isogenies to obtain a random PPSSAS.

3.2 Selection of Secrets

Our aim is to use scalars to encode the secret kernel to be used by the two parties of the key exchange as this allows for a compact representation of the secret.

Firstly, let $H/\mathbb{F}_q$ be a hyperelliptic curve of genus two and let J_H be its Jacobian. The secret kernels will be maximal isotropic subgroups of $J_H[\ell^n]$ of order ℓ^{2n}. As seen in §2, the kernels will have structure $C_{\ell^n} \times C_{\ell^{n-k}} \times C_{\ell^k}$, where $0 \leq k < n/2$. Hence they should be generated by three points: Q_1, Q_2 and Q_3. Furthermore, to fulfil the condition of isotropy, we also require that the generators satisfy

$$e_{\ell^n}(Q_1, Q_2) = e_{\ell^n}(Q_1, Q_3) = e_{\ell^n}(Q_2, Q_3) = 1\,.$$

Our approach is summarised by the following steps:

Pre-computation:

Step 1: Find generators for $J_H[\ell^n]$. Name them P_1, P_2, P_3, P_4.

Step 2: Find the values $\alpha_{i,j}$ such that $e_{\ell^n}(P_i, P_j) = e_{\ell^n}(P_1, P_2)^{\alpha_{i,j}}$.

Secret selection:

Step 3: Pick some $r_1, r_2, r_3, r_4 \in [1, \ldots, \ell^n - 1]^4$ such that they are not simultaneously divisible by ℓ.

Step 4: Pick a random[2] $0 \leq k < n/2$ and compute s_1, s_2, s_3, s_4 and t_1, t_2, t_3, t_4 by solving the two linear congruences

$$\begin{pmatrix} r_1 s_2 - r_2 s_1 + \alpha_{1,3}(r_1 s_3 - r_3 s_1) \\ +\alpha_{1,4}(r_1 s_4 - r_4 s_1) + \alpha_{2,3}(r_2 s_3 - r_3 s_2) \\ +\alpha_{2,4}(r_2 s_4 - r_4 s_2) + \alpha_{3,4}(r_3 s_4 - r_4 s_3) \end{pmatrix} \equiv 0 \mod \ell^k$$

$$\begin{pmatrix} r_1 t_2 - r_2 t_1 + \alpha_{1,3}(r_1 t_3 - r_3 t_1) \\ +\alpha_{1,4}(r_1 t_4 - r_4 t_1) + \alpha_{2,3}(r_2 t_3 - r_3 t_2) \\ +\alpha_{2,4}(r_2 t_4 - r_4 t_2) + \alpha_{3,4}(r_3 t_4 - r_4 t_3) \end{pmatrix} \equiv 0 \mod \ell^{n-k}$$

Step 5: Output $(s_1, \ldots, s_4, r_1, \ldots, r_4, t_1, \ldots, t_4)$ as the secret scalars which will give the generators of the kernel:

$$Q_1 = \sum [s_i] P_i, \quad Q_2 = \sum [r_i] P_i, \quad Q_3 = \sum [t_i] P_i\,.$$

Remark 1. Note the following:

(i) Step 1 can be performed using standard group theoretic algorithms.

(ii) Step 2 performs discrete logarithm computations modulo a 2 and 3-smooth modulus and so is extremely efficient by using the Silver–Pohlig–Hellman algorithm [8, §13.2].

(iii) In Step 4, we pick a random solution in the solution space for r_i and t_i. It can be shown that this ensures that the isotropic condition is upheld.

[2] This will not be a uniformly random choice if one wants to sample the entire keyspace.

3.3 Isogeny Algorithms

Computing an ℓ-isogeny between elliptic curves can be done with a complexity of $O(\ell)$. The general method to compute the codomains of this isogeny or to map points under the isogeny is to use Vélu's formula [25]. However, the efficient computation of arbitrary isogenies between abelian varieties of dimension greater than 1 is lacking. Here, we will present algorithms for computing the codomains of $(2,2)$ and $(3,3)$-isogenies and show how we can map subgroups under these isogenies. The speed-ups come from the use of simpler representations in the computation: the use of hyperelliptic curves in the (2,2) case and the use of Kummer surfaces in the (3,3).

Richelot Isogenies We will use Richelot isogenies to perform our $(2,2)$-isogenies as is standard in the literature. Richelot isogenies are relatively well-understood and have been implemented in various computational algebra programs. Useful references for Richelot isogenies are [20,3,1].

Note that Richelot isogenies operate on the level of hyperelliptic curves in the sense that they are morphisms between hyperelliptic curves. The support of the elements in the kernel of a (2,2)-isogeny defines a factorisation of the defining hyperelliptic curve polynomial into quadratic polynomials. One can find the hyperelliptic curve in the codomain via the Richelot correspondence. We can map points between hyperelliptic curves via this Richelot correspondence. We use this to extend the map on curves to a map on Jacobians by mapping the support of elements of the Jacobian.

(3,3)-isogenies over the Kummer Surface As for (3,3)-isogenies, we note that for the purposes of genus two isogeny cryptography, we do not need to map points under the isogeny but only need to map Kummer points under the isogeny since the Jacobian points that correspond to the Kummer points both generate identical subgroups.

Given an abelian variety A, the *Kummer variety* is defined by $A/\langle\pm 1\rangle$. This is a quartic surface in $\mathbb{P}^3$ and computations of isogenies on the Kummer surface was the object of study of [2]. We can use the formulae[3] presented in [2] to compute the images of Kummer points under the isogeny. This has also been noted by Costello in [5].

We remark that the procedure detailed in [2, §3] is incomplete. Using the notation in [2], a last transformation is necessary as c has shifted away from 1 due to prior transformations. At that stage, we have the following:

$$(s,t,c_0,c_1,c_2,m_0,m_1,m_2,u) = (s',t',1,-1,0,-r',0,1,1)\,.$$

We need one last transformation

$$y \mapsto (4/\lambda_1)^2 y$$

[3] The files containing the formulae can be found in `http://www.cecm.sfu.ca/~nbruin/c3xc3/`.

and set

$$s = \lambda_1/4, \quad r = \text{Coefficient of } x \text{ in } H_1, \quad t = \text{Coefficient of 1 in } H_1$$

to get the (r, s, t)-parameterisation of [2, Theorem 6].

The key to forming the cubic formula which maps Kummer points to Kummer points under the $(3, 3)$-isogeny lies in the biquadratic forms on the Kummer surface from [3, pg. 23]. Given the generators of the maximal isotropic subgroup of $J_H[3]$, the authors found two cubic forms which are each invariant under translation by T_1 and T_2 respectively. The cubic forms generated spaces of dimension 8 and intersect in dimension 4, which gives an explicit description of the quartic model of the Kummer surface.

3.4 Genus Two SIDH

We will present the key exchange protocol in genus two for completeness. The astute reader will see that all the steps carry over from the original scheme presented in §3.2 of [14].

Set-up Pick a prime p of the form $p = 2^{e_A}3^{e_B}f - 1$ where $2^{e_A} \approx 3^{e_B}$. Now, we pick a hyperelliptic curve H using the methods of §3.1 which will be defined over $\mathbb{F}_{p^2}$. We then generate the bases $\{P_1, P_2, P_3, P_4\}$ and $\{Q_1, Q_2, Q_3, Q_4\}$ which generate $J_H[2^{e_A}]$ and $J_H[3^{e_B}]$ respectively.

First Round Alice chooses her secret scalars $(a_i)_{i=1,...,12}$ using the steps outlined in §3.2 and computes the isogeny $\phi_A : J_H \to J_A$ with kernel given by

$$\left\langle \sum_{i=1}^{4}[a_i]P_i,\ \sum_{i=5}^{8}[a_i]P_i,\ \sum_{i=9}^{12}[a_i]P_i \right\rangle .$$

She also needs to compute the points $\phi_A(Q_i)$ for $i = 1, 2, 3, 4$. She sends the tuple

$$(G_2(J_A), \phi_A(Q_1), \phi_A(Q_2), \phi_A(Q_3), \phi_A(Q_4))$$

to Bob, where $G_2(J_A)$ is the G_2-invariants of the hyperelliptic curve associated to J_A.

At the same time, Bob chooses his secret scalars $(b_i)_{i=1,...,12}$ using the steps outlined in §3.2 and computes the isogeny $\phi_B : J_H \to J_B$ which has the kernel

$$\left\langle \sum_{i=1}^{4}[b_i]P_i,\ \sum_{i=5}^{8}[b_i]P_i,\ \sum_{i=9}^{12}[b_i]P_i \right\rangle .$$

He computes the points $\phi_B(P_i)$ for $i = 1, 2, 3, 4$, and sends the tuple

$$(G_2(J_B), \phi_B(P_1), \phi_B(P_2), \phi_B(P_3), \phi_B(P_4))$$

to Alice.

Second Round Alice will receive Bob's tuple and proceeds with computing J_B from the G_2-invariant, and the points

$$\left\langle \sum_{i=1}^{4}[a_i]\phi_B(P_i),\ \sum_{i=5}^{8}[a_i]\phi_B(P_i),\ \sum_{i=9}^{12}[a_i]\phi_B(P_i) \right\rangle .$$

This is the kernel of a $(2^{e_A}, 2^{e_A-k}, 2^k)$-isogeny $\phi'_A : J_B \to J_{BA}$. Bob will perform a similar computation and arrive at the PPSSAS J_{AB}. But since

$$J_{AB} = J_A/\phi_A(K_B) \cong J_H/\langle K_A, K_B\rangle \cong J_B/\phi_B(K_A) = J_{BA}\,,$$

they can then use the G_2-invariants of J_{AB} and J_{BA} as their shared secret.

Remark 2. The method in [2] allows us to find $\pm\phi_B(P_i)$. However, we need the map

$$(P_1, P_2, P_3, P_4) \mapsto (\phi_B(P_1), \phi_B(P_2), \phi_B(P_3), \phi_B(P_4))$$

or

$$(P_1, P_2, P_3, P_4) \mapsto (-\phi_B(P_1), -\phi_B(P_2), -\phi_B(P_3), -\phi_B(P_4))$$

to ensure that the subgroup generated by Alice in the second round is isotropic.

To fix this problem, one could check if

$$e_{2^{e_A}}(\phi_B(P_i), \phi_B(P_j)) = e_{2^{e_A}}(P_i, P_j)^{3^{e_B}}$$

for all $1 \leq i < j \leq 4$ and negate the $\phi_B(P_i)$'s accordingly.

4 Security and Analysis

4.1 Security Estimates

In this section, we will define the computational problem needed to analyse our cryptosystem.

Let p be a prime of the form $2^n \cdot 3^n \cdot f - 1$, and fix a hyperelliptic curve of genus two H over $\mathbb{F}_{p^2}$ and let J_H denote its Jacobian. Fix bases for $J_H[2^n]$ and $J_H[3^m]$, denoting them by $\{P_i\}_{i=1,2,3,4}$ and $\{Q_i\}_{i=1,2,3,4}$ respectively.

Problem 1 (Computational Genus Two Isogeny (CG2I) Problem). Let $\phi : J_H \to J_A$ be an isogeny whose kernel is given by K. Given J_A and the images $\{\phi(Q_i)\}$, $i \in \{1, 2, 3, 4\}$, find generators for K.

This problem is conjectured to be computationally infeasible for the same reasons as listed in [14]. However, due to the higher regularity of the genus two isogeny graph, we are able to perform a smaller number of isogeny computations to achieve the same security level as compared to SIDH.

Let us look at the complexities of the algorithms one can employ against the CG2I problem, where the task is to recover the isogeny $\phi_A : J_H \to J_A$ when given J_H and J_A. We note that from Proposition 3, we have that the number of elements in the n-sphere is $\ell^{3n-3}(\ell^2+1)(\ell+1) \approx \sqrt{p^3}$, hence a naive exhaustive search on the leaves of J_H has a complexity of $O(\sqrt{p^3})$. One can improve on this by considering the meet-in-the-middle search by listing all isogenies of degree ℓ^n from J_H and J_A and finding collisions in both lists. The meet-in-the-middle search has a complexity of $O(\sqrt[4]{p^3})$. One can perform better by employing a quantum computer to reduce the complexity to $O(\sqrt[6]{p^3})$ using Claw finding algorithms [23]. This compares favourably with the genus one case which has classical security of $O(\sqrt[4]{p})$, and quantum security of $O(\sqrt[6]{p})$. An example of a prime which one can use to achieve 128-bits of security is 171-bits, whereas the genus one case requires 512-bits for the same level of security.

4.2 Existing Attacks on SIDH

We will dedicate this section to examining the impact of the attacks proposed in the cryptanalysis papers [9,24,10,17,7]. We will group the attacks into two classes: Curves and points, and computing endomorphism rings.

Attacks on curves and points include the adaptive attack [9] and fault attacks [24,10]. Attacks via the computation of endomorphism rings include the methods using auxiliary points to find a subring of the endomorphism ring [17] and using the Deuring correspondence [7]. The purpose of computing the endomorphism ring is due to the result in [9] that showed a reduction, in most cases, that the SIDH problem is at most as difficult as computing the endomorphism ring. The key observation behind this result is that the isogenies tend to be short paths in the graph, and so a lattice reduction performed on the basis of the connecting ideal would yield an element that corresponds to the secret isogeny via results in [13].

Adaptive Attack Due to the similar construction of the two protocols, the adaptive attack still carries over to the genus two version. Suppose the attacker is playing the role of Bob and sends Alice the points

$$\phi_B(P_1), \phi_B(P_2), \phi_B(P_3), \phi_B([2^{n-1}]P_4 + P_4))\,.$$

Following the procedure detailed in [9], Bob will be able to recover the first bit of a_4. To recover the rest of the secret, one only needs to tweak the algorithm presented in the original paper.

Fault Attack The loop-abort fault attack presented in [10] would still apply, as our protocol still requires repeated computations of isogenies of low degrees, resulting in the existence of intermediate curves which is key to the attack.

The fault injection on a point as presented in [24] relies on the recovery of the image of one random point under the secret isogeny. Intuitively, the n-torsion points of an abelian variety of genus g is a $\mathbb{Z}/n\mathbb{Z}$-module of rank 2^g. Hence the recovery of the image of one random point as in the $g = 1$ case in [24] is akin to recovering a one-dimensional subspace and the task of finding the secret isogeny is the recovery of the complementary subspace.

This approach can still work in our setting, however we will require a minimum of 2 images of random points under the isogeny. This is because the complementary subspace in our case is of dimension 2, and so we will need at least two points to span that space.

Endomorphism Ring Computations Let E be a supersingular elliptic curve over k and let char $k = p > 0$. Then we know that $\operatorname{End} E \otimes \mathbb{Q} = B_{p,\infty}$, where $B_{p,\infty}$ is the quaternion algebra over $\mathbb{Q}$ ramified at p and ∞. Also, $\operatorname{End} E$ is a maximal order of $B_{p,\infty}$. In the case of higher genus, if A is a PPSSAV of dimension g, then we have that the endomorphism algebra is $\operatorname{End} A \otimes \mathbb{Q} = M_g(B_{p,\infty})$ [16, pg. 174, Cor. 2].

We will leave the thorough examination of the effects of endomorphism ring computations on the cryptosystem as an open problem.

5 Conclusion

We studied the (ℓ, ℓ)-isogeny graphs and cryptanalysed a genus two variant of the CGL hash function. We studied the implementation of the genus two SIDH cryptosystem by looking at the mapping of Kummer points under a $(3, 3)$-isogeny and Jacobian points under a $(2, 2)$-isogeny. We have shown that the genus two isogeny cryptosystem can be implemented, but the fact of the matter is: improvements in the algorithms need to be found before a practical implementation can be achieved.

References

1. Bruin, N., Doerksen, K.: The arithmetic of genus two curves with (4,4)-split Jacobians. Canadian Journal of Mathematics **63** (2009)
2. Bruin, N., Flynn, E.V., Testa, D.: Descent via (3,3)-isogeny on Jacobians of genus 2 curves. Acta Arithmetica **165** (2014)
3. Cassels, J.W.S., Flynn, E.V.: Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2. London Mathematical Society Lecture Note Series, Cambridge University Press (1996)
4. Charles, D.X., Lauter, K.E., Goren, E.Z.: Cryptographic Hash Functions from Expander Graphs. J. Cryptology **22**(1), 93–113 (2009)
5. Costello, C.: Computing supersingular isogenies on kummer surfaces. In: Advances in Cryptology - ASIACRYPT 2018. pp. 428–456 (2018)
6. Couveignes, J.M.: Hard homogeneous spaces. Cryptology ePrint Archive, Report 2006/291 (2006), `http://eprint.iacr.org/2006/291`
7. Eisenträger, K., Hallgren, S., Lauter, K.E., Morrison, T., Petit, C.: Supersingular isogeny graphs and endomorphism rings: Reductions and solutions. In: Advances in Cryptology - EUROCRYPT 2018, pp. 329–368 (2018)
8. Galbraith, S.D.: Mathematics of Public Key Cryptography. Cambridge University Press, New York, NY, USA, 1st edn. (2012)

9. Galbraith, S.D., Petit, C., Shani, B., Ti, Y.B.: On the security of supersingular isogeny cryptosystems. In: Advances in Cryptology - ASIACRYPT 2016, pp. 63–91 (2016)
10. Gélin, A., Wesolowski, B.: Loop-abort faults on supersingular isogeny cryptosystems. Post-Quantum Cryptography - PQCrypto 2017 pp. 93–106 (2017)
11. Gonzalez, J., Guàrdia, J., Rotger, V.: Abelian surfaces of GL[2]-type as Jacobians of curves. Acta Arithmetica **116**, 263–287 (2005)
12. Jao, D., Luca De Feo: Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. PQCrypto '11 Proceedings pp. 19–34 (2011)
13. Kohel, D., Lauter, K., Petit, C., Tignol, J.: On the Quaternion ℓ-isogeny Path Problem. LMS Journal of Computation and Mathematics **17**(Special issue A), 418–432 (2014)
14. Luca De Feo, Jao, D., Plût, J.: Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. J. Mathematical Cryptology **8**(3), 209–247 (2014)
15. Milne, J.S.: Abelian varieties. In: Cornell, G., Silverman, J.H. (eds.) Arithmetic Geometry, pp. 103–150. Springer New York, New York, NY (1986)
16. Mumford, D.: Abelian varieties, Tata Institute of Fundamental Research Studies in Mathematics, vol. 5. Tata Institute of Fundamental Research, Bombay (2008)
17. Petit, C.: Faster algorithms for isogeny problems using torsion point images. Advances in Cryptology - ASIACRYPT 2017 pp. 330–353 (2017)
18. Rostovtsev, A., Stolbunov, A.: Public-key cryptosystem based on isogenies. Cryptology ePrint Archive, Report 2006/145 (2006), `http://eprint.iacr.org/`
19. Serre, J.P.: Algebraic groups and class fields, Graduate Texts in Mathematics, vol. 117. Springer-Verlag, New York (1988), translated from the French
20. Smith, B.: Explicit Endomorphisms and Correspondences. Ph.D. thesis, University of Sydney (2005)
21. Takashima, K.: Efficient Algorithms for Isogeny Sequences and Their Cryptographic Applications, pp. 97–114 (2018)
22. Takashima, K., Yoshida, R.: An algorithm for computing a sequence of richelot isogenies. Bull. Korean Math. Soc **46**, 789–802 (2009)
23. Tani, S.: Claw Finding Algorithms Using Quantum Walk. ArXiv e-prints (2007)
24. Ti, Y.B.: Fault attack on supersingular isogeny cryptosystems. Post-Quantum Cryptography - PQCrypto 2017 pp. 107–122 (2017)
25. Vélu, J.: Isogénies entre courbes elliptiques. C.R. Acad. Sc. Paris, Série A. **273**, 238 – 241 (1971)

A Examples of Isogeny Graphs

We will consider kernels with order 256 in this example. The key to each example is to the find the number of $C_2 \times C_2$ subgroups of each kernel since this would correspond with the number of possible $(2,2)$-isogenies. Firstly, we note that the structure of maximal isotropic subgroups of order 256 must be $C_{16} \times C_{16}$, or $C_{16} \times C_4 \times C_4$, or $C_{16} \times C_8 \times C_2$ by Proposition 2. The isogeny graphs are given in Figure 1.

The easy case is when the kernel K_0 has the structure $C_{16} \times C_{16}$. This is because there is only one $C_2 \times C_2$ subgroup in K. Hence, there is only one isogeny path available and we have a straight line.

Now, let us consider the case when K_1 has the structure $C_{16} \times C_4 \times C_4$. We will label the isomorphism classes of the surfaces by (n), where n is a natural number. We will denote the first surface by (1).

We can represent the 3 generators of K_1 by P, Q and R, where their orders are 16, 4 and 4 respectively. There are 3 different $C_2 \times C_2$ subgroups of K given by $\langle [8]P, [2]Q \rangle$, $\langle [8]P, [2]R \rangle$ and $\langle [8]P, [2](Q+R) \rangle$ in accordance to Lemma 2. Hence, we can and will denote the $(2,2)$-subgroups of K by the scalar preceding Q and R. For instance, the three subgroups given here are denoted by $(2,0)$, $(0,2)$ and $(2,2)$.

These 3 subgroups lead to non-isomorphic surfaces labelled as $(2), (3)$ and (4). The edges are labelled by the subgroup corresponding to the isogeny.

Consider the vertex (2), and consider the $(2,2)$-isogeny from (2) with kernel $\langle [4]P, [2]R \rangle$[4] and denote the codomain by (8). One can see that the isogeny from (1) to (8) has kernel $\langle [4]P, [2]Q, [2]R \rangle$.

One can also map from (3) and (4) to (8) via the kernels (2,0) and (2,0). Immediately, one can spot the diamonds mentioned prior to this example. Indeed, the diamonds can be seen repeatedly in the graph.

Vertices can form tips of the diamond when there is a $C_4 \times C_2 \times C_2$ subgroup in the kernel. This is best illustrated in the next example where the kernel K_2 has structure $C_{16} \times C_8 \times C_2$. Using the notation from the previous example, K_2 will be given by $\langle P', Q', R' \rangle$, where $P' = P$, $[2]Q' = Q$ and $R' = [2]R$

Starting from the vertex (1) again, we have the same 3 subgroups, which result in the same surfaces (2), (3) and (4). We also have that the three surfaces will all have maps into (8) as before. However, residual kernel at (2) is now isomorphic to $C_8 \times C_8$, hence we see that the isogeny path from (2) down to (18) is a straight line. The residual kernel at (4) on the other hand, is $C_8 \times C_4 \times C_2$, hence it contains $C_4 \times C_2 \times C_2$ as a subgroup and so, (4) forms the tip of another diamond.

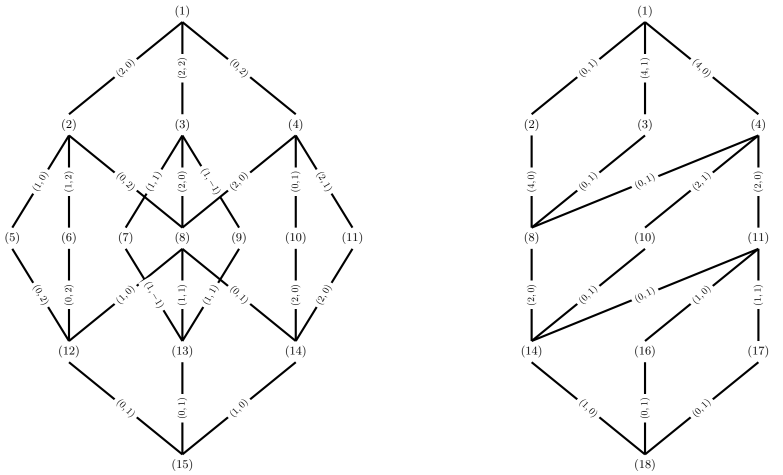
Another thing to note about this case is that the moment R is in the kernel, we cannot have $C_4 \times C_2 \times C_2$ as a subgroup of the residual kernel. This can be observed from the diagonal right-to-left lines in Figure 1b.

Lastly, Figure 2 shows all the neighbours which are two $(2,2)$-isogenies away. So the top vertex is connected to each of the middle and bottom vertices by an isogeny of degree 4 and 16 respectively. The diamonds corresponding to kernels with the structure $C_4 \times C_2 \times C_2$, (though contorted) are present and its number is as predicted in Proposition 3.

B Implementation

We have implemented the key exchange scheme in `MAGMA` using p of 100-bits. This yields a classical security of 75-bits and a quantum security of 50-bits. The first round of the key exchange which required the mapping of points took

[4] Note that we actually mean $\langle [4]\phi(P), [2]\phi(R) \rangle$, where ϕ corresponds to the $(2,2)$-isogeny from (1). We will drop ϕ for ease of notation.



(a) Kernel has structure $C_{16} \times C_4 \times C_4$. (b) Kernel has structure $C_{16} \times C_8 \times C_2$.

Fig. 1: Isogeny subgraphs when the kernel has order 256.

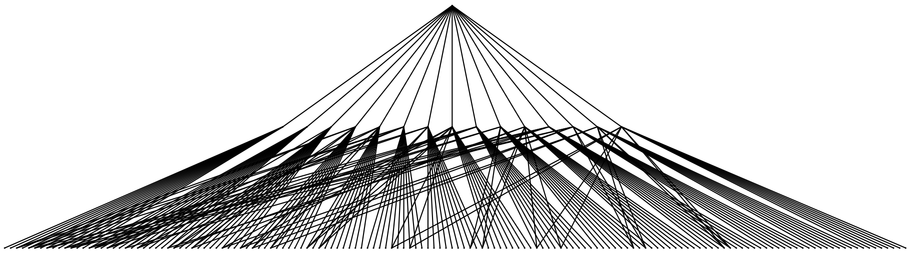


Fig. 2: Isogeny graph from an arbitrary vertex showing 2 layers of isogenies.

145.7 seconds for Alice and 145.41 seconds for Bob. The second round of the key exchange took 74.8 seconds for Alice and 72.29 seconds for Bob.

The implementation took parameters $e_A = 51$ and $e_B = 32$, and $f = 1$ with

$$p = 417263051601157862687607934156 7\,.$$

The base hyperelliptic curve is defined by

$$\begin{aligned}
H : y^2 = {} & (380194068372159317574541564775i + 1017916559181277226571754002873)x^6 \\
& + (364215171027660880880411150495 6i + 1449092825028873295033553368501)x^5 \\
& + (490668231383624479442418028296i + 3978975720631052645817531474 33)x^4 \\
& + (577409514474712448616343527931i + 1029071839968410755001691761655)x^3 \\
& + (402108952587684008123962498682 2i + 3862824071831242831691614151192)x^2 \\
& + (293067999461968740378768642515 3i + 1855492455663897070774056208936)x \\
& + 298274002835447856062494721265 7i + 2106211304320458155169465303811
\end{aligned}$$

where $i^2 = -1$ in $\mathbb{F}_{p^2}$.

The generators of the torsion subgroups are given by

$$P_1 = \left(\begin{array}{r} x^2 + (26432687449357966252936697262 27i + 13735594372435731040368670955 31)x \\ +204076626347274129662908417235 7i + 414833698788057207420599966605 5, \\ +(264364476301593721703530391416 7i + 310205268978118299504409008117 9)x \\ +181393667885122274620259652518 6i + 329204564864113091933313301721 8 \end{array}\right),$$

$$P_2 = \left(\begin{array}{r} x^2 + (150612007990926321749266432599 8i + 122841575518318509046978860885 2)x \\ +510940816723538210024413022814i + 325927805213930943126621646192, \\ +(158078138203724439253680316513 4i + 388783492272095457375014944616 3)x \\ +167573350393555136960752415082i + 122513578104074211357286049745 7 \end{array}\right),$$

$$P_3 = \left(\begin{array}{r} x^2 + (350578176787918687883291813443 9i + 190427275318108185252333498013 6)x \\ +646979589883461323280906338962i + 403466470460947461098796570690, \\ +(311311346636220579350524387279i + 101880637058298070900219749327 3)x \\ +140800486989533258726399479998 9i + 184982614972569331228308688882 9 \end{array}\right),$$

$$P_4 = \left(\begin{array}{r} x^2 + (263431478644781951008065949401 4i + 725406335749278053010239352 72)x \\ +153196653216372357842882714306 7i + 143029903868944468007154095810 9, \\ +(395713602396306434048602972412 4i + 304348230408614456709697813720)x \\ +888364867276729326209394828038i + 245313277415659460754892737915 1 \end{array}\right),$$

$$Q_1 = \left(\begin{array}{r} x^2 + (263085206348111442494103184745 0i + 661997004025942244483994748 67)x \\ +497300488675151931970215687005i + 759563233616865509503094963984, \\ +(171199041762601196423536899579 5i + 337054252822568259177537309084 6)x \\ +240924696043035350352017517675 4i + 148611537240401315354028299260 5 \end{array}\right),$$

$$Q_2 = \left(\begin{array}{r} x^2 + (950432829617443696475772551884i + 380976622923188369170746945096 1)x \\ +129388673102344467760710676378 3i + 215204408326901665315858826223 7, \\ +(361376512498299785234555800630 2i + 416606728563199821787356084674 1)x \\ +249487754997086691409398040034 0i + 342216682332131439236639802326 5 \end{array}\right),$$

$$Q_3 = \left(\begin{array}{r} x^2 + (186790947374380742487963372964 1i + 356101797346565520153144598651 7)x \\ +614550355856817299796257158420i + 371381886540651029896372607308 8, \\ +(846565504796531694760652292661i + 243014947674736028558572549178 9)x \\ +382710250761836228175352673508 6i + 878843682607965961832497258982 \end{array}\right),$$

$$Q_4 = \left(\begin{array}{r} x^2 + (249376610260991109771766079674 8i + 247455915099714654469886873508 1)x \\ +843886014491849541025676396448i + 270067475380398265867481111565 6, \\ +(245710900311630230018030400111 3i + 300075482504820765517164136114 2)x \\ +256052019822508740118324883295 5i + 249002870328185324742540165831 3 \end{array}\right).$$

The secret scalars of Alice and Bob are

$$\begin{array}{llll} \alpha_1 = 937242395764589\,, & \alpha_2 = 282151393547351\,, & \alpha_3 = 0, & \alpha_4 = 0, \\ \alpha_5 = 0, & \alpha_6 = 0, & \alpha_7 = 1666968036125619\,, & \alpha_8 = 324369560360356\,, \\ \alpha_9 = 0, & \alpha_{10} = 0, & \alpha_{11} = 0\,, & \alpha_{12} = 0\,, \\ \beta_1 = 103258914945647\,, & \beta_2 = 1444900449480064\,, & \beta_3 = 0, & \beta_4 = 0, \\ \beta_5 = 0, & \beta_6 = 0, & \beta_7 = 28000236972265\,, & \beta_8 = 720020678656772\,, \\ \beta_9 = 0, & \beta_{10} = 0, & \beta_{11} = 0\,, & \beta_{12} = 0\,, \end{array}$$

Using their secret scalars, they will obtain the following pair of hyperelliptic curves

$$\begin{aligned} H_A : y^2 = {} & (340470300458749582159617696505 8i + 403336181260435480105799382459)x^6 \\ & + (300158408642476293806227622234 0i + 311047190480692260365532924751 0)x^5 \\ & + (101719931062723098351158646333 2i + 159918969863143337265085754407 1)x^4 \\ & + (246956201233909294539836567868 9i + 115456647261523682741646762458 4)x^3 \\ & + (841874238658053023013857416200i + 422410815643904319729131959469)x^2 \\ & + (350758422718042697610977205296 2i + 233129826659556946265779873606 3)x \\ & + 272981662052090517559075818701 9i + 374870400664512900049856351473 4\,, \end{aligned}$$

$$\begin{aligned}H_B : y^2 = {} & (3434394689074752663579510896530i + 3258819610341997123576600332954)x^6\\ & + (3350255113820895191389143565973i + 2681892489448659428930467220147)x^5\\ & + (2958298818675004062047066758264i + 904769362079321055425076728309)x^4\\ & + (2701255487608026975177181091075i + 787033120015012146142186182556)x^3\\ & + (3523675811671092022491764466022i + 2804841353558342542840805561369)x^2\\ & + (3238151513550798796238052565124i + 3437885792433773163395130700555)x\\ & + 1829327374163410097298853068766i + 3453489516944406316396271485172\,.\end{aligned}$$

The auxiliary points computed are the following

$$\phi_B(P_1) = \pm\begin{pmatrix}\begin{array}{r} x^2 + (576967470035224384447071691859i + 3905591233169141993601703381059)x\\ +1497608451125872175852448359137i + 2622938093324787679229413320405,\\ (2205483026731282488507766835920i + 1887631895533666975170960498604)x\\ +2270438136719486828147096768168i + 1098893079140511975119740789184 \end{array}\end{pmatrix},$$

$$\phi_B(P_2) = \pm\begin{pmatrix}\begin{array}{r} x^2 + (2002807208424762458028352734443i + 3878472110821865480924821702529)x\\ +476628031810757734488740719290i + 2957584612454518004162519574871,\\ (394990862190771436107181555 3277i + 630639323620735966636718321043)x\\ +901597642385324157925700976889i + 2429302320101537821240219151082 \end{array}\end{pmatrix},$$

$$\phi_B(P_3) = \pm\begin{pmatrix}\begin{array}{r} x^2 + (4133157753622694250606077231439i + 2486410359530824865039464484854)x\\ +217800646374565182483064906626i + 1249364962732904444334902689884,\\ (1265490246594537172661646499003i + 2130834160349159007051974433128)x\\ +258028668098742560100073801 0969i + 578046610192146114698466530758 \end{array}\end{pmatrix},$$

$$\phi_B(P_4) = \pm\begin{pmatrix}\begin{array}{r} x^2 + (660110200377968407384419 0837i + 871063507296311847855491 40074)x\\ +2330339334251130536871893039627i + 1494511552650494479113393669713,\\ (1706314262702892774109446145989i + 3539074449728790590891503255545)x\\ +1950619453681381932329106130008i + 685170915670741858430774920061 \end{array}\end{pmatrix},$$

$$\phi_A(Q_1) = \begin{pmatrix}\begin{array}{r} x^2 + (3464040394311932964693107348618i + 1234121484161567611101667399525)x\\ +178957753932327738552710383385i + 3856858968014591645005318326985,\\ (2432835950855765586938146638349i + 3267484715622822051923177214055)x\\ +985386137551789348760277138076i + 1179835886991851012234054275735 \end{array}\end{pmatrix},$$

$$\phi_A(Q_2) = \begin{pmatrix}\begin{array}{r} x^2 + (3633827009609782610886962935 01i + 3499548729039922528103431054749)x\\ +3832512523382547716418075195517i + 3364204966204284852762530333038,\\ (3043817101596607612186808885116i + 4027557567198565187096133171734)x\\ +4087176631917166066356886198518i + 1327157646340760346840638146328 \end{array}\end{pmatrix},$$

$$\phi_A(Q_3) = \begin{pmatrix}\begin{array}{r} x^2 + (3946684136660787881888285451015i + 1250236853749119184502604023717)x\\ +3358152613483376587872867674703i + 4672522011510763890555248094 76,\\ (1562920784368105245499132757775i + 987920823075946850233644600497)x\\ +1675005758282871337010798605079i + 1490924669195823363601763347629 \end{array}\end{pmatrix},$$

$$\phi_A(Q_4) = \begin{pmatrix}\begin{array}{r} x^2 + (1629408242557750155729330759772i + 3235283387810139201773539373655)x\\ +1341380669490368343450704316676i + 1454971022788254094961980229605,\\ (2393675986247524032663566872348i + 3412019204974086421616096641702)x\\ +1890349696856504234320283318545i + 841699061347215234631210012075 \end{array}\end{pmatrix}.$$

This allows for both parties to compute the final isogeny to obtain

$$\begin{pmatrix}\begin{array}{c} 1055018150197573853947249198625i + 2223713843055934677989300194259,\\ 819060580729572013508006537232i + 3874192400826551831686249391528,\\ 1658885975351604494486138482883i + 3931354413698538292465352257393 \end{array}\end{pmatrix}$$

as their common G_2-invariants.