Supersingular Non-Superspecial Abelian Surfaces in Cryptography

Jason T. LeGrow[1], Yan Bo Ti[2], and Lukas Zobernig[1]

[1]Department of Mathematics, University of Auckland, New Zealand
{jason.legrow, lukas.zobernig}@auckland.ac.nz
[2]DSO National Laboratories, Singapore
yanbo.ti@gmail.com

Abstract

We consider the use of supersingular abelian surfaces in cryptography. Several generalisations of well-known cryptographic schemes and constructions based on supersingular elliptic curves to the 2-dimensional setting of superspecial abelian surfaces have been proposed. The computational assumptions in the superspecial 2-dimensional case can be reduced to the corresponding 1-dimensional problems via a product decomposition by observing that every superspecial abelian surface is non-simple and separably isogenous to a product of supersingular elliptic curves. Instead, we propose to use supersingular non-superspecial isogeny graphs where such a product decomposition does not have a computable description via separable isogenies. We study the advantages and investigate security concerns of the move to supersingular non-superspecial abelian surfaces.

1 Introduction

Isogeny-based cryptography is a subfield of cryptography whose protocols' security is based on the hardness of finding isogenies between given elliptic curves (or, more generally, abelian varieties). The first isogeny-based protocol appeared in 1997 in unpublished work of Couveignes [Cou06] and was independently rediscovered by Rostovtsev and Stolbunov in 2006 [RS06] — this protocol used complex multiplication on ordinary elliptic curves to construct a key establishment protocol *à la* Diffie and Hellman [DH76]. This CRS protocol is of theoretical interest, but is not efficient enough in practice, even in state-of-the-art implementations, see De Feo et al. [DFKS18].

The first documented use of supersingular elliptic curves for isogeny-based cryptography is the hash function of Charles et al. [CLG07] in 2006, and in 2011, Jao and De Feo proposed Supersingular Isogeny Diffie-Hellman (SIDH) [JDF11], which underlies SIKE [Aza+20], a third round alternate candidate for the NIST post-quantum standardization competition. Supersingular elliptic curves are studied in this context because they have a number of convenient features that are exploited for efficiency and security purposes. In particular:

1. For any primes $\ell \neq p$, the *supersingular ℓ-isogeny graph* $\mathcal{G}_{\ell,p}$ is a Ramanujan graph [Piz90; Piz98];
2. Any supersingular curve in characteristic p is defined over $\mathbb{F}_{p^2}$;

3. If $E/\mathbb{F}_{p^2}$ is supersingular then $\#E(\mathbb{F}_{p^2}) \in \{p^2 + 1, p^2 \pm p + 1, p^2 \pm 2p + 1\}$ — moreover, it is easy to construct curves $E/\mathbb{F}_{p^2}$ with a given number of $\mathbb{F}_{p^2}$-rational points [Brö09]; and,
4. If $E/\mathbb{F}_{p^2}$ is supersingular then $\mathrm{End}(E)$ is non-commutative.

Respectively, these properties guarantee that

1. Random walks in $\mathcal{G}_{\ell,p}$ mix rapidly, ensuring that even relatively-short walks yield nearly uniform outputs;
2. An isomorphism class of supersingular elliptic curves in characteristic p — represented by its j-invariant — requires only $2\log_2 p$ bits to encode, leading to small communication requirements and key sizes in isogeny-based key establishment protocols;
3. By choosing an appropriate form of the prime p, we can force certain torsion subgroups of E to be $\mathbb{F}_{p^2}$-rational. This allows isogenies of corresponding large prime-power degrees to be computed using (relatively efficient) arithmetic in $\mathbb{F}_{p^2}$, using Vélu's formulas [Vél71].
4. Quantum attacks using Kuperberg's algorithm [Kup05; Reg04] do not generally apply (although some schemes, like CSIDH [Cas+18], are still susceptible [BS20; Jao+20; BIJ18]).

Just as classical elliptic curve cryptography based on discrete logarithms naturally generalises to hyperelliptic curve cryptography, isogeny-based supersingular elliptic curve cryptography can naturally be generalised by considering (Jacobians of) hyperelliptic curves of genus 2. The primary benefit of working in genus 2 is that a smaller finite field can be used for the same security level, leading to faster field arithmetic and more compact representation of field elements. Takashima [Tak18] first proposed the genus-2 variant of the CGL hash function by replacing supersingular elliptic curves with superspecial abelian surfaces and 2-isogenies with Richelot isogenies. Flynn and Ti [FT19] then studied the superspecial Richelot isogeny graph and discovered the presence of non-trivial collisions in the genus-2 hash function that arose from (ℓ^2, ℓ, ℓ)-isogenies that they named *ℓ-diamonds*. In the same paper, Flynn and Ti also proposed the generalisation of SIDH to genus-2 which they named G2SIDH. They proposed the use of superspecial abelian surfaces and (2,2) and (3,3)-isogenies as the natural generalisations of the primary components in SIDH. Castryck et al. [CDS20] improved on Takashima's proposed hash function by avoiding the diamonds found by Flynn and Ti.

In the above cases of genus-2 cryptography, the schemes work in the graph of superspecial abelian surfaces. In this paper, we propose moving away from superspecial abelian surfaces towards (connected components of) supersingular non-superspecial abelian surfaces. Supersingular non-superspecial abelian surfaces are actually isogenous to superspecial abelian surfaces, so a priori there are no apparent difference between working on either types. However, supersingular non-superspecial abelian surfaces are only isogenous to superspecial abelian surfaces via inseparable isogenies. Since all of the cryptosystems mentioned above use $(2, 2)$ or $(3, 3)$-isogenies — and are co-prime to p — the effect is that the superspecial and supersingular non-superspecial graphs are not connected to each other.

Bearing this in mind, in this paper, we propose moving to the supersingular non-superspecial graph because of the lack of reducible surfaces there. This would provide the following advantages:

1. Implementations of genus-2 isogeny-based protocols in the superspecial graph must have either a branch condition (making constant-time implementations difficult) or termination condition (leading to possible protocol failures) to handle reducible surfaces; these are not necessary in the supersingular non-superspecial graph;

$A[p]$	Type	Codim. in $\mathcal{M}_2$
L^2	ordinary	0
$L \oplus I_{1,1}$	non-ordinary	1
$I_{2,1}$	supersingular non-superspecial	2
$I_{1,1} \oplus I_{1,1}$	superspecial	3

Table 1: Strata of the coarse moduli space of abelian surfaces over a finite field, see Pries [Pri08].

2. Side-channel attacks which exploit the existence of reducible surfaces in the secret isogeny path can be prevented; and,

3. The attack of Costello and Smith [CS20] does not apply (unless p-isogenies can be efficiently computed).

At the same time, we will examine the concerns of such a move by examining the size of the isogeny graph, and its structure.

2 Preliminaries

We fix a prime p and denote the finite field with p elements by $\mathbb{F}_p$ and its algebraic closure by $\overline{\mathbb{F}}_p$. We call an elliptic curve $E/\overline{\mathbb{F}}_p$ either *ordinary* or *supersingular*, depending on whether the p-torsion group of E satisfies $E[p] \cong \mathbb{Z}/p\mathbb{Z}$ or $E[p] \cong 0$, respectively. In fancier language, we say that the p-torsion group scheme of E is either $L \cong \mathbb{Z}/p\mathbb{Z} \oplus \mu_p$, or the *local-local Barsotti–Tate* (BT_1) group scheme $I_{1,1}$.

In two dimensions we find more than just these two possibilities. Consider an abelian surface $A/\overline{\mathbb{F}}_p$, then the p-torsion group scheme $A[p]$ of A is isomorphic to one of the following four possible group schemes given in Table 1.

Here $I_{2,1}$ is another certain BT_1 group scheme. The codimension of the associated strata in the coarse moduli space of abelian surfaces is given as well. We also call a genus-2 curve ordinary, non-ordinary, supersingular non-superspecial, or superspecial if its Jacobian is of that type.

Since the correct generalisation of the term "supersingular" depends on the *slopes of the Newton-polygon* corresponding to an abelian variety (see Oort [Oor00]), we have that superspecial abelian surfaces are in particular supersingular. Hence, we make the explicit distinction into "supersingular non-superspecial" and "superspecial" abelian surfaces.

There is a similar distinction of the p-torsion group schemes in higher dimension, but there we find even more possible types and the correspondence between supersingularity and group scheme types becomes fuzzy. Here we will restrict only to dimension 2, also because every abelian surface is given as either the product of two elliptic curves or as the Jacobian of a genus-2 hyperelliptic curve. This simple description of abelian surfaces lends itself to better applicability to cryptography. This does not hold in dimension 3 and higher and we would have to consider more complicated models for curves in general.

2.1 Superspecial Abelian Varieties

Ignoring any (principal) polarisation, there exists only one superspecial abelian surface. That is, every superspecial abelian surface A is isomorphic to a product of (any pair of) supersingular elliptic curves $A \cong E_1 \times E_2$, see Oort [Oor75, Theorem 2]. Hence we can fix any supersingular elliptic curve E and view $A = E \times E$ as our "canonical" (unpolarised) abelian surface.

It is only when considering data in the form of tuples of abelian surfaces along with some (principal) polarisation $\mathcal{L}$ on A of the form $(A, \mathcal{L})$ that we can effectively distinguish them. It is also true that Jacobians of hyperelliptic curves naturally admits a principal polarisation, hence it is useful to keep track of polarisations. This fact generalises also to dimension 3 and higher. In our case of dimension 2, every principally polarised superspecial abelian surface is then either the Jacobian of some superspecial genus-2 curve, or isomorphic to a product of two supersingular elliptic curves (in which case *the polarisation splits*). In both cases the principal polarisation arises in a canonical way via the Jacobian construction of the underlying genus-2 curve, or the product of the two genus-1 curves, respectively.

The following exposition for general dimension follows Ibukiyama et al. [IKO86]. Fix a prime p. Denote by $B_{p,\infty}$ the definite (i.e. ramified at ∞) quaternion algebra ramified at p. Let k be an algebraically closed field of characteristic p, and let E be a supersingular elliptic curve defined over k. Then $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q} \cong B_{p,\infty}$, and $\mathrm{End}(E) \cong \mathcal{O}_E$ is a maximal order of $B_{p,\infty}$.

Let A be an abelian variety. Let T_x denote translation by $x \in A$. For a line bundle $\mathcal{L}$ on A, denote by $\varphi_{\mathcal{L}}$ the morphism

$$\begin{aligned} \varphi_{\mathcal{L}} : A &\to \hat{A}, \\ x &\mapsto T_x^* \mathcal{L} \otimes \mathcal{L}^{-1}. \end{aligned}$$

As we mentioned, for any unpolarised superspecial abelian variety A over k of genus $g \geq 2$ we have $A \cong E^g$ for some supersingular elliptic curve E. Let $\mathcal{P}$ be the line bundle corresponding to the divisor $E^{g-1} \times \{0\} + E^{g-2} \times \{0\} \times E + \cdots + \{0\} \times E^{g-1}$. Then $\mathcal{P}$ defines a principal polarisation on A. Let $\mathrm{NS}(A)$ be the Neron–Severi group of A (divisor classes on A up to *algebraic* equivalence), and denote by $M_g(\mathcal{O}_E)$ the ring of $g \times g$-matrices over $\mathcal{O}_E$. Note that $\mathrm{End}(A) \cong M_g(\mathcal{O}_E)$. Consider the following morphism

$$\begin{aligned} j : \mathrm{NS}(A) &\to \mathrm{End}(A), \\ \mathcal{L} &\mapsto \varphi_{\mathcal{P}}^{-1} \circ \varphi_{\mathcal{L}}. \end{aligned}$$

Lemma 1. *The image of* $\mathrm{NS}(A)$ *by* j *is*

$$\left\{ H \in M_g(\mathcal{O}_E) \mid H^\dagger = H \right\},$$

the Hermitian matrices in $M_g(\mathcal{O}_E)$. *Extending to* $\mathrm{NS}^0(A) = \mathrm{NS}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$, *this induces a Jordan algebra structure on* $\mathrm{NS}^0(A)$. *Denote by* $\mathrm{HN}(.)$ *the* Hauptnorm *(see Braun and Koecher [BK65]) on* $\mathrm{NS}^0(A)$. *Then* $\deg \varphi_{\mathcal{L}} = (L^g/g!)^2 = \mathrm{HN}(j(\mathcal{L}))^2$, *where* L *is the divisor corresponding to* $\mathcal{L}$. *We have that* $\mathcal{L}$ *is ample if and only if* $j(\mathcal{L})$ *is positive definite.*

Proof. This follow from Ibukiyama et al. [IKO86, Proposition 2.8] and Mumford [Mum08]. □

Note that in our case, the Hauptnorm on $\mathrm{NS}^0(A)$ corresponds to the usual *reduced norm* on $M_g(\mathcal{O}_E)$. Ample line bundles in $\mathrm{NS}(A)$ give polarisations on A, and so by Lemma 1 there is a bijection

$$\left\{ \text{principal polarisations on } A \right\} \leftrightarrow \left\{ H \in \mathrm{GL}_g(\mathcal{O}_E) \mid H^\dagger = H, H > 0 \right\}.$$

Note that $\mathrm{GL}_g(\mathcal{O}_E)$ acts on the set of all positive definite Hermitian matrices in $M_g(\mathcal{O}_E)$ by conjugation. If we consider our objects up to automorphism we obtain the bijection

$$\left\{ \begin{array}{l} \text{Principal polarisations on } A \text{ up to au-} \\ \text{tomorphism.} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{l} \text{Conjugacy classes of positive definite} \\ \text{Hermitian matrices in } \mathrm{GL}_g(\mathcal{O}_E). \end{array} \right\}.$$

Lemma 2 (Jordan and Zaytman [JZ20, Proposition 31])**.** *Let $A \cong E^g$ be a superspecial abelian variety, and let H and H' correspond to the principal polarisations $\mathcal{L}$ and $\mathcal{L}'$, respectively. Let $\phi : A \longrightarrow A$ be an isogeny with maximal Weil isotropic kernel of degree ℓ^{gn} (with respect to the principal polarisation $\mathcal{L}$). Then $\phi^*\mathcal{L}' = \ell^n \mathcal{L}$ if and only if $M^\dagger H' M = \ell^n H$ for a matrix $M \in M_g(\mathcal{O}_E)$, and then M corresponds to ϕ.*

Fix any maximal order $\mathcal{O}$ of $B_{p,\infty}$. Then, by Lemmas 1 and 2, there is an equivalence of categories

$$\left\{\begin{array}{l}\text{Objects: Isomorphism classes of prin-}\\ \text{cipally polarised superspecial abelian}\\ \text{varieties over } k \text{ of genus } g \geq 2.\\[4pt] \text{Morphisms: Isogenies with maximal}\\ \text{Weil isotropic kernels of degree } \ell^{gn}.\end{array}\right\} \leftrightarrow \left\{\begin{array}{l}\text{Objects: Conjugacy classes of pos-}\\ \text{itive definite Hermitian matrices in}\\ \mathrm{GL}_g(\mathcal{O}).\\[4pt] \text{Morphisms: Conjugation by } M_g(\mathcal{O})\\ \text{sending one class to an } \ell^n\text{-multiple of}\\ \text{the other.}\end{array}\right\}.$$

2.2 Endomorphisms of Superspecial Abelian Surfaces

The Deuring correspondence gives a bijection between supersingular elliptic curves and maximal orders of $B_{p,\infty}$. Similarly, the discussion in Section 2.1 shows a bijection between principally polarised superspecial abelian surfaces and conjugacy classes of positive definite Hermitian matrices in $\mathrm{GL}_2(\mathcal{O})$, where $\mathcal{O}$ is a maximal order of $B_{p,\infty}$. Note, though, that unlike in dimension 1 where the Deuring correspondence gives us a canonical identification of curves and maximal orders, in dimension 2 all of our data is relative to a maximal order $\mathcal{O}$ (which we have to fix beforehand). Computationally, this requires us to determine endomorphism rings of supersingular elliptic curves. Changing data between different representations (relative to different maximal orders) is also not trivial. And yet, reducing the superspecial isogeny path problem from higher dimension to dimension 1 by finding reducible abelian varieties in the superspecial graph still has lower computational complexity than applying the usual path finding algorithms directly, see Costello and Smith [CS20] and especially Remark 2 ibid.

2.3 Supersingular Non-Superspecial Abelian Surfaces

Fix a prime p and let $k = \overline{\mathbb{F}}_p$. Let α_p by the finite group scheme $\alpha_p = \operatorname{Spec} k[x]/(x^p)$. Consider a supersingular abelian surface A over k. Then by Oort [Oor75, Corollary 7], there exists an exact sequence

$$0 \longrightarrow \alpha_p \xrightarrow{\iota_t} E \times E \xrightarrow{\psi} A \longrightarrow 0,$$

i.e. we have an inseparable isogeny $\psi : (E \times E)/\iota_t(\alpha_p) \longrightarrow A$. The possible embeddings $\iota_t : \alpha_p \longrightarrow E \times E$ are parametrised by an *embedding parameter* $t \in \mathbb{P}^1(k)$. By Oort [Oor75], A is superspecial if $t \in \mathbb{P}^1(\mathbb{F}_{p^2})$ and A is supersingular non-superspecial if $t \notin \mathbb{F}_{p^2}$. Let $\pi\mathcal{O}$ be the prime ideal over p in $\mathcal{O} = \operatorname{End}(E)$ (for some generator $\pi \in \mathcal{O}$).

Theorem 3 (Ibukiyama et al. [IKO86, Proposition 2.14])**.** *Let A be a supersingular non-superspecial abelian surface with $t \notin \mathbb{F}_{p^2}$. Then the set of principal polarisations on A is naturally bijective to*

$$P_A = \left\{ \begin{pmatrix} pa & c \\ \overline{c} & pb \end{pmatrix} \middle| \, a, b \in \mathbb{Z}; a, b > 0; c \in \pi\mathcal{O}; p^2ab - c\overline{c} = p \right\}.$$

The set P_A describes principal polarisations on A pulled back to $E \times E$. Hence the number of principal polarisations on A up to equivalence is given by counting the equivalence classes in P_A under the pullback of $\mathrm{End}(A)$ by ψ in $\mathrm{End}(E \times E) = M_2(\mathcal{O})$. The pullback of $\mathrm{End}(A)$ in $\mathrm{End}(E \times E)$ has different representations, depending on whether $t \in \mathbb{F}_{p^4} \setminus \mathbb{F}_{p^2}$ or $t \notin \mathbb{F}_{p^4}$. The number h of principal polarisations $\mathcal{L}$ on A up to equivalence is then as follows.

Theorem 4 (Ibukiyama [Ibu20, Theorem 1.1, Theorem 1.2]). *1. If $t \notin \mathbb{F}_{p^4}$, then*

$$h = \begin{cases} 1 & \textit{if } p = 2, \\ \frac{p^2(p^4-1)(p^2-1)}{5760} & \textit{for any } p \geq 3. \end{cases}$$

When p is odd, we have $\mathrm{Aut}(A, \mathcal{L}) = \{\pm 1\}$ for any principal polarisation.

2. If $t \in \mathbb{F}_{p^4} \setminus \mathbb{F}_{p^2}$, then

$$h = \begin{cases} 1 & \textit{if } p = 2, \\ \frac{p^2(p^2-1)^2}{2880} & \textit{if } p \equiv \pm 1 \pmod 5 \textit{ or } p = 5, \\ 1 + \frac{(p-3)(p+3)(p^2-3p+8)(p^2+3p+8)}{2880} & \textit{if } p \equiv \pm 2 \pmod 5. \end{cases}$$

If $p \equiv \pm 2 \pmod 5$, there is a unique principal polarisation $\mathcal{L}$ on A such that $\mathrm{Aut}(A, \mathcal{L}) \cong \mathbb{Z}/10\mathbb{Z}$, and for all the other principal polarisations we have $\mathrm{Aut}(A, \mathcal{L}) = \{\pm 1\}$.

2.4 G2SIDH

The G2SIDH is a generalisation of SIDH to genus-2. Let p be a prime of the form $p = 2^{e_A} \cdot 3^{e_B} \cdot f - 1$. Now, let H be the hyperelliptic curve given by

$$H : y^2 = x^6 + 1$$

over $\mathbb{F}_{p^2}$. The Jacobian of H, denoted by J_H, can be used as the base principally polarised superspecial abelian surface. One could also choose a different base principally polarised superspecial abelian surface by performing a random walk from J_H in the Richelot isogeny graph. Due to our choice of prime characteristic, we have that $\#J(\mathbb{F}_{p^2}) = (p+1)^4$ and so, we have that $J(\mathbb{F}_{p^2}) = J[2^{e_A}] \times J[3^{e_B}] \times J[f]$ as a group.

We then define symplectic generators for the 2^{e_A} and 3^{e_B}-torsion groups as $\langle P_1, P_2, P_3, P_4 \rangle = J[2^{e_A}]$ and $\langle Q_1, Q_2, Q_3, Q_4 \rangle = J[3^{e_B}]$. Symplectic generators of the torsion group $J[m]$ with respect to the Weil pairing are points (P_1, P_2, P_3, P_4) such that

$$e_m(P_1, P_3) = e_m(P_2, P_4) = \zeta,$$

where ζ is some primitive m-th root of unity and all other combinations are trivial.

In the first step of the key exchange, Alice chooses her secret isogeny ϕ_A such that the kernel of the isogeny has order 2^{2e_A}, which is a maximal isotropic subgroup, K_A, of order 2^{2e_A}. She does so by selecting scalars $k \in \{0, \frac{e_A}{2}\}$, $a \in [\ell^{e_A}]$, $b \in [\ell^{e_A - k}]$, $c \in [\ell^{e_A - 2k}]$, $d \in [\ell^k]$, and a permutation $\sigma \in D_8$, and computing the generators

$$\begin{aligned} K_{A,1} &= P_{\sigma(1)} + [d]P_{\sigma(2)} + [a]P_{\sigma(3)} + [b]P_{\sigma(4)}, \\ K_{A,2} &= \ell^k \cdot (P_{\sigma(2)} + [s_\sigma \cdot (b - dc)]P_{\sigma(3)} + [c]P_{\sigma(4)}), \\ K_{A,3} &= \ell^{e_A - k} \cdot ([-s_\sigma \cdot d]P_{\sigma(3)} + P_{\sigma(4)}), \end{aligned}$$

Let J_A be the codomain of ϕ_A. She sends the tuple

$$\left(J_A, \phi_A(Q_1), \phi_A(Q_2), \phi_A(Q_3), \phi_A(Q_4)\right)$$

to Bob.

Bob analogously completes his side of the computation and Alice thus receives the tuple

$$\left(J_B, \phi_B(P_1), \phi_B(P_2), \phi_B(P_3), \phi_B(P_4)\right).$$

She can then use her combination of secret scalars generating the kernel of her secret isogeny ϕ_A to compute an isogeny from J_B using $\phi_B(P_i)$ as the basis instead of P_i. Denote the codomain of this isogeny by J_{AB}. Bob will complete his side of the protocol and obtain the abelian surface J_{BA}. By construction, J_{AB} and J_{BA} are isomorphic as principally polarised abelian surfaces and thus also the corresponding hyperelliptic curves are isomorphic via Torelli's theorem [Mil86, Cor. 12.2]

2.5 CDS Hash

Constructing an isogeny-based hash function has its origins in 2006 when Charles, Goren and Lauter proposed using random walks in the 2-isogeny graph of supersingular elliptic curves as the basis of a hash function.

To compute the hash function, a base supersingular elliptic curve E_0 is chosen along with a 2-isogeny $\phi_{-1} : E_{-1} \to E_0$. Then each bit of the input to the hash function is used to determine the next step in the random walk since there are only two choices left. Exploiting the fact that the supersingular 2-isogeny graph is Ramanujan, they were able to prove that this hash function is secure if the input is sufficiently long.

The genus-2 variant of the CGL hash function was first proposed by Takashima [Tak18] which is to be performed in the superspecial (2,2)-isogeny graph. This hash function was broken by Flynn and Ti [FT19] when they discovered that the (2,2)-isogeny graph has 2-diamonds that admits non-trivial collisions in the hash function. This vulnerability is patched by Castryck et al. [CDS20] by using Lagrangian subgroups (instead of just isotropic subgroups) to avoid non-trivial collisions in the hash function. A final technicality that they had to overcome was the potential of encountering a reducible abelian surface in the superspecial graph. The probability of this occurrence after a random walk is $O(1/p)$ since there are a total of $\Theta(p^3)$ abelian surfaces, and only $O(p^2)$ of them are reducible.

The authors suggested three methods for dealing with encounters with reducible surfaces. The first is to ignore encounters with reducible surfaces. The second proposes to deterministically find a neighbouring irreducible surface to connect to. The final option involves gluing the 2-torsion points of the constituent elliptic curves to produce explicit (2,2)-isogenies to a non-reducible surface [CDS20, §6.3]. However, the authors elected not to include the latter two options and are willing to accept the $O(1/p)$ risk of encountering reducible surfaces.

3 Effects of Reducible Surfaces in the Superspecial Graph

In both cryptosystems, we see that the immediate benefit obtained in moving to the supersingular non-superspecial graph is the omission of reducible surfaces. This serves to rule out exceptions in the graph that both these cryptosystems do not prepare for. This lack of preparation would result in key exchange or encryption failures in the case of G2SIDH, or to hash failures in the case of G2Hash.

Implementing branches that take into account the occurrences of reducible surfaces may give rise to attacks on the respective protocols.

3.1 Attack on G2SIDH and CDS Hash with Reducible Surfaces

The authors of G2SIDH did not provision for the possibility of encountering reducible surfaces in their proposal of G2SIDH. At the same time, the CDS hash did not implement their proposed method for dealing with reducible surfaces. This oversight could lead to key exchange or hash failures and weak keys in the cryptosystems. One natural workaround key exchange and hash failures would be to implement or generalise the technique outlined by [CDS20], which is to form explicit (ℓ, ℓ)-isogenies by gluing along the constituent elliptic curve's ℓ-torsion.

The obvious repercussion of this is that we no longer have a constant time implementation of the key exchange scheme. This opens up G2SIDH and the CDS hash function to simple side-channel timing attacks that can detect if reducible surfaces exists in the path corresponding to the secret key.

Given two principally polarised abelian surfaces A_1 and A_2, an adversary can devise an attack based on this observation. Suppose that there is one reducible surface detected between A_1 and A_2, the adversary will compute all neighbours of A_1 and A_2 to find the reducible surface lying between the two surfaces. This situation is illustrated as such:

$$A \xrightarrow{\phi_0} E \times E' \xrightarrow{\phi_1} A' \tag{1}$$

In the context of G2SIDH, the isogeny $\phi \colon A \to A'$ would be decomposable as a non-backtracking sequence of n (ℓ, ℓ)-isogenies, for $\ell \in \{2, 3\}$ and $\ell^n \approx \sqrt{p}$. By [FT19, Section 4.1], a standard meet-in-the-middle attack solves this problem in time $\tilde{O}(\sqrt[4]{p^3})$. However, an attacker who knows that there is a reducible surface $E \times E'$ on the path from A to A' can potentially reduce the time required. With notation as in Equation (1), suppose that ϕ_0, ϕ_1 correspond to (ℓ, ℓ)-isogeny paths of length n_0, n_1 respectively, and suppose without loss of generality that $n_0 \leq n_1$.[1] The attacker enumerates all (ℓ, ℓ)-isogeny paths of length n_0 starting from A, until he arrives at a reducible surface $\hat{A} \cong \hat{E} \times \hat{E}'$ — under the heuristic assumption that reducible surfaces are uniformly distributed in the superspecial graph, with overwhelming probability there is only one such surface, and it is in fact $E \times E'$. Then the attacker launches the standard meet-in-the-middle attack from $\hat{A}$ to A'.

The first step of this attack requires time $\tilde{O}(\ell^{3n_0})$, while the second requires $\tilde{O}(\ell^{\frac{3n_1}{2}})$. In the optimal situation in which $n_0 = \frac{1}{3}n$ and $n_1 = \frac{2}{3}n$, this attack has complexity $\tilde{O}(\ell^n) = \tilde{O}(\sqrt[6]{p^3})$.

If more reducible surfaces are detected, such that we have

$$A \xrightarrow{\phi_0} E_1 \times E_1' \xrightarrow{\phi_1} E_2 \times E_2' \xrightarrow{\phi_2} \cdots \xrightarrow{\phi_{m-1}} E_m \times E_m' \xrightarrow{\phi_m} A'$$

where each ϕ_j is a path of length n_j, then the meet-in-the-middle attack has complexity $\tilde{O}(\ell^{n_{j^*}} + \sum_{j \neq j^*} \ell^{n_j})$ where $j^* = \arg\max_j \{n_j\}$.

Remark 5. *This attack affects a vanishingly small proportion of the keys, and it is exceedingly unlikely for a path to contain more than one reducible surface. However, it should be noted that these weak keys still exist, and would result in a lack of security. Removing them is as easy as beginning with a different base curve (a supersingular non-superspecial base curve).*

[1] It is reasonable to model that a timing attack will reveal which of n_0 and n_1 is larger, and the proof in the case $n_0 > n_1$ is analogous.

3.2 The Attack of Costello and Smith

Costello and Smith [CS20] address the superspecial isogeny problem in arbitrary genus g; in particular, given two principally polarised superspecial abelian surfaces A, A' of dimension g defined over $\overline{\mathbb{F}}_p$ and a prime $\ell \neq p$, they propose two algorithms to find a chain of $(\ell, \ell, \ldots, \ell)$-isogenies from A to A'. Their classical algorithm [CS20, Theorem 1] runs in expected time $\tilde{O}(p^{g-1})$ (with success probability $2^{-(g-1)}$) while their quantum algorithm [CS20, Theorem 2] runs in time $\tilde{O}(\sqrt{p^{g-1}})$. This is a dramatic improvement over the performance of naïve meet-in-the-middle algorithms: There are $\Theta(p^{\frac{g(g+1)}{2}})$ in the superspecial graph, so the naïve classical algorithm takes time $\tilde{O}(p^{\frac{g(g+1)}{4}})$.

Note that supersingular non-superspecial surfaces are actually isogenous to reducible surfaces as well, but these isogenies are inseparable, and it is not known how to compute them efficiently (see Pieper [Pie21]) — thus the attack of Costello and Smith cannot be applied in the non-superspecial case.

3.3 Moving to the Supersingular Non-Superspecial graph

The attack on weak keys in Section 3.1 illustrates the choice that genus-2 cryptography practitioners have to make when using superspecial surfaces: A constant time implementation or the chance of protocol failures. Avoiding reducible surfaces by moving the to supersingular non-superspecial graph would remove that choice. Furthermore, this move would not degrade the security of the cryptosystems as we shall see in the next section.

For the remainder of this section, we discuss the advantages of moving to the supersingular non-superspecial graph; in particular, moving the to supersingular non-superspecial graph removes reducible surfaces from consideration.

3.3.1 Constant time algorithms with no failure conditions.

Indeed, the first two advantages are linked. Practitioners that employ genus-2 cryptosystems on the superspecial graph would have to choose between having a constant time implementation (by not preparing for reducible surfaces), or eliminating protocol failures (by preparing for reducible surfaces). Moving to the supersingular non-superspecial graph allows the user to have their cake and eat it too.

3.3.2 Eliminating weak keys.

Weak keys can manifest in schemes that work over the superspecial graph by when reducible surfaces are present in the path dictated by the keys. As we have seen at the start of this section, the presence of reducible surfaces in the paths can reduce the security of the keys significantly.

4 Supersingular Isogeny Graphs

In this section we will elaborate on the superspecial and supersingular non-superspecial isogeny graphs. We are interested in their number of vertices, their connectedness properties, their field of definition, and their overall structure.

4.1 The Number of Superspecial Curves

Recall the discussion about superspecial abelian surfaces in Section 2.1. It gives us a way of counting the number of isomorphism classes of principally polarised superspecial abelian surfaces via the following observation made by Ibukiyama et al. [IKO86].

Let B be the definite quaternion algebra over $\mathbb{Q}$ with discriminant D and let $\mathcal{O}$ be a maximal order of B. Write $D = D_1 D_2$ for two positive integers D_1, D_2 and set $L_n(D_1, D_2)$ the set of left $\mathcal{O}$-lattices in B^n which are equivalent to $(\mathcal{O} \otimes \mathbb{Z}_p)^n$ at p if p does not divide D_2, and otherwise to the other local equivalence class if p divides D_2. Denote by $H_n(D_1, D_2)$ the number of global equivalence classes in $L_n(D_1, D_2)$. In particular, for a prime number p, denote by $H_n(p, 1)$ the class number of the *principal genus* and by $H_n(1, p)$ the class number of the *non-principal genus*.

Let k be a algebraically closed field of characteristic p. As we saw, every principally polarised superspecial abelian surface A over k arises from choosing a principal polarisation on a product $E \times E$ for a supersingular elliptic curve E over k. Let $B_{p,\infty} = \mathrm{End}(E) \otimes \mathbb{Q}$ the endomorphism algebra of E, which is the definite quaternion algebra ramified at p. Then the number of principally polarisations on $E \times E$ up to automorphisms is equal to $H_2(p, 1)$ for $B_{p,\infty}$.

On the other hand, as a principally polarised abelian variety, either $A = E_1 \times E_2$ for two supersingular elliptic curves E_1 and E_2, or $A = \mathrm{Jac}(C)$ for a superspecial genus-2 curve C. Hence the number of isomorphism classes of superspecial genus-2 curves over k is given by $H_p = H_2(p, 1) - h_p(h_p + 1)/2$, where $h_p = H_1(p, 1)$ is the number of isomorphism classes of supersingular elliptic curves over k, see Ibukiyama et al. [IKO86, Corollary 2.12]. The number H_p is finite and behaves like $\Theta(p^3)$; every superspecial genus-2 curve can be defined over $\mathbb{F}_{p^2}$, see Ibukiyama and Katsura [IK94, Theorem 1].

This settles the question about the number of superspecial curves, but what about the supersingular non-superspecial ones? We will look at that in the next section.

4.2 The Number of Supersingular Non-Superspecial Curves

Consider the 3-dimensional coarse moduli space $\mathcal{M}_2(k)$ of isomorphism classes of genus-2 curves over a finite field k or characteristic p. Recall Table 1, which describes the stratification of the coarse moduli space of abelian surfaces in characteristic p. It induces a similar stratification of $\mathcal{M}_2(k)$.

In Section 4.1 we have seen that the number of superspecial abelian surfaces is finite, which matches the codimension 3 of the superspecial stratum in Table 1. On the other hand, the stratum containing the supersingular non-superspecial points is 1-dimensional and hence over $k = \overline{\mathbb{F}}_p$ there exist infinitely many isomorphism classes of supersingular non-superspecial genus-2 curves.

Since we require three *absolute invariants* (see Cardona, Quer, Nart, and Pujolàs [CQ05; CNP05]) to describe a point in $\mathcal{M}_2(k)$, for $k = \mathbb{F}_q$ the codimension-2 supersingular locus has $\Theta(q)$ elements, see also Zobernig [Zob21] for some exact results in small characteristic.

4.3 Supersingular Non-Superspecial Isogeny Graphs

Recall now the discussion of Section 2.3, specifically Theorem 4. Fix one supersingular non-superspecial abelian surface A, say corresponding to a choice of the embedding parameter $t \notin \mathbb{F}_{p^2}$. Then Theorem 4 tells us the number of principal polarisations $\mathcal{L}$ on A. All these tuples $(A, \mathcal{L})$ are the Jacobian of some supersingular non-superspecial genus 2 curve $H_{(A,\mathcal{L})}$ (with the canonical principal polarisation).

Fix some prime ℓ coprime to p. Then the vertices of the (ℓ,ℓ)-isogeny graph containing any $(A,\mathcal{L})$ ranges exactly over the abelian surfaces $(A,\mathcal{L})$ of possible principal polarisations $\mathcal{L}$ on A. It is defined over the field of definition of t; this can be seen using a similar argument as in Ibukiyama and Katsura [IK94]. It is furthermore connected; this can also be seen using a similar strong approximation argument as in Oort [Oor01, Lemma 7.9] Jordan and Zaytman [JZ20, Theorem 42]. Consider two surfaces $(A,\mathcal{L})$ and $(A,\mathcal{L}')$, corresponding to which we have two Hermitian matrices H and H', respectively. Then, by strong approximation, there exists a matrix M such that $M^{\dagger}HM = \ell^n H'$ for some large enough n. This corresponds to a chain of (ℓ,ℓ)-isogenies between the pair of surfaces $(A,\mathcal{L})$ and $(A,\mathcal{L}')$.

Hence, for a starting curve corresponding to $t \in \mathbb{F}_{p^4} \setminus \mathbb{F}_{p^2}$ we get an (ℓ,ℓ)-isogeny graph with $\Theta(p^6)$ vertices, and for $t \notin \mathbb{F}_{p^4}$ we get a graph with $\Theta(p^8)$ vertices.

4.4 Isogeny Graph Structure

In dimension one, for ordinary elliptic curves, we find volcanoes whose *crater* is a cyclic graph of length $\#\operatorname{Cl}(\mathcal{O}_K)$, where $\mathcal{O}_K$ is the ring of integers of some imaginary quadratic number field K. In particular, let D be the discriminant of $\mathcal{O}_K$ and denote by t the trace of Frobenius of any of the elliptic curves $E/\mathbb{F}_q$ in the volcano. Then the depth of the volcano is given by $\operatorname{ord}_\ell(v)$, where $4q = t^2 - v^2 D$.

These ordinary elliptic curve volcanoes can be *oriented* via the following observation: Over a fixed finite field $\mathbb{F}_q$, the depth of a volcano is finite. At the *floor*, all cyclic subgroups correspond to ascending isogenies, whereas on the crater we either have horizontal or descending isogenies. By using correctly the subgroup structure, we can make sure that we either ascend or descend the volcano and so reach the crater or the floor. Using this information, it is possible to compute explicitly the endomorphism ring $\operatorname{End}(E)$ of each elliptic curve E in the volcano.

In dimension two, isogeny graphs of ordinary abelian surfaces assemble into a similar volcano structure. On the other extreme, superspecial abelian surfaces form connected graphs which, unlike the supersingular isogeny graphs of elliptic curves, are not *Ramanujan graphs* in general but still *expander graphs*. They are in fact Ramanujan graphs only for a few small ground field primes and isogeny degrees, see Jordan and Zaytman [JZ20], and Aikawa et al. [ATY22].

As expected, for supersingular non-superspecial abelian surfaces we find a tree-like structure locally around vertices in the isogeny graph, see Amorós et al. [Amo+21] for a discussion of the underlying *Bruhat-Tits tree* in one dimension. But, most importantly, by restricting to the supersingular isogeny graph we do not end up with the same "orientability" concerns as in the case of ordinary elliptic curve volcanoes. The supersingular non-superspecial isogeny graph arranges into an infinite number of components, one for each supersingular non-superspecial abelian surface A corresponding to $t \notin \mathbb{F}_{p^2}$. Each of these components is made up of vertices corresponding to tuples $(A,\mathcal{L})$ for the finite set of possible principal polarisations $\mathcal{L}$ on A, and defined over the field of definition of t.

4.5 Constructing Supersingular Non-Superspecial Curves

We can use the following proposition to generate a starting curve H which is known to lie in the supersingular non-superspecial component of size $\Theta(p^6)$, for primes $p \equiv 2,3 \pmod 5$. Additionally, Ti et al. [TVZ22] give several methods to construct supersingular non-superspecial genus 2 curves using a complex multiplication method.

Proposition 6 (Ibukiyama et al. [IKO86], Proposition 1.13)**.** *Let $H : y^2 = x^5 - 1$ be a hyperelliptic curve over $\mathbb{F}_{p^r}$, where $p \neq 5$, then H is*

1. *ordinary if* $p \equiv 1 \pmod 5$*,*
2. *supersingular non-superspecial if* $p \equiv 2, 3 \pmod 5$*,*
3. *superspecial if* $p \equiv 4 \pmod 5$*.*

We can also answer in which component of the supersingular non-superspecial isogeny graph the Jacobian of the specific curve H of Proposition 6 lies.

Lemma 7. *Let* $p \equiv 2, 3 \pmod 5$*, then the Jacobian of the curve* $H : y^2 = x^5 - 1$ *is a principally polarised supersingular non-superspecial abelian surfaces corresponding to an embedding parameter* $t \in \mathbb{F}_{p^4} \setminus \mathbb{F}_{p^2}$*.*

Proof. The geometric automorphism group of H is $\mathbb{Z}/10\mathbb{Z}$, and so the result follows from Proposition 6 and Theorem 4. □

Hence, if we choose a prime $p \equiv 2, 3 \pmod 5$, the curve $H : y^2 = x^5 - 1$ lies in a connected component of the supersingular non-superspecial isogeny graph which is defined over $\mathbb{F}_{p^4}$, with $\Theta(p^6)$ vertices.

4.6 Examples

We start with an example graph for the curve $H : y^2 = x^5 - 1$ over $\mathbb{F}_{7^4}$. The $(2, 2)$-isogeny graph in Figure 1 has 40 vertices, see also Theorem 4.

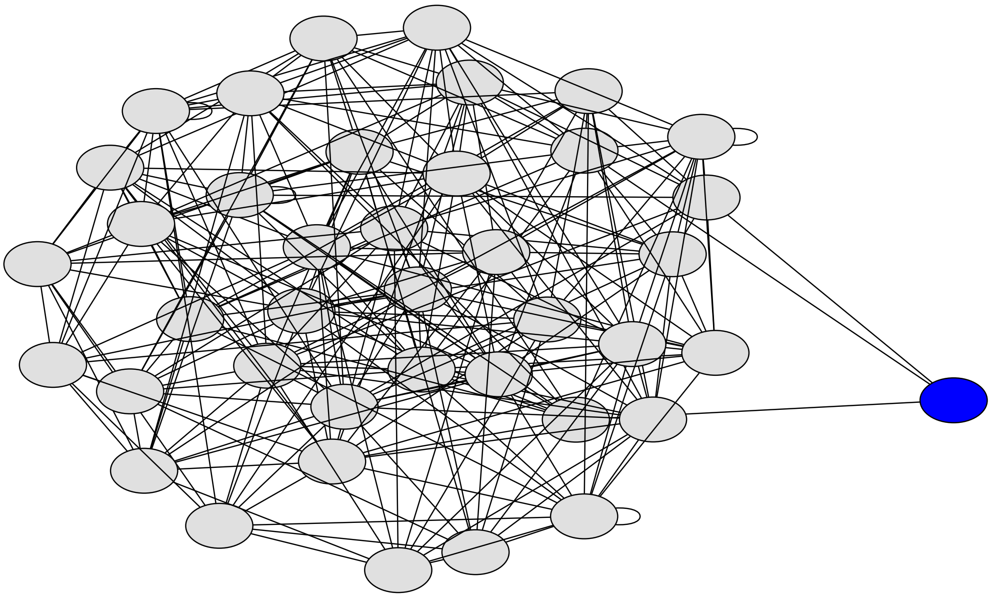

Figure 1: The curve $H : y^2 = x^5 - 1$ sitting in the $(2, 2)$-isogeny graph whose edges are given by $(2, 2)$-isogenies defined over $\mathbb{F}_{7^4}$. The vertex corresponding to the curve H is drawn in blue. Multiple edges are collapsed into one.

Let us also look at an example of a larger graph. One can check that the curve

$$H : y^2 = 10x^6 + 2x^5 + 3x^4 + 9x^3 + 5x^2 + 5x + 4$$

over $\mathbb{F}_{11}$ with absolute invariants $(0, 6, 8)$ is supersingular non-superspecial. The $(2, 2)$-isogeny graph containing H is given in Figure 2. It has 605 vertices and is defined over $\mathbb{F}_{11^4}$, hence we know that the Jacobian of H must correspond to an embedding parameter $t \in \mathbb{F}_{11^4} \setminus \mathbb{F}_{11^2}$.

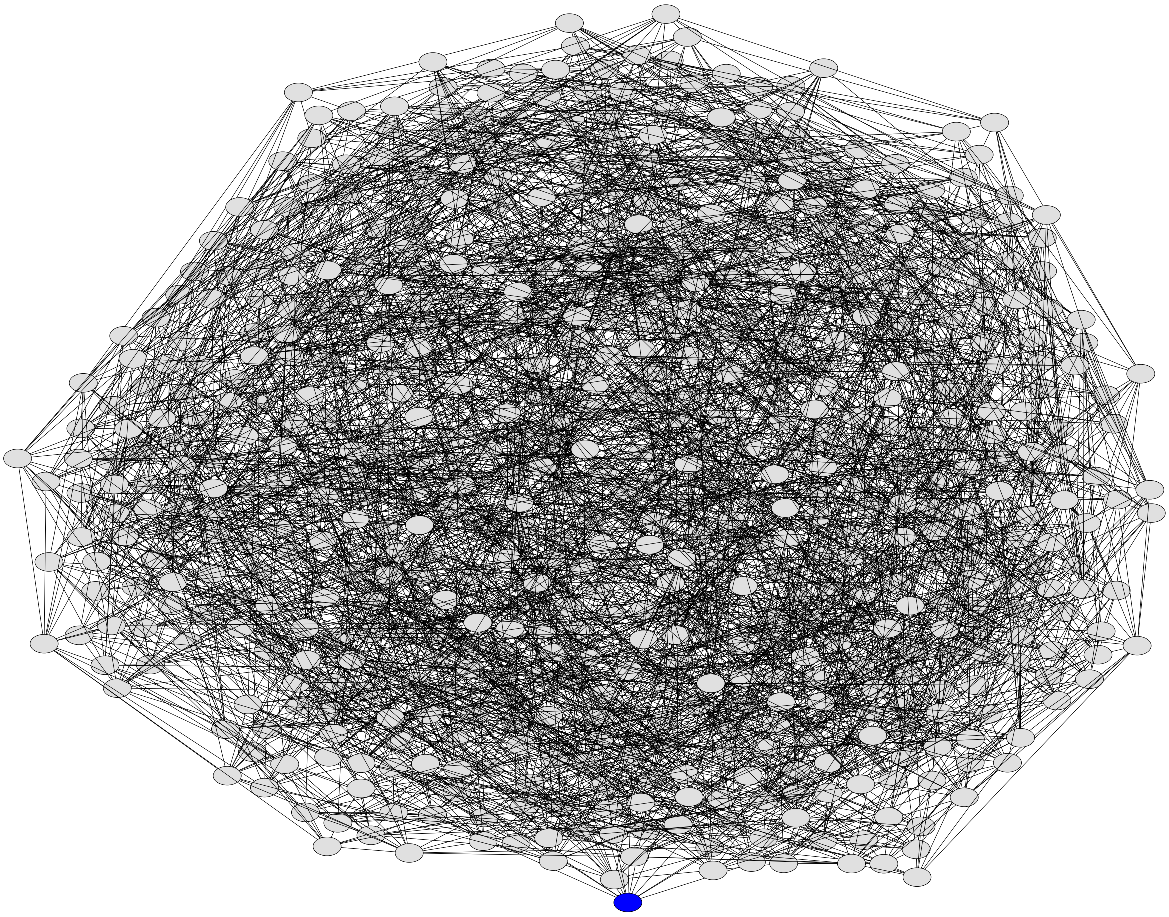

Figure 2: The curve H sitting in the $(2, 2)$-isogeny graph whose edges are given by $(2, 2)$-isogenies defined over $\mathbb{F}_{11^4}$. The vertex corresponding to the curve H is drawn in blue. Multiple edges are collapsed into one.

In Figure 3 we only show vertices that are at most two edges from our starting curve H. This gives a better understanding of the local tree-like structure in the supersingular non-superspecial isogeny graph.

5 Protocols in Supersingular Non-Superspecial Components

In this section we discuss parameter choices and security of genus-2 isogeny-based protocols in supersingular non-superspecial components, and compare against the corresponding superspecial protocols CDS and G2SIDH.

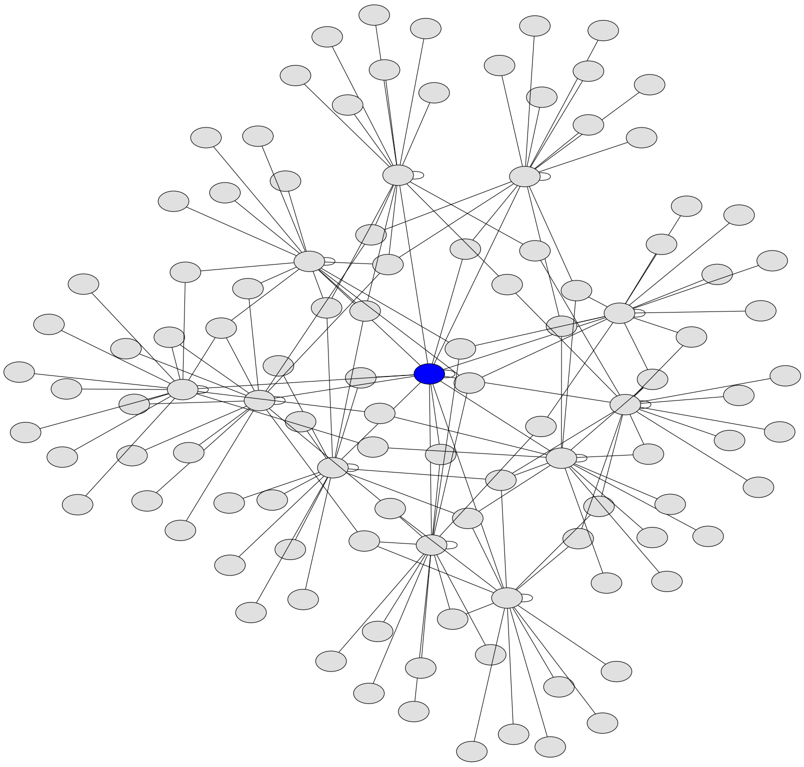

Figure 3: The local neighbourhood of the curve H in the $\mathbb{F}_{p^4}$-subgraph of the $(2,2)$-isogeny graph. The vertex corresponding to the curve H is drawn in blue. Multiple edges are collapsed into one.

5.1 Hash Functions in Supersingular Non-Superspecial Components

By Lemma 7 and the work of Section 4.3, for any primes $p \equiv \pm 2 \pmod 5$ and $\ell \neq p$, the hyperelliptic curve $H\colon y^2 = x^5 - 1$ is in the supersingular non-superspecial component whose edges are (ℓ, ℓ)-isogenies defined over $\mathbb{F}_{p^4}$.

The techniques of [CDS20, Propositions 1 and 3] yield a hash function in a straightforward fashion: Given a message $m = m_{n-1}m_{n-2}\cdots m_0 \in \{0,1\}^{3n}$, we construct a "good" sequence[2] of n $(2,2)$-isogenies by processing $m_0, m_1, \ldots, m_{n-1}$ in sequence; in particular, associate to each binary string of length three one of the eight kernels given in [CDS20, Proposition 3], and follow the kernel corresponding to m_0, then m_1, and so on until m_{n-1}. Together this path corresponds to an $(2^n, 2^n)$-isogeny with codomain H'; we set the output of our hash function to be the absolute invariants of H'.

This hash function is preimage resistant and collision resistant, respectively, under the assumption that each of the follow computational problems is hard.

Problem 8. *Given a prime p and two supersingular non-superspecial genus-2 curves $H/\overline{\mathbb{F}}_p, H'/\overline{\mathbb{F}}_p$ whose embedding parameter t satisfies $t \in \mathbb{F}_{p^4} \setminus \mathbb{F}_{p^2}$, find a $(2^n, 2^n)$-isogeny $\phi\colon J_H \to J_{H'}$.*

[2] These sequences are constructed to avoid the "trivial cycles" that arise from ℓ-diamonds (see Flynn and Ti [FT19]), which were present in the hash function of Takashima [Tak18].

Problem 9. *Given a prime p and a supersingular non-superspecial curve $H/\overline{\mathbb{F}}_p$ whose embedding parameter t satisfies $t \in \mathbb{F}_{p^4} \setminus \mathbb{F}_{p^2}$, find:*

1. *A $(2^n, 2^n)$-isogeny $\phi\colon H \to H'$*
2. *A $(2^{n'}, 2^{n'})$-isogeny $\phi'\colon H \to H''$*

such that $\ker\phi \neq \ker\phi'$ *and $J_{H'}$ is $\overline{\mathbb{F}}_p$-isomorphic to $J_{H''}$.*

These problems are precisely analogous to [CDS20, Problems 1 and 2].

As there are $\Theta(p^6)$ vertices in this supersingular non-superspecial component, generic classical algorithms yield preimages or collisions in time $\tilde{O}(p^3)$. Much the same is true in the quantum setting; though some generic algorithms boast complexity $\tilde{O}(p^2)$ for Problems 8 and 9, Jaques and Schanck [JS19] suggest that these algorithms do not outperform the classical square-root algorithms in practice due to overhead introduced by the required data structures. Thus to achieve λ bits of (classical or quantum) security, we should take $\log_2 p \approx \frac{\lambda}{3}$. This is half the bit length of the required characteristic in the superspecial graph [CDS20, §8], and one-third the bit length of the required in the supersingular graph in genus 1 [CLG07]. The output of the hash function is a triple of elements of $\mathbb{F}_{p^4}$, so this has total bit length 2λ — the same as [CLG07] and [CDS20].

5.2 Key Exchange in Supersingular Non-Superspecial Components

Abstractly, G2SIDH key exchange works in a supersingular non-superspecial component in much the same way as described in Section 2.4, simply by starting from a supersingular non-superspecial hyperelliptic curve H. The only major complication is in choosing H: Ideally it would be chosen such that its embedding parameter t satisfies $t \in \mathbb{F}_{p^4} \setminus \mathbb{F}_{p^2}$ (so that it lies in the component of size $\Theta(p^6)$) and its Jacobian satisfies $\#J_H(\mathbb{F}_{p^4}) = (p+1)^8 = 2^{8e_A}3^{8e_B}f^8$ (and we would work in a field of characteristic p whose bit length is half that of the primes used in G2SIDH). Unfortunately our distinguished curve $H\colon y^2 = x^5 - 1$ does not satisfy this order condition; however, techniques of the kind used in [TVZ22] can be used to find an appropriate starting curve.

6 Conclusion and Open Questions

We have shown that it is sensible to work in supersingular non-superspecial isogeny graphs. Doing so circumvents several problems we find in the superspecial graph which stem from the fact that there we encounter two types of vertices: Jacobians of genus 2 curves and reducible surfaces in the form of products of elliptic curves. On the other hand, in supersingular non-superspecial graphs we find only Jacobians as vertices and do not need to make explicit distinctions for different vertex types. Finally, we leave the reader with several open questions begging for future research:

- Determine exactly the expansion coefficients of the various supersingular genus 2 graphs (superspecial and supersingular non-superspecial components), as mentioned in Section 4.4. One possible approach would be to study Hecke operators acting on automorphic forms of Hermitian quaternionic lattices corresponding to the principal polarisations of supersingular non-superspecial abelian surfaces, c.f. [Piz90; ATY22].

- Determine efficient parameters and good starting curves for key exchange using supersingular non-superspecial isogeny graphs.

- Work out efficient algorithms for computing (ℓ, ℓ)-isogenies for $\ell > 3$.

References

[Amo+21] Laia Amorós, Annamaria Iezzi, Kristin Lauter, Chloe Martindale, and Jana Sotáková. "Explicit Connections Between Supersingular Isogeny Graphs and Bruhat–Tits Trees". In: *Women in Numbers Europe III: Research Directions in Number Theory*. Springer, 2021, pp. 39–73.

[ATY22] Yusuke Aikawa, Ryokichi Tanaka, and Takuya Yamauchi. *Isogeny graphs on superspecial abelian varieties: Eigenvalues and Connection to Bruhat-Tits buildings*. 2022. URL: https://arxiv.org/abs/2201.04293.

[Aza+20] Reza Azarderakhsh, Matthew Campagna, Craig Costello, Luca De Feo, Basil Hess, Amir Jalali, Brian Koziel, Brian LaMacchia, Patrick Longa, Michael Naehrig, Geovandro Pereira, Joost Renes, Vladimir Soukharev, and David Urbanik. *Supersingular Isogeny Key Encapsulation*. Tech. rep. https://sike.org/files/SIDH-spec.pdf. 2020.

[BIJ18] Jean-François Biasse, Annamaria Iezzi, and Michael J. Jacobson. "A Note on the Security of CSIDH". In: *Progress in Cryptology – INDOCRYPT 2018*. Springer, 2018, pp. 153–168.

[BK65] Hel Braun and Max Koecher. *Jordan Algebren*. Grundlehren der mathematischen Wissenschaften, Volume 128. Springer, 1965.

[Brö09] Reinier Bröker. "Constructing supersingular elliptic curves". In: *Journal of Combinatorics and Number Theory* 1.3 (2009), pp. 269–273.

[BS20] Xavier Bonnetain and André Schrottenloher. "Quantum Security Analysis of CSIDH". In: May 2020, pp. 493–522.

[Cas+18] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. "CSIDH: An Efficient Post-Quantum Commutative Group Action". In: *Advances in Cryptology – ASIACRYPT 2018*. Springer, 2018, pp. 395–427.

[CDS20] Wouter Castryck, Thomas Decru, and Benjamin Smith. "Hash functions from superspecial genus-2 curves using Richelot isogenies". In: *J. Math. Cryptol.* 14.1 (2020), pp. 268–292.

[CLG07] Denis X. Charles, Kristin E. Lauter, and Eyal Z. Goren. "Cryptographic hash functions from expander graphs". In: *Journal of Cryptology* 22.1 (Sept. 2007), pp. 93–113.

[CNP05] Gabriel Cardona, Enric Nart, and Jordi Pujolàs. "Curves of genus two over fields of even characteristic". In: *Mathematische Zeitschrift* 250.1 (2005), pp. 177–201.

[Cou06] Jean-Marc Couveignes. *Hard homogeneous spaces*. Cryptology ePrint Archive, Report 2006/291. https://ia.cr/2006/291. 2006.

[CQ05] Gabriel Cardona and Jordi Quer. "Field of moduli and field of definition for curves of genus 2". In: *Computational Aspects of Algebraic Curves*. 2005, pp. 71–83.

[CS20] Craig Costello and Benjamin Smith. "The Supersingular Isogeny Problem in Genus 2 and Beyond". In: *Post-Quantum Cryptography - 11th International Conference, PQCrypto 2020*. Vol. 12100. Lecture Notes in Computer Science. Springer, 2020, pp. 151–168.

[DFKS18] Luca De Feo, Jean Kieffer, and Benjamin Smith. "Towards Practical Key Exchange from Ordinary Isogeny Graphs". In: *Advances in Cryptology – ASIACRYPT 2018*. Springer, 2018, pp. 365–394.

[DH76] Whitfield Diffie and Martin E. Hellman. "New directions in cryptography". In: *IEEE Transactions on Information Theory* 22.6 (1976), pp. 644–654.

[FT19] E. Victor Flynn and Yan Bo Ti. "Genus Two Isogeny Cryptography". In: *Post-Quantum Cryptography - 10th International Conference, PQCrypto 2019*. Vol. 11505. Lecture Notes in Computer Science. Springer, 2019, pp. 286–306.

[Ibu20] Tomoyoshi Ibukiyama. "Principal polarizations of supersingular abelian surfaces". In: *Journal of the Mathematical Society of Japan* 72.4 (2020), pp. 1161 –1180.

[IK94] Tomoyoshi Ibukiyama and Toshiyuki Katsura. "On the field of definition of superspecial polarized abelian varieties and type numbers". In: *Compositio Mathematica* 91.1 (1994), pp. 37–46.

[IKO86] Tomoyoshi Ibukiyama, Toshiyuki Katsura, and Frans Oort. "Supersingular curves of genus two and class numbers". In: *Compositio Mathematica* 57.2 (1986), pp. 127–152.

[Jao+20] David Jao, Jason LeGrow, Christopher Leonardi, and Luis Ruiz-Lopez. "A subexponential-time, polynomial quantum space algorithm for inverting the CM group action". In: *Journal of Mathematical Cryptology* 14.1 (2020), pp. 129–138.

[JDF11] David Jao and Luca De Feo. "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies". In: *Post-Quantum Cryptography*. Springer Berlin Heidelberg, 2011, pp. 19–34.

[JS19] Samuel Jaques and John M. Schanck. "Quantum Cryptanalysis in the RAM Model: Claw-Finding Attacks on SIKE". In: *Advances in Cryptology – CRYPTO 2019*. Springer, 2019, 32–61.

[JZ20] Bruce W. Jordan and Yevgeny Zaytman. *Isogeny graphs of superspecial abelian varieties and Brandt matrices*. 2020. URL: https://arxiv.org/abs/2005.09031.

[Kup05] Greg Kuperberg. "A Subexponential-Time Quantum Algorithm for the Dihedral Hidden Subgroup Problem". In: *SIAM Journal on Computing* 35.1 (2005), pp. 170–188.

[Mil86] J. S. Milne. "Jacobian Varieties". In: *Arithmetic Geometry*. Springer, 1986, pp. 167–212.

[Mum08] David Mumford. *Abelian varieties*. Vol. 5. Tata Institute of Fundamental Research Studies in Mathematics. Hindustan Book Agency, New Delhi, 2008.

[Oor00] Frans Oort. "Newton Polygons and Formal Groups: Conjectures by Manin and Grothendieck". In: *Annals of Mathematics* 152.1 (2000), pp. 183–206.

[Oor01] Frans Oort. "A Stratification of a Moduli Space of Abelian Varieties". In: *Moduli of Abelian Varieties*. Birkhäuser, 2001, pp. 345–416.

[Oor75] Frans Oort. "Which Abelian Surfaces are Products of Elliptic Curves?" In: *Mathematische Annalen* 214 (1975), pp. 35–48.

[Pie21] Andreas Pieper. *Constructing all Genus 2 Curves with Supersingular Jacobian*. 2021. URL: https://arxiv.org/abs/2105.13752.

[Piz90] Arnold K. Pizer. "Ramanujan graphs and Hecke operators". In: *Bulletin of the American Mathematical Society* 23.1 (1990), pp. 127 –137.

[Piz98] Arnold K. Pizer. "Ramanujan Graphs". In: *Computational Perspectives on Number Theory* (1998), pp. 159–178.

[Pri08] Rachel Pries. "A short guide to p-torsion of abelian varieties in characteristic p". In: *Computational arithmetic geometry*. Vol. 463. Contemporary Mathematics. American Mathematical Society, 2008, pp. 121–129.

[Reg04] Oded Regev. *A Subexponential Time Algorithm for the Dihedral Hidden Subgroup Problem with Polynomial Space*. 2004. URL: https://arxiv.org/abs/quant-ph/0406151.

[RS06] Alexander Rostovtsev and Anton Stolbunov. *Public-key cryptosystem based on isogenies*. Cryptology ePrint Archive, Report 2006/145. https://ia.cr/2006/145. 2006.

[Tak18] Katsuyuki Takashima. "Efficient algorithms for isogeny sequences and their cryptographic applications". In: *Mathematical modelling for next-generation cryptography*. Springer, 2018, pp. 97–114.

[TVZ22] Yan Bo Ti, Gabriel Verret, and Lukas Zobernig. *Abelian Varieties with p-rank Zero*. 2022. URL: https://arxiv.org/abs/2203.08401.

[Vél71] Jacques Vélu. "Isogénies entre courbes elliptiques". In: *C. R. Acad. Sci. Paris Sér. A-B* 273 (1971), A238–A241.

[Zob21] Lukas Zobernig. *Genus 2 Curves in Small Characteristic*. 2021. URL: https://arxiv.org/abs/2111.07270.