Reducible gluing of abelian varieties

DAMIEN ROBERT

Abstract. This note extend Kani's work on reducible gluing of elliptic curves to abelian varieties.

1. Introduction

Kani's lemma [Kan97, § 2] has been a hot topic in isogeny based cryptography [CD22; MM22; Rob22a; Rob22b]. It is easy to extend it to abelian varieties, see [Rob22a, Lemma 3.4]. But Kani's work on reducible gluing of elliptic curves in [Kan97] goes further than just this lemma. The purpose of these notes is to cover the extension of Kani's work to higher dimensional abelian varieties. This is mostly a straightforward adaptation of Kani's proofs from elliptic curves to abelian varieties, with a few subtleties stemming from the fact that maximal isotropic kernels in abelian varieties are not always nicely described.

Kani's work in [Kan97, § 2] cover three related topics: how to combine an N_1-isogeny $f_1 : E_0 \to E_1$, and a N_2-isogeny $f_2 : E_0 \to E_2$ into an N_1+N_2-isogeny $F : E_0 \times E_0' \to E_1 \times E_2$, why they are all of this form, and describe the kernel of F. The applications mentioned above only really need the case where N_1 is prime to N_2 which simplify things. Nevertheless, the general case is interesting and Kani deals with it in details for elliptic curves. In Section 3 we show how his results extend to dimension g abelian varieties. But first we need to describe maximal isotropic subgroups in more details, this is done in Section 2.

Throughout these notes we only deal with separable isogenies. In particular, when looking at N-isogenies, we implicitly restrict to the case where N is prime to the characteristic p of the base field (or $p = 0$).

2. Maximal isotropic kernels

Let (A, λ_A) be a ppav.

Definition 2.1. A subgroup $K \subset A[N]$ is called isotropic (with respect to the Weil pairing $e_{A,N}$ on A) if $K \subset K^{\perp}$, ie if $e_{A,N}(P,Q) = 1$ for all $P, Q \in K$.

In the theory of bilinear form, such a subgroup K is usually called totally isotropic. An isotropic subgroup $H \subset G$ for a quadratic form q on G usually means that there is an isotropic element $x \neq 0 \in H$, ie such that $q(x) = 0$. However, since $e_{A,N}$ is alternating, every non trivial subgroup of $A[N]$ is isotropic in this sense.

Lemma 2.2. *Let $K \subset A[N]$ be a subgroup. The following are equivalent:*

(1) *K is isotropic, and maximal among isotropic kernels (ie K is maximal isotropic);*
(2) *$K = K^{\perp}$.*
(3) *K is isotropic of cardinal N^g.*

Date: September 26, 2022.

Proof. 1 ⇒ 2 ⇒ 3 ⇒ 1, using that $\#K^{\perp}\#K = N^{2g}$ since $e_{A,N}$ is symplectic, which shows that in particular an isotropic group has cardinal $\#K \leq N^g$. □

Lemma 2.3. *Let K be a maximal isotropic subgroup and $\ell \mid \#K$. Then $K[\ell]$ is of dimension at least g (over $\mathbb{Z}/\ell\mathbb{Z}$), so contains a maximal isotropic subgroup K' for $A[\ell]$.*

Proof. By the symplectic CRT theorem, we may assume $N = \ell^e$. If $K[\ell]$ was of dimension $r < g$, we would have $\#K \leq (\ell^e)^r < (\ell^e)^g$, and K would not be maximal. So $K[\ell]$ is of rank $r \geq g$, hence we can always extract an isotropic subgroup of rank g by the structure theorem of symplectic vector spaces. (Be careful that K itself will not be isotropic for $A[\ell]$ if $r > g$). □

Corollary 2.4. *Every N-isogeny can be decomposed as product of ℓ_i-isogenies with $N = \prod \ell_i$.*

If K is a finite abelian group, we define its rank r has the minimal integer r such that there exists a surjection $\mathbb{Z}^r \to K$. This is also the number of elementary divisors $d_1 \mid d_2 \mid \ldots d_r$ with $d_1 \neq 1$, giving the structure $K \simeq \prod \mathbb{Z}/d_i\mathbb{Z}$. This is also the maximum of the dimensions of the $K[p]$ as a $\mathbb{Z}/p\mathbb{Z}$ vector space over all p (dividing $\#K$). We call a "basis" of K a system of generators $(g_1, \ldots, g_r)$ of cardinal r.

Lemma 2.5. *A maximal isotropic kernel $K \subset A[N]$ of rank g always has an isotropic complement K', meaning that $A[N] = K \oplus K'$ is a symplectic decomposition. In particular, if $(e_1, \ldots, e_g)$ is a basis of K, it extends into a symplectic basis $(e_1, \ldots, e_g, f_1, \ldots f_g)$ of $A[N]$, and if $m \mid N$, $K[m]$ is maximal isotropic in $A[m]$.*

Proof. By the symplectic CRT theorem, we may reduce to the case $N = \ell^g$. Since K is of rank g and is of cardinal ℓ^g, it is homogeneous. It has a symplectic complement by [PSV10, Theorem 10.14]. □

Example 2.6. In $A[\ell]$ (with ℓ prime) an isotropic subgroup K is maximal iff it is of rank g (by the structure theorem of symplectic vector spaces).

Lemma 2.7. *If $K \subset A[\ell^e]$ is homogeneous (all its invariants are equal), it is either of rank g or of rank $2g$, In the latter case, $e = 2f$ and $K = A[\ell^f]$.*

If $K \subset A[N]$ is homogeneous or more generally if each ℓ-Sylow of K is homogeneous (this condition is equivalent to, if $d_1 \mid \cdots \mid d_{2g}$ are the invariants of H where d_i is allowed to be 1, then each prime divisor ℓ of N divides at most one quotient d_{i+1}/d_i), then $N = N_1^2 N_2$ with $\gcd(N_1, N_2) = 1$, $K[N_1^2] = K[N_1] = A[N_1]$ *and $K[N_2]$ maximal isotropic of rank g in* $A[N_2]$.

Proof. By [PSV10, Theorem 10.14], K is standard (see below). Let $(e_1, \ldots, e_g, f_1, \ldots, f_g)$ a symplectic basis of $A[N]$ adapted to a standard decomposition $K = K_1 \oplus K_2$. Then since K is homogeneous, either K has for basis (say) $(e_1, \ldots, e_k, f_{k+1}, \ldots f_g)$ so it has rank g, or for basis $(\ell^f e_1, \ldots, \ell^f e_g, \ell^f f_1, \ldots \ell^f f_g)$ with $e = 2f$.

The general case comes from the symplectic CRT. □

It is often convenient to treat the case of maximal isotropic subgroups of the form $A[n]$ and those of rank g together. The following notion encompass these two cases:

Lemma 2.8. *Let $A[N] = A_1[N] \oplus A_2[N]$ be a symplectic decomposition. Let $K_1 \subset A_1[N]$ be any subgroup. Let $K_2 = K_1^{\perp} \cap A_2[N]$. Then $K = K_1 \oplus K_2$ is maximal isotropic. Conversely, if $K = K_1 \oplus K_2$ is maximal isotropic with $K_i \subset A_i[N]$, then $K_2 = K_1^{?} \cap A_2[N]$.*

Proof. K_2 is orthogonal to K_1 by definition, and orthogonal to itself because it lives in $A_2[N]$. Hence K is isotropic. We have $K_1^? = A_1[N] \oplus K_2$, so since $K_1^{??} = K_1$, $K_2^? = K_1 \oplus A_2[N]$. So $K^? = K_1^? \cap K_2^? = K$, hence K is maximal isotropic. The converse follows by the same calculation. □

Definition 2.9. A isotropic subgroup K is called standard if there is a symplectic decomposition $A[N] = A_1[N] \oplus A_2[N]$ such that $K = K_1 \oplus K_2$ where $K_i = K \cap A_i[N]$.

In particular, if $K = K_1 \oplus K_2$ is a standard isotropic subgroup, $K_2 \subset K_1^\perp \cap A_2[N]$, and by Lemma 2.8, K is maximal iff we have equality.

Example 2.10.

- a maximal isotropic kernel of rank g is standard by Lemma 2.5.
- a homogeneous maximal isotropic kernel is standard by Lemma 2.7.
- For an elliptic curve, a maximal isotropic subgroup $K \subset E[N]$ is always of the form $K = \langle P, Q \rangle$ where $P = me_1$, $Q = nf_1$ with (e_1, f_1) a symplectic basis of $E[N]$, $m \mid n$ and $N = mn$. In particular, K is standard.

  If $m = 1$, $K = \langle P \rangle$ is cyclic. If $m = n$, $K = E[n] \subset E[n^2]$. Since an isogeny $f : E \to E'$ of degree N is always an N-isogeny, $K = \operatorname{Ker} f$ is maximal isotropic, and f decomposes as $f = g \circ [m]$, where g has cyclic kernel, where m is as above for K.
- Let (e_1, e_2, f_1, f_2) be a symplectic basis of $A[\ell^2]$, A an abelian surface. Then $K = \langle e_1, e_2 \rangle$ is maximal isotropic of rank $g = 2$.

  $K = \langle e_1, \ell e_2, \ell f_2 \rangle$ is standard of rank 3. Notice that $K[\ell]$ is not isotropic in $A[\ell]$.
- In higher dimension, not every maximal isotropic kernel is standard [PSV10, Theorem 10.13].

The nice thing about standard maximal isotropic subgroups is that we can reduce to hyperbolic planes.

Lemma 2.11. *Let $A[N] = \oplus_{i=1}^g H_i$ be a symplectic decomposition of $A[N]$ into hyperbolic planes (ie a subgroup of rank 2 such that the symplectic forms stay non degenerate), $K_i \subset H_i$ an isotropic subgroup of H_i and $K = \oplus_{i=1}^g K_i$. Then K is standard isotropic, and is maximal iff each K_i is maximal in H_i.*

Conversely, if K is maximal standard isotropic, then there exists a symplectic decomposition $A[N] = \oplus_{i=1}^g H_i$ such that $K = \oplus_{i=1}^g K \cap H_i$.

Proof. By the symplectic CRT, we reduce to the case $N = \ell^e$. Each $K_i \subset H_i$ is standard in H_i by Example 2.10. Let (e_i, f_i) be a symplectic basis of H_i, these glue together to form a symplectic basis of $A[N]$, hence a symplectic decomposition of $A[N]$. This shows that $K = \oplus_{i=1}^g K_i$ is standard. Furthermore, $K^\perp \cap H_i = K_i^{\perp_{H_i}}$, so K is maximal in $A[N]$ iff each K_i is maximal in H_i.

Conversely, let $K = K_1 \times K_2$ be a decomposition of a maximal standard isotropic K induced by a symplectic decomposition of $A[N]$. Take $(e_1, \dots, e_g)$ a basis of $A_1[N]$ compatible with K, ie such that $K = \oplus_{i=1^g} K \cap \langle e_i \rangle$. This is possible because $A_1[N]$ is homogeneous. Then the dual basis $(f_1, \dots, f_g)$ of $A_2[N]$ with respect to $(e_1, \dots, e_g)$ is adapted to K_2 because $K_2 = K_1^\perp \cap A_2[N]$. Letting $H_i = (e_i, f_i)$, we get that $K = \oplus_{i=1}^g K \cap H_i$. □

3. Gluing abelian varieties

We generalize Kani's study of gluing of elliptic curves [Kan97, § 2] to the case of abelian varieties. As mentioned in the introduction, this is mostly a straightforward generalisation of his proofs.

3.1. **Gluing.** Let A, B be two abelian varieties of dimension g. A gluing $F : A \times B \to C$ is an isogeny from the product $A \times B$ to a dimension $2g$ abelian variety C. An uninteresting case is when F can be written as a diagonal isogeny $F = (f_1, f_2) : A \times B \to A' \times B'$ where $f_1 : A \to A'$ and $f_2 : B \to B'$ are two isogenies. More generally, if $\operatorname{Ker} F = H_A \times H_B$ then F is the composition of a diagonal isogeny followed by an automorphism. We call such a F a product gluing (because its kernel is a diagonal product).

We will look at the case when A, B are principally polarised, and F is an N-isogeny. Note that in the case of a product isogeny $F = (f_1, f_2)$, if f_1 is an N_1-isogeny and f_2 a N_2-isogeny, then F is a (N_1, N_2)-isogeny.

We will call F a *minimal gluing* if it does not factorize through such a *product gluing*. An equivalent condition is that $\operatorname{Ker} F \cap A \times 0 = \{0\}$ and $\operatorname{Ker} F \cap 0 \times B = \{0\}$. Let $g_1 = \dim A$, $g_2 = \dim B$, and F be a N-minimal gluing. Then the projections p_A and p_B are injective on $\operatorname{Ker} F$. Since $\operatorname{Ker} F$ is maximal isotropic in $(A \times B)[N]$, it is of cardinal $N^{g_1+g_2}$, so we get that $g_1 + g_2 \leq 2g_1$ and $g_1 + g_2 \leq 2g_2$, so $g_1 = g_2$. Henceforth, we let $g = g_1 = g_2$.

Lemma 3.1. *Let $\psi : A[N] \to B[N]$ be an anti-isometry with respect to the Weil pairing. Then $K = \{(P, \psi(P) \mid P \in A[N]\}$ is the kernel of a minimal N-gluing $F : A \to B \times C$. Conversely, the kernel* $\operatorname{Ker} F$ *of a minimal N-gluing is of this form. Furthermore, to check that F is minimal it suffices to check that* $\operatorname{Ker} F \cap 0 \times B = 0$ *or* $\operatorname{Ker} F \cap A \times 0 = 0$.

Proof. Let F be a minimal gluing and $K = \operatorname{Ker} F$. Since $K \cap 0 \times B = \{0\}$, the projection $p_A : A \times B \to A$ is injective on K. Since $K \subset (A \times B)[N]$ is maximal isotropic in the N-torsion, it is of cardinal N^{2g}, so the image of K is surjective in $A[N]$. Hence $p_A^{-1} : A[N] \to K$ is well defined, and composing with p_B we see that there is a well defined function ψ such that $K = \{(P, \psi(P)) \mid P \in A[N]\}$.

Since K is maximal isotropic, we get $e_{A \times B, N}((P_1, \psi(P_1)), (P_2, \psi(P_2))) = e_{A,N}(P_1, P_2) e_{B,N}(\psi(P_1), \psi(P_2)) = 1$, so $\psi : A[N] \to B[N]$ is an anti-isometry.

Conversely, the same computation shows that if ψ is an anti-isometry, $K = \{(P, \psi(P) \mid P \in A[N]\}$ is isotropic in $(A \times B)[N]$, hence is maximal isotropic since it is of cardinal N^{2g}. Furthermore, since ψ is an anti-isometry, it is injective (hence bijective), so $K \cap A \times 0 = 0$. This proves the last statement. □

Remark 3.2. Since $(1, -1)$ and $(-1, 1)$ are automorphisms of $A \times B$, the kernel $K' = \{(P, -\psi(P) \mid P \in A[N]\}$ also define a minimal N-gluing which is isomorphic to the one associated to K.

3.2. **Reducible gluing.** Now it can happen that in a minimal gluing $F : A \times B \to C$, C splits into a product even when F is not a product isogeny. We say that F is reducible.

When $g = 1$, in that case C splits as a product of elliptic curves, so $F = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ is automatically a matrix of n-isogenies (n depending on the component), because elliptic curves have their Neron-Severi group of rank 1 (ie is trivial). In dimension $g > 1$, C may not split into a product of two dimension g abelian varieties. And even if it does, the matrix $F = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ may not be given by individual n-isogenies if A or B has non trivial Neron-Severi group.

Definition 3.3. A (minimal) gluing $F : A \times B \to C$ is said to be reducible if $C \simeq A' \times B'$ with A', B' of dimension g, and $F = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ is given by a n_a-isogeny $a : A \to A'$, a n_b-isogeny $A \to B'$, a n_c-isogeny $c : B \to A'$ and a n_d-isogeny $d : B \to B'$. It is said to be non trivial reducible if F is not a product gluing.

Here by abuse of notation, we allow the case $n = 0$, where the notion of "0-isogeny" means that the morphism is 0 (so is not an actual isogeny).

Lemma 3.4. *Let F be a reducible N-gluing. Then $F = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$, with $n_a = n_d$, $n_b = n_c$, $n_a + n_b = N$, $\tilde{c}a = -\tilde{d}b$.*

In particular, F is not diagonal iff $n_b = n_c \neq 0$.

Proof. The contragredient isogeny is given by $\tilde{F} = \begin{pmatrix} \tilde{a} & \tilde{b} \\ \tilde{c} & \tilde{d} \end{pmatrix}$, and the equation $\tilde{F}F = N$ gives $n_a + n_b = N$, $n_c + n_d = N$, $\tilde{a}c + \tilde{b}d = 0$, $\tilde{c}a + \tilde{d}b = 0$. By duality the last equation is already implied by the third one. The third equation also implies $n_a n_c = n_b n_d$, so $n_a = n_d$, $n_b = n_c$. □

3.3. **Isogeny diamonds.** Lemma 3.4 shows that the following notion is natural:

Definition 3.5. A (n_1, n_2)-isogeny diamond is a decomposition of a $n_1 n_2$-isogeny $f : A \to B$ between principally polarised abelian varieties into two different decompositions $f = f_1' \circ f_1 = f_2' \circ f_2$ where f_1 is a n_1-isogeny and f_2 is a n_2-isogeny. (Then f_1' will be a n_2-isogeny and f_2' a n_1-isogeny.) This decomposition is said to be minimal if $\operatorname{Ker} f_1 \cap \operatorname{Ker} f_2 = \{0\}$ (this is equivalent to the fact that f_1 and f_2 do not factorize through a common isogeny), and it is said to be orthogonal if n_1 is prime to n_2 (in which case it is automatically minimal).

$$\begin{tikzcd}
A \arrow[r, "f_1"] \arrow[d, "f_2"] & A_1 \arrow[d, "f_1'"] \\
A_2 \arrow[r, "f_2'"] & B
\end{tikzcd}$$

In [Kan97, § 2], Kani reserves the name isogeny diamond to what we call here a minimal isogeny diamond. We changed the term here slightly, because an isogeny diamond always induces a reducible gluing $F : A \times B \to A_1 \times B_2$, even if it is not minimal.

Remark 3.6.
If we have an isogeny diamond starting from A as above, taking duals where needed we also have an isogeny diamond starting from A_1, A_2 and B. If the isogeny diamond starting from A is minimal, we will see in the proof of Corollary 3.9 that the one from B is too, ie $\operatorname{Ker} \widetilde{f_1'} \cap \operatorname{Ker} \widetilde{f_2'} = 0$. However, the one from A_1 (or A_2) may not be minimal.

As a counterexample, take a symplectic decomposition $A[\ell] = K_1 \oplus K_2, f_1 : A \to A_1$ the quotient by K_1 and $f_2 : A \to A_2$ the quotient by K_2; f_1' the quotient of A_1 by $f_1(K_2)$ and f_2' the quotient of A_2 by $f_2(K_1)$. Then $f_1' : A_1 \to A$ is exactly the dual isogeny $\widetilde{f_1}$, so $\operatorname{Ker} f_1' \cap \operatorname{Ker} \widetilde{f_1} = \operatorname{Ker} f_1' \neq 0$.

An isogeny diamond is completely determined by (f_1, f_2, f). So it determines $H_1 = \operatorname{Ker} f_1$, $H_2 = \operatorname{Ker} f_2$ and $H = \operatorname{Ker} f$. In particular, H is maximal isotropic in $A[n_1 n_2]$, $H_1 \subset H$ maximal isotropic in $A[n_1]$, and $H_2 \subset H$ maximal isotropic in $A[n_2]$. Note that if $H_1 \cap H_2 = 0$ (ie the diamond is minimal), then $H = H_1 \oplus H_2$ since both members have the same cardinality.

When we have a commutative square as above, this square is a pushout iff $\operatorname{Ker} f = \operatorname{Ker} f_1 + \operatorname{Ker} f_2$ where $f = f_2' \circ f_2 = f_1' \circ f_1$. So a minimal isogeny diamond is a pushout square.

Conversely, if f is the pushout of a n_1-isogeny f_1 by a n_2-isogeny f_2, and $\gcd(n_1, n_2) = 1$, then f is a (orthogonal) isogeny diamond. But in general, the pushout f_1' of f_1 need not be an n_1-isogeny, in which case the pushout is not a diamond.

Lemma 3.7 (Kani). *Let $f = f_1' \circ f_1 = f_2' \circ f_2$ be a (n_1, n_2)-isogeny diamond as above. Then $F = \begin{pmatrix} f_1 & \widetilde{f_1'} \\ -f_2 & \widetilde{f_2'} \end{pmatrix}$ is a n-isogeny $A \times B \to A_1 \times A_2$ where $n = n_1 + n_2$. Furthermore, if f is minimal,* $\operatorname{Ker} F = \{(\tilde{f}_1, f_1' x), x \in A_1[n]\}$, *and if f is an orthogonal isogeny diamond, then* $\operatorname{Ker} F = \{(n_1 x, f x), x \in A[n]\}$.

Proof. For the product polarisations, the dual isogeny $\tilde{F}$ is given by $\tilde{F} = \begin{pmatrix} \widetilde{f_1} & \widetilde{f_2} \\ -f_1' & f_2' \end{pmatrix}$ and we directly check that $\tilde{F}F = (n_1 + n_2)\operatorname{Id}$. Furthermore, $\operatorname{Ker} F$ is the image of $\tilde{F}$ on $A \times B[d]$, and if n_1 is prime to n_2 this is also the image of $\tilde{F}$ on $A[n] \times \{0\}$, so $\operatorname{Ker} f = \{(\tilde{f}_1 x, -f_1' x), x \in A[n]\} = \{(n_1 x, -f x), x \in A[n]\}$. □

Remark 3.8.

- One may of course permute f_1 and f_2, to get the same matrix F up to permutation of the coordinates. In terms of kernels, this amount to permuting H_1 and H_2 and replacing f by $-f$. It is not hard to prove that $\operatorname{Ker} F$ is completely determined by (H_1, H_2, f), and that there is a bijection between the $\operatorname{Ker} F$ for the isogeny diamonds, and the triplet (H_1, H_2, f) modulo the above equivalence: $(H_1, H_2, f) \equiv (H_2, H_1, -f)$. The exact same proof as in [Kan97, Theorem 2.3] (more precisely the first three paragraphs p. 9) hold.
- Since we have automorphisms $(-1, -1)$, $(-1, 1)$ and $(1, -1)$ on $A \times B$, we can also use the matrix $F' = \begin{pmatrix} f_1 & -\widetilde{f_1'} \\ f_2 & \widetilde{f_2'} \end{pmatrix}$, whose kernel, in the case of an orthogonal isogeny diamond, is $\operatorname{Ker} F' = \{(n_1 x, -f x), x \in A[n]\}$. In general, $\operatorname{Ker} F' \neq \operatorname{Ker} F$: there are two different reducible isogenies $A \times B \to A_1 \times A_2$.
- Note that F is not a product gluing, so in particular is a non trivial reducible gluing. Indeed if $\operatorname{Ker} F$ was a digonal product $G_1 \times G_2$, we would have $G_1 \subset \operatorname{Ker} f_1$, $G_2 \subset \operatorname{Ker} \widetilde{f_2'}$. So $\# G_1 \leq n_1^g$, $\# G_2 \leq n_2^g$, but $\operatorname{Ker} F = \# G_1 \# G_2 = n^{2g}$, which is a contradiction.

Corollary 3.9. *There is a bijection between triple (H_1, H_2, f) of isogeny diamonds modulo the equivalence defined above, and non diagonal maximal reducible kernels K of $A[n]$.*

This bijection induces an equivalence between minimal isogeny diamonds and minimal reducible gluing.

Proof. The first statement result from the combination of Lemmas 3.4 and 3.7 and Remark 3.8.

For the second statement, we need to prove that F is minimal iff $\operatorname{Ker} f_1 \cap \operatorname{Ker} f_2 = 0$. Note that $\operatorname{Ker} F \cap A \times 0 = \operatorname{Ker} f_1 \cap \operatorname{Ker} f_2$, so one application is clear. For the converse, since $\operatorname{Ker} F \cap 0 \times B = \operatorname{Ker} \widetilde{f_1'} \cap \operatorname{Ker} \widetilde{f_2'}$ we need to prove that if the diamond is minimal, $\operatorname{Ker} \widetilde{f_1'} \cap \operatorname{Ker} \widetilde{f_2'} = 0$, ie the diamond starting from B is also minimal. But this is a consequence of Lemma 3.1. □

References

[CD22] W. Castryck and T. Decru. *An efficient key recovery attack on SIDH (preliminary version).* Cryptology ePrint Archive, Paper 2022/975. 2022. URL: https://eprint.iacr.org/2022/975.

[FC90] G. Faltings and C.-L. Chai. *Degeneration of abelian varieties.* Ergebnisse der Mathematik und ihrer Grenzgebiete (3) 22. Springer-Verlag, Berlin, 1990.

[Kan97] E. Kani. "The number of curves of genus two with elliptic differentials." In: *Journal für die reine und angewandte Mathematik* 485 (1997), pp. 93–122.

[MM22] L. Maino and C. Martindale. *An attack on SIDH with arbitrary starting curve*. Cryptology ePrint Archive, Paper 2022/1026. 2022. URL: https://eprint.iacr.org/2022/1026.

[Mil91] J. Milne. *Abelian varieties*. 1991. URL: http://www.jmilne.org/math/CourseNotes/av.html.

[MFK94] D. Mumford, J. Fogarty, and F. Kirwan. *Geometric invariant theory*. Vol. 34. Springer Science & Business Media, 1994.

[PSV10] A. Prasad, I. Shapiro, and M. Vemuri. "Locally compact abelian groups with symplectic self-duality". In: *Advances in Mathematics* 225.5 (2010), pp. 2429–2454.

[Rob22a] D. Robert. "Breaking SIDH in polynomial time". Aug. 2022. URL: http://www.normalesup.org/~robert/pro/publications/articles/breaking_sidh.pdf. eprint: 2022/1038.

[Rob22b] D. Robert. "Evaluating isogenies in polylogarithmic time". Aug. 2022. URL: http://www.normalesup.org/~robert/pro/publications/articles/polylog_isogenies.pdf. eprint: 2022/1068.

INRIA Bordeaux–Sud-Ouest, 200 avenue de la Vieille Tour, 33405 Talence Cedex FRANCE
Email address: damien.robert@inria.fr
URL: http://www.normalesup.org/~robert/

Institut de Mathématiques de Bordeaux, 351 cours de la liberation, 33405 Talence cedex FRANCE