KANI FOR BEGINNERS

STEVEN D. GALBRAITH

We give a brief and self-contained description of Kani's reducibility theorem, as used by Castryck-Decru and Maino-Martindale.

There is nothing original in this note. It is just a translation of Kani's paper, with the goal of showing the very close relationship between Kani's work and the SIDH protocol.

Let E_0 be an elliptic curve with subgroups H_1 and H_2 of co-prime order. Let $\phi : E_0 \to E_1 = E_0/H_1$ and $\gamma : E_0 \to E_2 = E_0/H_2$. Let ϕ' have kernel $\gamma(H_1)$ and γ' have kernel $\phi(H_2)$. Consider the standard SIDH square, which Kani calls an "isogeny diamond configuration".

$$\begin{array}{ccc} E_0 & \xrightarrow{\phi} & E_1 = E_0/H_1 \\ \gamma \downarrow & & \gamma' \downarrow \\ E_2 = E_0/H_2 & \xrightarrow{\phi'} & E_3 \end{array}$$

We have the following basic facts.

Lemma 0.1. *Let notation be as above. Then*

(1) $\gamma' \circ \phi = \phi' \circ \gamma$
(2) $\phi \circ \hat{\gamma} = \hat{\gamma}' \circ \phi'$
(3) $\gamma \circ \hat{\phi} = \hat{\phi}' \circ \gamma'$
(4) $\hat{\phi} \circ \phi = [\#H_1]$
(5) $\hat{\gamma} \circ \gamma = [\#H_2]$.

Let $N = \#H_1 + \#H_2$. Let $\{P_0, Q_0\}$ be a basis for $E_0[N]$. Let $(P_1, Q_1) = (\phi(P_0), \phi(Q_0))$, $(P_2, Q_2) = (\gamma(P_0), \gamma(Q_0))$ and

$$(P_3, Q_3) = (\phi'(P_2), \phi'(Q_2)) = (\gamma'(P_1), \gamma'(Q_1)).$$

We now define a map

$$\rho : E_2 \times E_1 \to E_0 \times E_3$$

by

$$\rho(X, Y) = (\hat{\gamma}(X) + \hat{\phi}(Y), \phi'(X) - \gamma'(Y)).$$

One can verify that this makes sense since $\hat{\gamma} : E_2 \to E_0$, $\hat{\phi} : E_1 \to E_0$ and so on. Similarly, since all the maps are isogenies, it follows that ρ is a group homomorphism.

Kani proves that ρ is an isogeny with kernel $H = \langle (P_2, P_1), (Q_2, Q_1) \rangle$. Such a map of Abelian surfaces is called an (N, N)-isogeny. To prove this properly requires the theory of Abelian varieties and polarizations. But for beginners we just prove two simpler claims.

Lemma 0.2. *There is a map $\hat{\rho} : E_0 \times E_3 \to E_2 \times E_1$ such that $\hat{\rho} \circ \rho = [N]$. (Hence it makes sense to think of ρ as having degree N^2.)*

Proof. Write

$$\rho(X, Y) = \begin{pmatrix} \hat{\gamma} & \hat{\phi} \\ \phi' & -\gamma' \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix}.$$

Define

$$\hat{\rho}(X, Y) = \begin{pmatrix} \gamma & \hat{\phi}' \\ \phi & -\hat{\gamma}' \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix}.$$

One can check that

$$\hat{\rho} \circ \rho = \begin{pmatrix} \gamma \circ \hat{\gamma} + \hat{\phi}' \circ \phi' & \gamma \circ \hat{\phi} - \hat{\phi}' \circ \gamma' \\ \phi \circ \hat{\gamma} - \hat{\gamma}' \circ \phi' & \hat{\gamma}' \circ \gamma' + \phi \circ \hat{\phi} \end{pmatrix}.$$

Applying Lemma 1 one sees this is the matrix $(N, 0; 0, N)$, which corresponds to the map $[N] : E_2 \times E_1 \to E_2 \times E_1$ as required. □

Lemma 0.3. *ρ maps $H = \langle (P_2, P_1), (Q_2, Q_1) \rangle$ to $(0, 0)$.*

Proof.

$$\begin{aligned} \rho(P_2, P_1) &= (\hat{\gamma}(P_2) + \hat{\phi}(P_1), \phi'(P_2) - \gamma'(P_1)) \\ &= (\hat{\gamma} \circ \gamma(P_0) + \hat{\phi} \circ \phi(P_0), \phi' \circ \gamma(P_0) - \gamma' \circ \phi(P_0)) \\ &= = ([N]P_0, 0) \end{aligned}$$

using the properties of Lemma 1 (in particular that $\phi' \circ \gamma - \gamma' \circ \phi = 0$). Same argument applies to (Q_2, Q_1) and hence any linear combination of these group elements. □

Since H has order N^2 and ρ has degree N^2 it follows that $\ker(\rho) = H$.

Hopefully this note is sufficient to convince you that ρ is an (N, N)-isogeny from $E_2 \times E_1 \to E_0 \times E_3$. What is not obvious from this note, but crucial to the attack, is that if H is a "random" (Weil isotropic) subgroup then $E_2 \times E_1/H$ is not likely to be a product of elliptic curves, but is the Jacobian of a genus 2 curve.

Mathematics Department, University of Auckland, NZ.
Email address: `s.galbraith@auckland.ac.nz`