A NOTE ON IMPLEMENTING DIRECT ISOGENY DETERMINATION IN THE CASTRYCK-DECRU SIKE ATTACK

RÉMY OUDOMPHENG

Abstract. Matrix formulations of Kani's theorem given in [MM] are known to link directly elliptic curve isogenies in a commutative diagram (*isogeny diamond*) and the corresponding isogeny of abelian surfaces determined by Kani's theorem.

This allows to compute the result of the Castryck-Decru attack in an extremely fast way, by giving all ternary digits of the secret key in a single computation once the first digits, necessary to apply Kani's theorem, have been determined by exhaustive enumeration.

Higher dimensional analogues have been described by Damien Robert in [Rob].

This short note attempts to explain precisely what type of computations must be done in order to achieve that.

1. Kani's theorem and isogeny diamonds

We refer to [Gal] for a quick and short introduction to Kani's theorem and how it can be elegantly formulated using matrices of isogenies.

Considering a diagram of isogenies which is commutative even after replacing parallel arrows with the dual isogenies:

$$\begin{array}{ccc} E & \xrightarrow{\phi} & E' \\ \downarrow{\scriptstyle \tau} & & \downarrow{\scriptstyle \tau'} \\ C & \xrightarrow[\phi']{} & C' \end{array}$$

Kani's theorem [Kan97] says that if $\deg \phi + \deg \tau = N$ then the (N, N)-torsion subgroup $G \subset E[N] \times C'[N] \subset E \times C'$ defined by the graph of $\tau'\phi = \tau\phi'$ is isotropic for the Weil pairing and defines a quotient of abelian surfaces $E \times C'/G \simeq E' \times C$

Since the computation of this quotient surface only depends on the knowledge of the graph of the isogeny on the N-torsion subgroup, and not the isogeny itself, Castryck and Decru used data shared in SIKE key exchange to apply Kani's theorem and a criterion for the quotient surface to be a product of elliptic curve as an oracle to determine the secret key step-by-step.

2. Formulas for the $(2, 2)$-isogeny defined by a degree 2 elliptic subcover

The last step of the chain of $(2, 2)$-isogenies computing the quotient $C \times E/G$, which is not computed explicitly in [CD], is the splitting step where the codomain of the isogeny is again a product of elliptic curves.

It can be computed by essentially reversing the gluing formulas seen for example in [HLP00]. The splitting formulas can be found in [Smi].

Starting with a curve:

$$H : y^2 = G_1(x)G_2(x)G_3(x)$$

Date: 12 August 2022.

where G_i are linearly dependent degree 2 polynomials, we determine an homography σ of $\mathbb{P}^1$ such that the transformed hyperelliptic curve has form:

$$H' : y^2 = d(x^2 - \alpha_1)(x^2 - \alpha_2)(x^2 - \alpha_3)$$

This is done by solving the equation:

$$\begin{pmatrix} G_{1,0} & G_{1,1} & G_{1,2} \\ G_{2,0} & G_{2,1} & G_{2,2} \\ G_{3,0} & G_{3,1} & G_{3,2} \end{pmatrix} \begin{pmatrix} 2cd \\ ad+bc \\ 2ab \end{pmatrix} = 0$$

corresponding to the fact that

$$\tilde{G}_i = G_i\Big(\frac{ax+b}{cx+d}\Big)(cx+d)^2 = Ax^2 + B$$

The equation has solutions precisely when the matrix of coefficients (G_{ij}) is singular.

$$\begin{array}{ccc} H & \xrightarrow{\pi} & \mathbb{P}^1 \\ \uparrow{\scriptstyle\tilde{\sigma}} & & {\scriptstyle\sigma}\uparrow \\ H' & \xrightarrow[\pi']{} & \mathbb{P}^1 \end{array}$$

The map $H' \to H$ can be described explicitly as:

$$(x, y) \mapsto \Big(\frac{ax+b}{cx+d}, \frac{y}{(cx+d)^3}\Big)$$

We define curves with the following equations:

$$\begin{aligned} H' : y^2 &= (\tilde{G}_{1,2}x^2 + \tilde{G}_{1,0})(\tilde{G}_{2,2}x^2 + \tilde{G}_{2,0})(\tilde{G}_{3,2}x^2 + \tilde{G}_{3,0}) \\ E_1 : y^2 &= (\tilde{G}_{1,2}x + \tilde{G}_{1,0})(\tilde{G}_{2,2}x + \tilde{G}_{2,0})(\tilde{G}_{3,2}x + \tilde{G}_{3,0}) \\ E_2 : y^2 &= (\tilde{G}_{1,2} + \tilde{G}_{1,0}x)(\tilde{G}_{2,2} + \tilde{G}_{2,0}x)(\tilde{G}_{3,2} + \tilde{G}_{3,0}x) \end{aligned}$$

and the projection maps:

$$\begin{aligned} H' \to E_1 &: (x, y) \mapsto (x^2, y) \\ H' \to E_2 &: (x, y) \mapsto (1/x^2, y/x^3) \end{aligned}$$

which are easily shown to coincide with the ones defined in the gluing construction.

The computation of the abelian surface isogeny requires computing the image of a divisor $D \in \operatorname{Jac} H$ to E_1 and E_2.

This can be done explicitly without variable elimination, by mapping $D \in JacH \mapsto D' \in \operatorname{Jac} H'$ using the homography σ on Mumford coordinates, then mapping D' to E_i by defining auxiliary variables x_1, x_2 for the roots of the first Mumford coordinate of D', and computing the image in $\operatorname{Jac} E_i \simeq E_i$ using Mumford coordinates and replacing symmetric functions of x_1 and x_2 by the coefficients of D'.

Then Cantor's reduction formulas can be used to compute the coordinates of the corresponding point on E_i.

3. Description of the simplified implementation

In the context of Castryck-Decru attack, the first step is to construct a prefix of the secret isogeny: $\phi = \phi_{\text{pre}}\phi_{\text{suf}}$ such that we are able, using the endomorphism ring of

E_{start} to define an isogeny of suitable degree targeting a curve C, to construct an isogeny diamond:

$$\begin{array}{ccccc} E_{\text{start}} & \xrightarrow{\phi_{\text{pre}}} & E & \xrightarrow{\phi_{\text{suf}}} & E' \\ & & \downarrow \tau & & \downarrow \tau' \\ & & C & \xrightarrow[\phi']{} & C' \end{array}$$

The prefix has been determined using the "glue-and-split" construction as an oracle, and the suffix is unknown. Since the action of this diamond on a 2^a torsion subgroup is known, and since degrees have been chosen suitably, this diagram defines a computable exact sequence

$$0 \to G \to C \times E' \to E \times C' \to 0$$

where the map $C \times E' \to E \times C'$ is a chain of $(2,2)$-isogenies comprising a gluing map, Richelot isogenies, and a terminal splitting map as described in the previous section.

As explained in matrix descriptions of Kani's theorem, the quotient map $q : C \times E' \to E \times C'$ acts on C precisely by

$$q(P_C, 0) = (\pm\tau^*(P_C), \pm\phi'(P_C))$$

Let's complete the diagram as follows:

$$\begin{array}{ccccc} E_{\text{start}} & \xrightarrow{\phi_{\text{pre}}} & E & \xrightarrow{\phi_{\text{suf}}} & E' \\ \tau_{\text{start}} \downarrow & & \downarrow \tau & & \downarrow \tau' \\ C_{\text{start}} & \xrightarrow[\phi_{\text{pre,C}}]{} & C & \xrightarrow[\phi']{} & C' \end{array}$$

Since 3^b is coprime to 2^a, the isogenies τ act in an invertible way on 3-torsion: if P_3, Q_3 are generators of the 3^b torsion subgroup of E_{start}, then:

$$q(\tau\phi_{\text{pre}}(P_3), 0)_2 = \pm\phi'\tau\phi_{\text{pre}}(P_3) = \tau'(\phi(P_3))$$

meaning that $q \circ \tau \circ \phi_{\text{pre}}$ is an explicitly computable map whose kernel is exactly the kernel of the secret isogeny ϕ.

The computation of q requires mapping a point in either a product of elliptic curves, or a genus 2 Jacobian, through a chain of $(2,2)$-isogenies.

The kernel can be explicitly computed as follows: let (P_3, Q_3) be the basis of 3^b-torsion used to encode the secret key, and choose a symplectic basis of the 3^b-torsion of C'. Note that in the Jacobian splitting step, it may be unclear which factor is E and which factor is C'. Trying both ensures success.

Then compute the image of P_3, Q_3 in C' through the diagram above and the chain of $(2,2)$-isogenies. Then the Weil pairings of their images in C' with the chosen symplectic basis will define a 2×2-matrix in μ_{3^b} or equivalently, $\mathbb{Z}/3^b\mathbb{Z}$ whose kernel recovers the secret key s such that $P_3 + sQ_3$ maps to zero.

The resulting code implemented using SageMath will be published to the `https://github.com/remyoudompheng/Castryck-Decru-SageMath` Git repository.

References

[CD] Wouter Castryck and Thomas Decru, *An efficient key recovery attack on SIDH* (*preliminary version*), available at `https://eprint.iacr.org/2022/975`.

[Gal] Steven D. Galbraith, *Kani for beginners*, available at `https://www.math.auckland.ac.nz/~sgal018/kani.pdf`.

[HLP00] Everett W. Howe, Franck Leprévost, and Bjorn Poonen, *Large torsion subgroups of split Jacobians of curves of genus two or three*, Forum Mathematicum **12** (2000), 315–364.

[Kan97] Ernst Kani, *The number of curves of genus two with elliptic differentials*, Journal fur die reine und angewandte Mathematik **485** (1997), 93–121.

[MM] Luciano Maino and Chloe Martindale, *An attack on SIDH with arbitrary starting curve*, available at `https://eprint.iacr.org/2022/1026`.

[Rob] Damien Robert, *Breaking SIDH in polynomial time*, available at `https://eprint.iacr.org/2022/1038`.

[Smi] Benjamin Smith, *Explicit endomorphisms and correspondences* (*PhD dissertation*).