

# 1 The basic scheme

The diagram and parameters:

$$\begin{array}{ccccc}
 & d_{A,1} = 2^a - 3^b & & d_{A,2} = 3^b & \\
 & & & & \\
 E_0 & \xrightarrow{\varphi_{A,1}} & E_{A,1} & \xrightarrow{\varphi_{A,2}} & E_A \\
 \downarrow \varphi_1 & & & & \downarrow \varphi_2 \\
 E_1 & & & & E_2
 \end{array}
 \quad
 \begin{array}{l}
 d_1 = 2^{2a} + 2^a 3^b + 3^{2b} \\
 d_2 = 3^{2b}
 \end{array}$$

Check that the parameters satisfy

$$d_1 * d_{A,1} + d_2 * d_{A,2} = 2^{3a}$$

the prime is taken to be  $p = 2^{3a}3f - 1$  and the  $d_2$ -isogeny is computed using radical isogeny which cost

$$2b \log(p)$$

compared to

$$2b \log(2b)$$

for a  $2b$ -long 3-rational isogeny, which is much more costly but reduces the size of  $p$ . And we can't use the techniques for  $d_1$  and  $d_{A,1}$  for  $d_2$  (we could for  $d_{A,2}$ ).

## 1.1 Remarks

The  $d_1$ -isogeny has no reason to be smooth, as well as the  $d_{A,1}$ -isogeny. How do they compute it? They are computing them using the endomorphism ring of  $E_0$  from:

- Represent  $d_1(D - d_1)$  as a norm in  $\text{End}(E_0)$  (we need  $d_1(D - d_1) > p$ ). (Same for  $d_{A,1}$ )
- Do Kani on

$$\begin{array}{ccc}
 E_0 & \xrightarrow{\quad} & E \\
 \downarrow \varphi & \searrow \delta & \downarrow \\
 E & \xrightarrow{\omega} & E_0
 \end{array}$$

Since we can evaluate  $\delta$ .

- Evaluate  $\varphi$  from the 2-dimensional isogeny.

They argue that the output of this algorithm can compute  $\tilde{O}(2^{2a})$  curves which is sufficiently secure.

## 1.2 Other parameter choices

We could take  $p = 2^{2a}3^b f - 1$  with

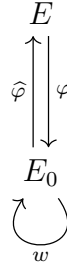
- $d_1 = 2^a + 3^b$
- $d_2 = 3^b$
- $d_{A,1} = 2^a - 3^b$
- $d_{A,2} = 3^b$

But now the size of the isogenies are not balanced and the side isogenies have only  $\lambda/2$ -security.

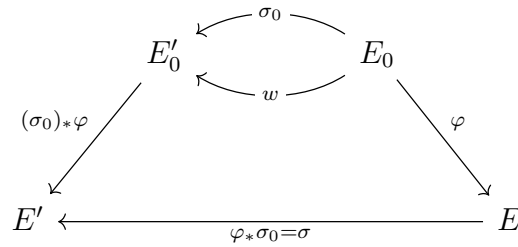
## 2 The generalized lollipop attack

**REMEMBER:** At anytime, Kani is able to interpolate an isogeny of degree  $d$  from torsion images of degree  $N$  **if**  $N > d$  (recall that  $N^2 > 4 * d$  suffices to uniquely determine our isogeny and that the 2-dimensional isogeny has degree  $d + f$ ).

This [paper](#) proposes an attack on FESTA and M-SIDH. They generalize the usual lollipop attack with diagram



to a generalized lollipop attack with diagram



The context is the following:

**Definition 2.0.1.** Define a generalized lollipop diagram associated to an isogeny  $\varphi : E_0 \rightarrow E$  as the added data of the diagram above.

To get a FESTA trapdoor instance we add

- A matrix  $A$  in  $X \subset GL_2(\mathbb{Z}/N\mathbb{Z})$ .

- A basis  $\langle P, Q \rangle$  of  $E_0[N]$ .

Now consider  $\psi = \varphi' \circ \omega \circ \widehat{\varphi}$ . Under some assumptions on the basis and the endomorphism  $\omega \circ \widehat{\sigma}_0$  we can in fact compute the image of  $\psi$  on the scaled torsion  $A * (\varphi(P)\varphi(Q))^t$ . Let's see why, define  $M$  by

$$\widehat{\sigma}_0 \circ \omega(P, Q) = \mathbf{M} \cdot (P, Q)^t$$

$$\begin{aligned} [s] \circ \psi \left( \begin{pmatrix} \varphi(P) \\ \varphi(Q) \end{pmatrix} \right) &= (\varphi' \circ \sigma_0) \circ (\widehat{\sigma}_0 \circ \omega) \circ \widehat{\varphi} \left( \begin{pmatrix} \varphi(P) \\ \varphi(Q) \end{pmatrix} \right) \\ &= \sigma \circ \varphi \circ \mathbf{M} \circ [d] \left( \begin{pmatrix} P \\ Q \end{pmatrix} \right) \end{aligned}$$

Now by abuse of notation, for any  $\varphi$ , we write  $\mathbf{M} \circ \varphi = \varphi \circ \mathbf{M}$ . The left  $\mathbf{M}$  acting on the image basis of the one on the right. Now

$$[s] \circ \psi \left( \mathbf{A} \cdot \begin{pmatrix} \varphi(P) \\ \varphi(Q) \end{pmatrix} \right) = [d] \mathbf{A} \cdot \mathbf{M} \cdot \mathbf{A}^{-1} \sigma \left( \mathbf{A} \cdot \begin{pmatrix} \varphi(P) \\ \varphi(Q) \end{pmatrix} \right)$$

Now if we can evaluate everything on the right we can evaluate  $\psi$  at torsion points. In particular we need

- $\mathbf{A} \cdot \mathbf{M} = \mathbf{M} \cdot \mathbf{A}$ .
- Being able to compute  $\sigma$ .

Now for the first condition in the FESTA case  $A$  is diagonal, so that  $M$  has to be diagonal. Meaning that  $P, Q$  are eigenvectors of  $\widehat{\sigma}_0 \circ \omega$ . For the second condition, this is even more restrictive, we would need to be able to compute a pushforward through  $\phi$ . There are two cases that we can handle:

- When  $\sigma_0 = \pi$  is the frobenius.
- When  $\sigma_0 = id$  is the identity.

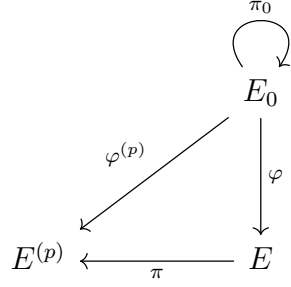
The next section deals with the frobenius case.

## 2.1 The frobenius case

We are in the case where

- $\sigma_0 = \pi_0$  is the frobenius.
- $\omega$  is an endomorphism to the conjugate.

And in particular if  $E_0$  is defined over  $\mathbb{F}_p$ . We can take  $\omega = id!$



## 2.2 In practice

If we are on the FESTA case the condition  $\mathbf{M.A}=\mathbf{A.M}$  is that  $(P, Q)$  are eigenvectors of the frobenius. If we are in the M-SIDH case, the matrix  $A$  is scalar so any  $M$  does it!

## 2.3 Remarks

The case where we have a single hidden image  $\lambda\varphi(P)$  of size  $N$  reduces to the FESTA case and not the M-SIDH case. Indeed we can see that from

$$\begin{array}{ccccc}
 \langle P, Q \rangle = E[2^{2n}] & \subset & E & \xrightarrow{\quad} & F & \supset & \langle \varphi(P), Q' \rangle = F[2^{2n}] \\
 & & \downarrow \psi & & \downarrow \psi' & & \\
 [\psi(P), [2^n]\psi(Q)] & & E / \langle [2^n]P \rangle & \xrightarrow{\quad \varphi' \quad} & F / \langle [2^n]\varphi(P) \rangle & & [\psi' \circ \varphi(P), [2^n]\psi(Q')] \\
 & & \downarrow & & \downarrow & & \\
 & & E / \langle P \rangle & \xrightarrow{\quad} & F / \langle \varphi(P) \rangle & & 
 \end{array}$$

There we have  $\phi'(\ker(\hat{\psi})) = \ker(\hat{\psi}')$  but  $\psi$  and  $\psi'$  project the  $2^n$ -torsion to a single line so we have to have  $\phi' \circ \psi(Q) = \lambda\psi'(Q)$  i.e. we can compute scaled torsion image by a diagonal matrice so we are in the FESTA case.

**Careful:** Here we suppose that we have  $\phi(P)$  and not  $\lambda\phi(P)$  but we could totally do that, so yes in the diagram above we can compute the weil pairing to get  $\lambda$  but not in general. **Careful2:** In the original FESTA, the size of the torsion we have is two times smaller so that having simply  $\lambda\phi_A(P)$  is not enough.

## 3 Counter-measures for QFESTA