Isogeny interpolation

Castryck, Decru, Maino, Martindale, Panny, Pope, Robert, Wesolowski

Caipi symposium, Rennes, April 30, 2024

These notes were written up by J. Kieffer, who apologizes for any typos or mistakes. Slides from Wouter's introductory talk will be available on the symposium website.

Introduction. The topic of this talk can be seen as a follow-up of the SIDH attacks, on the constructive side. It is a work in progress. The starting point is:

Lemma 1. *Let E, E' be elliptic curves over a field, and let $\varphi : E \to E'$ be an isogeny of degree $d \geq 1$. Then φ is uniquely determined by the images of $4d+1$ distinct points on E.*

Question: can this be made effective? This leads to formalizing the isogeny interpolation problem. Throughout, the base field is a finite field $\mathbb{F}_q$ of characteristic p.

Isogeny interpolation problem (IIP). *Given two elliptic curves E, E' over $\mathbb{F}_q$, a degree $d \geq 1$, and interpolation data, i.e. the data of*

- *base points $P_1, \ldots, P_k$ on E for some $k \geq 1$ (not necessarily defined over $\mathbb{F}_q$) such that the group $G = \langle P_1 \ldots, P_k \rangle \subset E(\overline{\mathbb{F}}_q)$ satisfies $\#G > 4d$,*
- *image points $P'_1, \ldots, P'_k$ on E',*
- *a challenge point X on E,*

compute $\varphi(X)$ where φ is the unique isogeny such that $\varphi(P_i) = P'_i$ for each $1 \leq i \leq k$, or $\perp$ if such an isogeny does not exist.

Main theorem. *There is a deterministic algorithm to solve the IIP which works as soon as $p \nmid \#G$ and which runs in polynomial time in the following quantities:*

- *k and $\log q$,*
- *the largest degree of the defining fields of P_i and the challenge point X,*
- *the largest degree of the fields of definition of each individual point in $E[\ell^{\lfloor e/2 \rfloor}]$ whenever ℓ^e is a prime power dividing $\#G$,*
- *the largest prime factor of $\#G$.*

Wouter asks: can we remove the hypothesis $p \nmid \#G$? [There was a discussion after the talk involving Dieudonné modules.] Can one omit the degree of the fields of definition of torsion points in the above list?

Example of an open case: $p = 2$, $q = 2^r$, E is ordinary, and P is a generator of the cyclic group $E[2^n]$ for some $n \geq 1$.

Remark 2.

- Since E, E' are defined over $\mathbb{F}_q$ by assumption, φ will always be defined over a small extension. After taking it, we can assume that φ is defined over $\mathbb{F}_q$. We can also assume that G is defined over $\mathbb{F}_q$ after taking its closure under Frobenius.
- If E is supersingular, then the "extra" conditions can be removed: $p \nmid \#G$ always holds and we can arrange that each point in $E[\ell^e]$ is defined over a small field (compared to the fields of definition of the points P_i.)
- The group G always have at most two generators, in fact there exist $a, b \geq 1$ such that $G \simeq \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/ab\mathbb{Z}$ and $p \nmid a$. However these generators might live in a larger field extension than the base points given in the IIP.
- Instead of $E[\ell^{\lfloor e/2 \rfloor}]$ in the main theorem, we could write $E[\ell^{\lceil e/2 \rceil}]$, because this relative field extension has degree polynomial in ℓ.
- We can assume that the order of the challenge point X is coprime to $\#G$. [Wouter presented the following argument to me after the talk.] Indeed we can always write $X = X_1 + X_2$ where the order of X_1 is coprime to $\#G$, and every prime factor of $\mathrm{ord}(X_2)$ divides $\#G$. We can compute $\varphi(X_1)$, so it suffices to concentrate on the computation of $\varphi(X_2)$. For this, we pick small primes $\ell_1, \ldots, \ell_r$ different from p that do not divide $\#G$, such that $\ell_1^2 \cdots \ell_r^2 = \#E[\ell_1 \cdots \ell_r] > 4d$. For each i, we pick basis points $R_{i,1}, R_{i,2}$ of $E[\ell_i]$ and we use the algorithm to compute $\varphi(R_{i,1}), \varphi(R_{i,2})$. This gives new interpolation data, now with a group whose order is coprime to $\mathrm{ord}(X2)$, and this can be used to compute $\varphi(X_2)$ as wanted. All the primes ℓ_i have size $O(\log \#G)$, which is polynomial in the quantities of the theorem.
- The SIDH attack (Robert's theorem) can be summarized as: the main theorem is true for $G = E[N]$ when N and d are coprime.

From now on we keep the assumptions: φ and G are defined over $\mathbb{F}_q$, and the order of X is coprime to $\#G$. There are two main steps:

1. Generalize the SIDH attacks to the case $G = E[N]$ but N and d are not coprime;
2. Reduce general subgroups G to the case $G = E[N]$. The reduction will involve an N that is very much not coprime to d, so step 1 is important.

First step: $G = E[N]$ where $\gcd(N, d) > 1$. A naive attempt is to decompose φ as

$$E \xrightarrow{\varphi_c} E_c \xrightarrow{\varphi'} E'$$

where φ_c has degree c and the degree of φ' is d/c, hence is coprime to N/c. From the interpolation data, we can recover E_c and pushforward the IIP to $G' = E_c[N/c]$. However, we don't always have $\#G' > 4(d/c)$ because $\#G' = N^2/c^2$, not N^2/c. Still, this approach works to factor out any "multiplication-by-c" component from φ, so we can and do assume that $\ker\varphi \cap E[N]$ is cyclic.

Instead we adapt the SIDH attacks to this new setting. To simplify the situation, we assume that we can use dimension 2 isogenies only and ignore the meet-in-the-middle improvement (cf. Wouter's slides), i.e. we assume:

$$N > d \text{ and } N - d = a^2 \text{ is a perfect square.}$$

(Things can be appropriately generalized to isogenies in dimensions 4 and 8.) We consider the endomorphism

$$\Phi = \begin{pmatrix} a & \widehat{\varphi} \\ -\varphi & a \end{pmatrix} \in \mathrm{End}(E \times E').$$

Compared to the usual SIDH attack, we still have $\widehat{\Phi}\circ\Phi = [N]$, but it's not obvious that the kernel of Φ is isomorphic to $(\mathbb{Z}/N\mathbb{Z})^2$ (though this is true a posteriori when $\ker\varphi \cap E[N]$ is cyclic). We don't have a formula for $\ker\Phi$: the set $\{(aP, \varphi(P)) : P \in E[N])\}$ is contained in the kernel but is too small to be all of it. If we can compute $\ker\Phi$, we can evaluate Φ, in particular $\Phi(X)$, so we're done.

To compute $\ker\Phi$, write

$$\ker\Phi = \{(P,Q) \in E \times E' : aP + \widehat{\varphi}(Q) = 0 \text{ and } -\varphi(P) + aQ = 0\}.$$

We want to solve the system. From the IIP data, we know how φ acts on $E[N]$, but we need to compute how $\widehat{\varphi}$ acts on $E'[N]$.

Lemma 3. *We can compute the action of $\widehat{\varphi}$ on $E'[N]$. Thus, we can solve the above linear system and compute* $\ker\Phi$.

Writing $\varphi\circ\widehat{\varphi} = [N]$ or $\widehat{\varphi}\circ\varphi = [N]$ doesn't help because N and d are not coprime.

Proof. Choose bases (P_1, P_2) and (Q_1, Q_2) of $E[N]$, resp. $E'[N]$. We show how to compute e.g. $\widehat{\varphi}(Q_1)$. Write $\widehat{\varphi}(Q_1) = \lambda P_1 + \mu P_2$ for some unknown $\lambda, \mu \in \mathbb{Z}/N\mathbb{Z}$. Let's compute λ. Let e be the Weil pairing on $E[N]$. Then as e is alternating, we have

$$e(\widehat{\varphi}(Q_1), P_2) = e(P_1, P_2)^\lambda$$

By properties of the dual isogeny, we also get

$$e(\widehat{\varphi}(Q_1), P_2) = e(Q_1, \varphi(P_2)) \quad \text{(this time on } E'[N]),$$

which we can compute. Finally discrete logarithms in $\mathbb{Z}/N\mathbb{Z}$ can be computed in polynomial time in the quantities of the main theorem. □

Second step: reduction from general G to $G = E[N]$. For simplicity, assume G is cyclic and $k = 1$, with $\mathrm{ord}(P_1) = N > 4d$. We can assume that P_1' is a point of exact order N, because otherwise we can easily "kill" the part of $\ker\varphi$ that intersects $G = \langle P_1\rangle$. We proceed as follows.

1. We extend P_1 to a basis (P_1, P_2) of $E[N]$. The point P_2 might live over a large field extension, which explains why the fields of definition of torsion points matter in the main theorem. In the end, it is sufficient to consider $E[\ell^{\lfloor e/2\rfloor}]$ because of meet-in-the-middle and CRT techniques, but this was too techical to be part of the talk.
2. We extend P_1' to a basis (P_1', P_2') of $E[N]$. Now $\varphi(P_1) = P_1'$ and $\varphi(P_2) = \lambda P_2' + \mu P_1'$ for some unknown λ, μ.
3. We compute λ using the Weil pairing as above, using
$$e(\varphi(P_1), \varphi(P_2)) = e(P_1, P_2)^d = e(P_1', P_2')^\lambda.$$
However μ is still unknown.
4. To "kill" μ, we consider the further isogeny $\psi : E' \to E''$ whose kernel is $\langle P_1'\rangle$. We have $\deg(\psi) = N$. Note:
   - $\psi\varphi(P_1) = 0$ and $\psi\varphi(P_2) = \lambda\psi(P_1')$, so $\psi\varphi$ is known on $E[N]$.
   - $N^2 > 4\deg(\psi\varphi) = 4Nd$ because $N > 4d$.
   - N is very much not coprime to $Nd = \deg(\psi\varphi)$.

   We apply the IIP on $E[N]$ for the isogeny $\psi\varphi$ as in the first step. This yields $\psi\varphi(X)$.
5. We recover $\varphi(X)$ as $[M]\widehat{\psi}(\psi\varphi(X))$, where M is an inverse of N modulo $\mathrm{ord}(X)$ (recall that at the very beginning, we assumed that N and $\mathrm{ord}(X)$ are coprime.)

Remark 4.
- This doesn't quite give the main theorem yet: we need to work prime power by prime power to avoid taking a huge field compositum.
- The final algorithm uses $(\ell, \ldots, \ell)$-isogenies in higher dimensions for all prime divisors ℓ of $\#G$, which is why the complexity in the main theorem is polynomial in such ℓ's. Avoiding this polynomial dependency seems difficult.

Q&A session. Q: What's the issue if $p \mid \#G$?

A: $E[p]$ is not isomorphic to $(\mathbb{Z}/p\mathbb{Z})^2$ so the algorithm doesn't work as is. Andreas Pieper has an isogeny algorithm that relies on Dieudonné modules in this case that may prove useful.

Q: What about interpolating isogenies between abelian surfaces?

A: Robert's theorem (the case $G = E[N]$ with N and d coprime) works for abelian varieties in any dimension. This work is mainly about elliptic curves, but the main ideas should work in general.

Q: Is the decisional version of the problem (i.e. is the output $\perp$?) easier?

A: At present, we only know if the output is $\perp$ at the end of the algorithm (e.g. after evaluating Φ, we find that its image is a random Jacobian instead of $E \times E'$; this verification can be made deterministic). We don't know if we can do better. A positive answer would speed up the verification step in SQIsign(HD).