Quantum torsion-point attacks

Péter Kutas

No Institute Given

1 Introduction

In this lecture note we will examine the algorithmic problem of defining a group action on the SIDH key space and applying Kuperberg's hidden shift algorithm to retrieve the secret isogeny in overstretched SIDH variants [4]. We suppose the reader is familiar with the SIDH key exchange and basic results concerning supersingular elliptic curves.

In [1] the authors show how one can reduce finding the secret isogeny in CSIDH to a hidden shift problem involving the class group acting on the sets of supersingular elliptic curves over $\mathbb{F}_p$. This action has some very special properties. It is free and transitive which implies a direct one-to-one correspondence between supersingular elliptic curves over $\mathbb{F}_p$ and elements of the class group of $\mathbb{Z}[\sqrt{p}]$. If one considers the whole supersingular isogeny graph, then there are many different class group actions which do not commute as in the $\mathbb{F}_p$ case. Thus, it is not obvious how one could generalize the attack from [1] to the SIDH setting. The main idea of the result in this note is to use a completely different group action and exploit the torsion point information provided in SIDH.

First we introduce a generic framework called a "malleability oracle" which provides a wide variety of situations where hidden shift attacks could be applicable (even potentially outside of isogeny-based cryptography). Then we provide an instantiation of the malleability oracle in the SIDH setting.

2 Malleability oracles

First let us briefly recall some important algorithmic problems which are interesting from a quantum standpoint.

Problem 2.1 (Hidden shift problem). Let G be a group and let X be a set. Let $f_1, f_2 : G \to X$ be functions which can be evaluated on any $g \in G$ efficiently. Suppose that there exists an $x \in G$ such that $f_1(gx) = f_2(g)$. Find x.

Kuperberg showed that the hidden shift problem can be solved in subexponential time if G is abelian and f_1, f_2 are injective [3]. The main idea of Kuperberg's algorithm is a reduction to a different problem which is called the the hidden subgroup problem:

Problem 2.2. Let G be a group and let X be a set. Let $f : G \to X$ be a function which is constant along the cosets of some subgroup H. Find H

Remark 2.3. In the special case where f is a group homomorphism, the hidden subgroup problem is equivalent to finding the kernel of the homomorphism.

The hidden subgroup problem is a central problem in algebraic quantum algorithms. When G is abelian, then there exists a polynomial-time algorithm which finds the hidden subgroup. This is of particular interest for cryptographers as this is the celebrated algorithm of Peter Shor which can be applied to factoring and discrete logarithms [5]. When G is non-abelian, then the picture is much less clear. Nevertheless, when G is the dihedral group, then the hidden subgroup problem can be solved in subexponential time. It is not hard to show that the hidden shift problem for an abelian group can be reduced to a dihedral hidden subgroup problem.

Exercise 2.4. Suppose you have access to an oracle for solving the hidden subgroup problem for the dihedral group D_n (which has $2n$ elements). Let f_1, f_2 be injective functions from $\mathbb{Z}/n\mathbb{Z}$ to some set X with the property that $f_1(g+x) = f_2(x)$ for some $x \in G$ and every $g \in G$. Find x with the help of he oracle.

(Hint: use the fact that D_n is a semidirect product of a cyclic group of order n and a cyclic group of order 2.)

Now we turn our attention to the concept of malleability oracles. We recall some basic definitions concerning group actions first:

Definition 2.5. *Let G be a group acting on a set X. The group action is* transitive *if for every pair $x, y \in X$ there exists a $g \in G$ such that $gx = y$. The group action is* free *if $gx = x$ implies $g = 1$.*

Remark 2.6. One can also rephrase these notions in terms of stabilizers and orbits. The transitivitiy condition means that there is exactly one orbit. A group action is free if and only every elements stabilizer is trivial. If both conditions are satisfied, then there is a bijection between the group elements and the elements of X.

Definition 2.7. *Let $f : X \to Y$ be an injective one-way function. Let G be a group which acts on the set X. Then the input of a malleability oracle is a value $f(x)$ and an element $g \in G$. The output is $f(gx)$.*

Now the question is the following. Suppose we have access to a malleability oracle. How hard is it to invert f? The next lemmas shows that if G is abelian and the action of G is free and transitive, then one can invert f in subexponential time:

Lemma 2.8. *Let $f : X \to Y$ be an injective (one-way) function and let G be a group acting transitively on I. Given a malleability oracle for G at $o := f(i)$, a preimage of o can be computed by solving a hidden shift problem.*

Proof. Take an element $j \in X$ and define the functions $f_j(g) : g \mapsto f(gj)$ and $f_i(g) : g \mapsto f(gi)$. Note that we can evaluate both functions efficiently (the first one is clear, the second one is an implication of the malleability oracle). We show that these two functions are shifts of each other. Since G acts transitively on X, there exists an s such that $sj = i$. Then one has that

$$f_i(g) = f(gi) = f(gsj) = f_j(gs).$$

From this it is clear that finding the hidden shift s is sufficient to find i.

Lemma 2.9. *Suppose that the action of G is free and transitive and that G is finite abelian. Then there exists a subexponential algoithm that inverts f.*

Proof. We leave this as an exercise (Hint: you need to show that the functions f_i and f_j are injective).

Exercise 2.10. Let G, H be finite cyclic groups. Let $f : G \to H$ be such that $f(x + y) = f(x) + f(y)$ (i.e., f is a homomorphism). Show that one can invert f in quantum polynomial time. (Hint: reduce the problem to a discrete log instance)

It is not suprising that the attack from [1] against CSIDH fits into the malleability oracle framework. In the next section are goal is to show how one can construct a malleability oracle for overstretched SIDH (i.e., where the isogeny degrees involved are significantly larger than p).

3 Applications to overtretched SIDH

3.1 The group action

Suppose that $\phi : E \to E_A$ is a secret isogeny of degree A and one is provided with the images of P_B, Q_B generating $E[B]$ under the isogeny ϕ. Our goal is to use mallebaility oracles for retrieving the secret isogeny from this information. In order to define a malleability oracle we need to define an injective function first. The natural candidate is to choose the function which takes a cyclic subgroup H of order A of E to the elliptic curve E/H. The one-wayness of this function is at the core of isogeny-based cryptography. However, this function is not necessarily injective. Suppose that E has a cyclic endomorphism of degree A^2. Then if one takes the first A part of this endomorphism then this curve is the image of two different cyclic subgroups under the above mentioned function. In order to handle this issue we take the special starting curve $E : y^2 = x^3 + x$. Now a different issue arises. Namely, that E contains a non-scalar automorphism ι which implies that $E/H \cong E/\iota(H)$. The question arises: can we give a useful characterization when $E/H_1 \cong E/H_2$? In order to achieve this we impose two conditions on A. We assume that A is a power of 2 and that $A^2 < \frac{p+1}{4}$. Then one can show the following:

Exercise 3.1. Suppose that $A^2 < \frac{p+1}{4}$. Let ϕ and ϕ' be two isogenies of degree A from E to a curve E_A. Then either $\ker\phi = \ker\phi'$ or $\ker\phi = \iota(\ker\phi')$. (Hint: show that the only endomorphisms of degree A^2 of E are A and $A\iota$)

On one hand, this shows that the natural choice for a one-way function is not injective. However, this also shows that it is quite close to being injective. Namely let $P \in E$ be such that $P, \iota(P) = Q$ generate $E[A]$ and take the following two subsets of cyclic subgroups of order A:

$$I_1 = \{\langle P + \alpha Q \rangle |\ \alpha \equiv 0 \pmod 2\},\ I_2 = \{\langle P + \alpha Q \rangle |\ \alpha \equiv 1 \pmod 2\}$$

Exercise 3.2. Show that if we restrict the one-way function sending a cyclic subgroup to the corresponding elliptic curve to I_1 or I_2, then it becomes injective.

Exercise 3.3. Let E_A be a curve of distance A from E (i.e., there exists a degree A cyclic isogeny from E to E_A). Then there exists an isogeny ψ from E to E_A such that the kernel of ψ is generated by $P + \alpha Q$ for some $\alpha \in \mathbb{Z}$.

Now we have created two injective one-way functions with domains I_1 and I_2. Note that our eventual goal is to invert these one-way functions but we do not apriori know whether our secret kernel belongs to I_1 or I_2 (the previous exercise shows that it does belong to at least one of them). However, this can be dealt with by running the inversion algorithm twice (potentially in parallel): once for I_1 and once for I_2. One of the algorithms will fail and the other one will succeed (failure can be detected in subexponential time).

Our next goal is to provide a group action on I_1 and I_2. We need a group action with very specific properties: the group has to be finite abelian and the action has to be free and transitive.

As a start one can look at the endomorphism ring of E which we denote by $O = \mathrm{End}(E)$. This is an abelian group with respect to addition but that's not very useful in this context. Instead one can look at $(O/AO)^*$ which is essentially looking at endomorphisms modulo A and only taking the ones whose degree is coprime to A. Note that in our case A is a power of 2, therefore we look at endomorphisms whose degree is odd. This is a group isomorphic to $GL_2(\mathbb{Z}/A\mathbb{Z})$. The action of this group on a cyclic subgroup is quite natural: let θ be an endomorphism in O and X be a point of order A. Then $\theta * X := \theta(X)$. Since the degree of θ was coprime to A, the order $\theta(X)$ will be A.

There are various concerns with this group action as neither the group is abelian nor is the induced action free. The key idea is to restrict this group action substantially.

The first observation is that instead of working with $GL_2(\mathbb{Z}/A\mathbb{Z})$, one should be working with $PGL_2(\mathbb{Z}/A\mathbb{Z})$, meaning that we identify two endomorphisms if they differ by scalar multiplication modulo A. Then we restrict to endomorphisms of the form $a + b\iota$ which already form an abelian subgroup. Finally, we need that I_1 and I_2 are invariant under this action, so the group we use is $G = \{a + b\iota |\ b \equiv 0 \pmod 2\}$ viewed as a subgroup of $PGL_2(\mathbb{Z}/A\mathbb{Z})$.

Exercise 3.4. Show that the action of G is free and transitive on I_1.

Unfortunately, the action of G on I_2 is not transitive.

Exercise 3.5. Show that the action of G has two orbits on I_2.

This is actually a small technical issue which can be dealt with by slightly modifying the acting group G. Essentially one needs a group which has half the number of elements and acts freely and transitively on both orbits. Note that one cannot use G as the induced action won't be free since G has more elements than the cardinality of the orbits.

For the rest of the note we restrict ourselves to the set I_1 for simplicity. Now we have an injective one-way function from I_1 to the set of elliptic curves of distance A from E. We also have a group action on I_1 which is abelian, free and transitive. In order to be able to use our malleability oracle framework we need to solve the following issue.

Given E/X (but not the kernel X), how do we compute $E/\theta(X)$?

3.2 The main idea and the lifting problem

The key idea for computing $E/\theta(X)$ comes from the diagram presented in Figure 1: Let the kernel of the secret isogeny φ be generated by X. Now the idea is to use the isomorphism $E/\theta(X) \cong E_A/\varphi(\ker\theta)$. Note that we know how φ acts on $E[B]$ so if the degree of θ divided B, then one could compute $E_A/\varphi(\ker\theta)$ using the torsion information. Observe that since we are working with endomorphisms modulo A an element in the acting group G has several lifts in O. Now the key problem remains to lift an endomorphisms of the form $\theta = a + b\iota$ to an endomorphism θ' in O with the following properties:

$$\begin{tikzcd}
E \arrow[r, "\varphi"] \arrow[d, "\theta"'] & E_A \arrow[d] \\
E \arrow[r] & E/\theta(\ker\varphi) \cong E_A/\varphi(\ker\theta)
\end{tikzcd}$$

Fig. 1. SIDH key exchange instance with isogenies φ and the endomorphism θ.

- $\theta - \theta'$ is identically to the zero map on $E[A]$, i.e. θ and θ' are the same modulo A
- $\deg(\theta')$ divides B

A similar lifting problem is considered in the KLPT algorithm [2] but in that case an element of the form $a\iota + bj$ is lifted, where j is the Frobenius endomorphism.

Exercise 3.6. Suppose that $B > pA^4$. Then every element of the form $a\iota + bj$ can be lifted to an element of norm dividing B. Show that every $\theta = a + b\iota$ can be written as the product of two elements of the form $a\iota + bj$ and derive a lifting condition from this.

There is a better way of lifting elements of the form $\theta = a + b\iota$ which is described in Algorithm 1 (this is taken directly from [4], for more details on the correctness we refer to said paper).

Algorithm 1: Lift element from $\mathbb{Z}[i]$ to quaternion of norm B or eB

```
Input: $\theta = a_0 + b_0 i \in \mathrm{End}(E)$, $q := \mathrm{Disc}(\mathbb{Z}[i])$ and parameters $p$, $\varepsilon$, $A$,
       $B > p^2A^4$
Output: $\theta' = \lambda a_0 + Aa_1 + (\lambda b_0 + Ab_1)i + Ac_1 j + Ad_1 k$ and $\mathrm{Norm}(\theta') = B$ or
        $eB$ with probability $1 - \varepsilon$ and $\perp$ otherwise
Let $h(x, y) := \mathrm{Norm}(x + yi)$;
if $\lambda$ in $B = \lambda^2 h(a_0, b_0) \pmod{A}$ has solution for $\lambda$ then
    Compute $\lambda$;
else
    $e \leftarrow$ smallest quadratic non-residue $\pmod{A}$;
    Compute $\lambda$ in $eB = \lambda^2 h(a_0, b_0) \pmod{A}$;
Compute linear relation between $a_1$ and $b_1$ mod $A$, say $e_b b_1 = e_a a_1 + e_c$
  $\pmod{A}$ for some integers $e_a, e_b, e_c$, using
      $$2\lambda(a_0 a_1 + b_0 b_1) = \frac{eB - h(\lambda a_0, \lambda b_0)}{A} \pmod{A};$$
$C \leftarrow 2\log(\varepsilon)\log(|q|p^2A^4)/\log(1 - \log^{-1}(|q|p^2A^4))$;
for $m = 0, 1, \dots, C$ do
    Substitute $b_1$ using expression $e_b b_1 = e_a a_1 + e_c + mA$ in
        $$eB = h(\ \lambda a_0 + Aa_1\ ,\ \lambda b_0 + Ab_1\ ) \pmod{p};$$
    if solution for $a_1$ $\pmod{p}$ exists then
        Compute $a_1$ and $b_1$ modulo $p$ and lift them to integers in $[-p/2, p/2]$;
        $r \leftarrow \frac{eB - h(\lambda a_0 + Aa_1, \lambda b_0 + Ab_1)}{pA^2}$;
        if $r$ is prime then
            Use Cornacchia's algorithm to find solutions for $c_1, d_1$ in
              $h(c_1, d_1) = r$ or determine that no solution exists;

        if solution is found then
            return $\theta' = \lambda a_0 + Aa_1 + (\lambda b_0 + Ab_1)i + Ac_1 j + Ad_1 k$;
return $\perp$
```

Exercise 3.7. Instead of lifting $\theta = a + b\iota$, improve on the lifting conditions by lifting $j\theta$ first and then applying the Frobenius isogeny. Show that this way one can achieve lifting whenever $B > pA^4$.

Finally, we can conclude with the following theorem:

Theorem 3.8. *Let $B > pA^4$, then one can retrieve SIDH secret keys in quantum subexponential time*

As a summary, here are the key ingredients of the proof:

- Special subgroup of the starting endomorphism ring modulo A acting freely and transitively on certain sets of cyclic subgroups
- A lifting algorithm for special endomorphism
- The commutative diagram described in Figure 1
- Kuperberg's hidden shift algorithm

4 Open problems

In this section we discuss an open problem which arises naturally in this context. Note that the discussion in this section will be even less formal and precise than in previous sections.

We have shown in previous sections that having a free and transitive group action on cyclic subgroups of order A leads to a subexponential attack on overstretched SIDH. Note that torsion point images are only used in the lifting procedure. So one can ask the following question. Suppose you have access to an oracle which given an endomorphism θ and a curve E/X of distance A, returns $E/\theta(X)$. How hard is it to retrieve X. We have shown that in this case X can be retrieved in quantum subexponential time. The natural question arises: is there a polynomial-time algorithm for this task?

We outline a possible approach to tackle this problem. The key idea is trying to reduce the problem to a hidden subgroup problem as opposed to a hidden shift problem. Let $G_0 = PGL_2(\mathbb{Z}/A\mathbb{Z})$ and let use the natural action of this group as before. Now the action will be transitive but far from free. However, one can look at the stabilizer of an element. The stabilizer will contain multiple elements now since the order of the stabilizer is $|G_0|$ divided by the size of its orbit. The function $X \mapsto E/\theta(X)$ is constant along the cosets of the stabilizer of X, thus computing the stabilizer of X is an instance of the hidden subgroup problem. Why is a stabilizer useful?

One can look at elements of G_0 as matrices in $M_2(\mathbb{Z}/A\mathbb{Z})$ and kernels as vectors in $(\mathbb{Z}/A\mathbb{Z})^2$ where the group action is multiplying the matrix with the corresponding vector. Now the stabilizer of a vector (x, y) is essentially a collection of matrices for which (x, y) is an eigenvector. This implies that if one has access to several matrices from the stabilizer, then one can compute the secret X by computing a common eigenvector of these matrices. The main issue here is that there is no efficient algorithm in general which solves the hidden subgroup problem for $PGL_2(\mathbb{Z}/A\mathbb{Z})$. Of course one can restrict the action again to some subgroup which poses the following open problem:

Problem 4.1. Find a subgroup of $PGL_2(\mathbb{Z}/A\mathbb{Z})$ such that the corresponding action allows to retrieve the secret kernel from the stabilizer and such that the group admits an efficient hidden subgroup algorithm.

Here is a quick exercise on how this algorithm could work for a special subgroup:

Exercise 4.2. Let G_0 be the group consisting of the matrices of the form

$$\begin{pmatrix} 1 & 0 \\ * & y \end{pmatrix},$$

where y is either 1 or -1. Show that G_0 is isomorphic to a dihedral group. Compute the stabilizer of $(1, a)^T$ and show how one can retrieve a from the stabilizer.

Bibliography

[1] Andrew Childs, David Jao, and Vladimir Soukharev. Constructing elliptic curve isogenies in quantum subexponential time. *Journal of Mathematical Cryptology*, 8(1):1–29, 2014.

[2] David Kohel, Kristin Lauter, Christophe Petit, and Jean-Pierre Tignol. On the quaternion ℓ-isogeny path problem. *LMS Journal of Computation and Mathematics*, 17(A):418–432, 2014.

[3] Greg Kuperberg. A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. *SIAM Journal on Computing*, 35(1):170–188, 2005.

[4] Péter Kutas, Simon-Philipp Merz, Christophe Petit, and Charlotte Weitkaemper. One-way functions and malleability oracles: Hidden shift attacks on isogeny-based protocols. In *Advances in Cryptology–EUROCRYPT 2021*. 2021.

[5] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999.