Hidden Stabilizers, the Isogeny To Endomorphism Ring Problem and the Cryptanalysis of pSIDH

Mingjie Chen, Muhammad Imran, Gábor Ivanyos, Péter Kutas, Antonin Leroux, Christophe Petit

28th November 2023

Supersingular Isogeny Diffie-Hellman (SIDH)

- Choose a prime p, and $N_A, N_B \in \mathbb{N}$ with $\gcd(N_A, N_B) = 1$
  Choose E_0 a supersingular curve over $\mathbb{F}_{p^2}$
- Alice picks a cyclic subgroup $G_A \subset E_0[N_A]$ defining an isogeny $\phi_A : E_0 \to E_A = E_0/G_A$ and she sends E_A to Bob
- Bob picks a cyclic subgroup $G_B \subset E_0[N_B]$ defining an isogeny $\phi_B : E_0 \to E_B = E_0/G_B$ and he sends E_B to Alice

$$\begin{tikzcd} & E_A = E_0/G_A \arrow[dr, "\phi'_B"] & \\ E_0 \arrow[ur, "\phi_A"] \arrow[dr, "\phi_B"'] & & E_0/\langle G_A, G_B\rangle \\ & E_B = E_0/G_B \arrow[ur, "\phi'_A"] & \end{tikzcd}$$

- Shared key is $E_0/\langle G_A, G_B\rangle$

A useful isogeny diagram

$$\begin{tikzcd} E_0 \arrow[r, "\theta"] \arrow[d, "\varphi"] & E_0 \arrow[d, "{[\theta]^*\varphi}"] \\ E \arrow[r, "{[\varphi]^*\theta}"] & E' \end{tikzcd}$$

where $\ker([\theta]^*\varphi) = \theta(\ker\varphi)$ and $\ker([\varphi]^*\theta) = \varphi(\ker\theta)$.

- This is basically an SIDH diagram where one of the isogenies is an endomorphism
- Key observation is that $E/\varphi(ker(\theta))$ is isomorphic to $E_0/\theta(ker(\varphi))$
- This motivates that endomorphisms somehow act on fixed degree isogenies

A group action

- How to look at endomorphisms as a group?
- Fix an integer N and conside all endomorphisms whose degree is coprime to N
- These clearly form a group (as the dual is a quasi inverse) but what is this group
- Let $End(E_0) = O$. Then $O/NO \cong M_2(\mathbb{Z}/N\mathbb{Z})$
- short proof: every endomorphism can be written as matrix by viewing its action on $E_0[N]$ and modulo N you have N^4 distinct choices hence you should get everything
- Now from this it follows that $(O/NO)^*$ is isomorphic to $GL_2(\mathbb{Z}/N\mathbb{Z})$

A group action II

- Cyclic isogenies of a fixed degree can be identified with (projective) points in $(\mathbb{Z}/N\mathbb{Z})^2$ and this set admits a natural group action of $GL_2(\mathbb{Z}/N\mathbb{Z})$
- Natural strategy of finding an isogeny of a fixed degree N this way: take a different isogeny of degree N and try to use the group action to map the known isogeny to the unknown one
- EC21: K, Merz, Petit, Weitkämper: try to attack SIDH with this idea
- Transporting one element to another one looks like a hidden shift problem

EC21 approach

- For Kuperberg to make sense we have to restrict to an abelian subgroup of $GL_2(\mathbb{Z}/N\mathbb{Z})$
- Evaluation of the group action goes using the above diagram
- We cannot directly translate the isogenies as they are not known so the group technically only acts on the curves N-isogenous to E_0 (we need to assume that there is a one-to-one correspondence between N-isogenies and order N cyclic subgroups)
- This only works for θs whose degree divides B in SIDH
- Lucky: θ is only defined modulo N so maybe there is a representative of every coset whose degree divides B
- Unlucky: only if B is very big, in that case one can find it for a quaternion lifting problem

Remarks

- EC21, an interesting idea but strictly worse than previous SIDH attacks
- Many annoying technical details have to handled and we are throwing away most of the information when restricting to an abelian subgroup
- How can we leverage more information? Idea: let's look at stabilizers!
- When does it happen that θ keeps the isogeny intact? If the kernel of θ is an eigenvector of θ
- if I have access to the stabilizer and it is big enough, then hopefully I can retrieve its kernel by finding common eigenvectors of matrices (Kipnis-Shamir!)
- Can this idea be used for cryptanalysis

pSIDH

- Is there some way of getting a Diffie-Hellman-lik key exchange on supersingular elliptic curves and avoiding the SIDH attacks

  Way 1: SIDH countermeasures

  Way 2: pSIDH where one provides an isogeny representation
- Isogeny representation: Some information that allows you to evaluate the secret isogeny on any point (up to a scalar)

pSIDH II

- Why would that seem secure as there is seemingly an infinite amount of torsion information? $\rightarrow$ use isogenies with big prime degree
- In pSIDH the endomorphism ring of the starting curve is known and this representation is accomplished by revealing some endomorphisms (suborder representation) on the public curve

Problem (IsERP)

Given the endomorphism ring of E_0 and an isogeny representation of an isogeny of degree N from E_0 to E_1, compute the endomorphism ring of E_1

- This problem is again well-known for smooth degree isogenies, the difficult case is when the isogeny has a big prime degree

The group action revisited

- Our goal is to apply the previous group action in this framework
- One simple issue is that if you only have E, E_A, then it is not clear how you can evaluate the group action without knowing the kernel
- In the useful diagram you "take a detour" when evaluating the group action, so in EC21 we act on curves and not isogenies and one needs a one-to-one correspondence between them
- Idea: Let us act on isogeny representations as they are in bijection with cyclic subgroups!
- Luckily you can actually transmit the isogeny representation through the useful diagram

Stabilizers

- "It is our stabilizers, Harry, that show what we truly are" by Albus Dumbledore
- We know the acting group but what are the stabilizers? Let's fix a basis and calculate it for $(1, 0)$
- What are the matrices whose eigenvector is $(1, 0)$? Upper triangular ones. This also implies that any stabilizer is just a conjugate of upper triangular matrices (these are called Borel subgroups)
- Computing stabilizers is a special instance of the famous hidden subgroup problem. However, $GL_2(\mathbb{Z}/N\mathbb{Z})$ is non-abelian
- "Non-abelian HSP can not be solved in polynomial time" by every cryptographer
- Even though the above statement is almost true, there are exceptions!

Stabilizers II

- The most well-known exception is normal subgroups but Borel subgroups are not normal
- Other exceptions include groups that are almost abelian like nilpotent groups with nilpotency class 2, again not our case
- Finally Borel subgroups in GL_2 is also a case that can be solved in polynomial time basically reducing it to a generalized hidden shift problem
- Generalized hidden shift: you have many (roughly the order of the group many) functions f_i and there is an element $h \in G$ such that $f_i(x) = f_{i+1}(x + h)$

Hidden Borel subgroup, a classical algorithm

- Let $S \in (\mathbb{Z}/N\mathbb{Z})^2$ be a cyclic subgroup corresponding to the isogeny and let H be the corresponding stabilizer
- We can define a function $f : G \to (\mathbb{Z}/N\mathbb{Z})^2$ as $g \mapsto g * S$
- Let $V = (\mathbb{Z}/N\mathbb{Z})^2$. Suppose $N = l^k$ (you can generalize with CRT). Then the idea is to recover $S \cap l^i V$ recursively by using a simple condition to test whether a given group element is in H
- If $\sigma + 1$ is invertible mod N, then it is in H if and only if $f(\sigma + 1) = f(1)$
- Finding $S \cap l^{k-1} V$ is done by brute-force ($l + 1$ choices) and the testing procedure and then this idea is carried out with an iterated lifting

Matrix representation

- The above trick really works with matrices so we need to represent O/NO as actual 2×2 matrices
- Usual evaluate them on the N-torsion won't work as the N-torsion is defined over a huge extension
- Instead you study the structure of O/NO as a ring and find an explicit isomorphism to $M_2(\mathbb{Z}/N\mathbb{Z})$

Problem

Given an algebra A isomorphic to $M_n(K)$ given by a multiplication table, find an explicit isomorphism

Matrix representation II

- This problem for generic algebras is pretty interesting as has a connection with norm equations, parametrizations of algebraic varieties, finding generators of the Mordell-Weil group, this special case is pretty easy though
- This problem is actually already there in KLPT
- For prime N this basically boils down to finding a zero divisor, or equivalently an element in O whose norm is divisible by N. This is just solving a quadratic form modulo N (that generates a minimal left ideal and the action of the algebra on the ideal gives you the explicit isomorphism)
- For non-prime N we solve this in the paper. One can factor N and reduce to the prime power case and use idempotent lifting

Stabilizer revisited

- Suppose you can compute the group action, then you can compute the stabilizer
- What is this stabilizer really? Let ϕ be the secret isogeny and let I_ϕ be the corresponding left ideal
- Then one has that if $\theta \in I_\phi$, then $\theta(ker(\phi)) = 0$. This implies that $\mathbb{Z} + I_\phi$ is in the stabilizer
- Now take σ from the stabilizer. Let $ker(\phi) = A$, then $\sigma(A) = \lambda A$ and thus $\sigma - \lambda \in I_\phi$

Stabilizer revisited II

- Thus $Stab(\phi) = Z + I_\phi$ which is the Eichler order of level N corresponding to the secret isogeny
- Two ways of getting the endomorphism:
  1. Take a non-trivial element of the stabilizer, compute its eigenvalue and that gets you an element from I_ϕ
  2. Take a different isogeny ψ, compute the stabilizer, conjugate the two stabilizers and a conjugating endomorphisms will map one isogeny to the other one and the useful diagram will reveal the endomorphism ring of the codomain
- It is not hard to see that conjugating stabilizers is the same as solving the transportation problem for the group action. Indeed, $g * x = y$ is equivalent to $gStab(x)g^{-1} = Stab(y)$. There is one technical element missing for this approach but that will be resolved later

Evaluating the group action

- Seems like we have everything we need. Hold on: how do we evaluate this group action

$$
\begin{tikzcd}
E_0 \arrow[r, "\theta"] \arrow[d, "\varphi"] & E_0 \arrow[d, "{[\theta]^*\varphi}"] \\
E \arrow[r, "{[\varphi]^*\theta}"] & E'
\end{tikzcd}
$$

- Key observation is that $E/\phi(ker(\theta))$ is isomorphic to $E_0/\theta(ker(\phi))$
- We have unlimited torsion point information, so this is fine right? No, as θ might not have a smooth degree. Good news: θ is only specified modulo N Bad news: Is it really easy to lift θ to an element of powersmooth norm?

The lifting problem

- PQLP: Given θ and N find $\tau \in O$ such that $Norm(\theta + N\tau)$ is powersmooth
- This is something that appears in KLPT but there it is enough to solve this for $j\mathbb{Z}[i]$ (in EC21 we solve it for $\mathbb{Z}[i]$)
- In KLPT this is the only step that requires the use of $j - 1728$. Why is this not straightforward? Because the norm equation is too ugly...
- Solving a norm equation is like meeting a lion. It is much better to meet it in a safe space than encounter it in the wild

Lifting problem

- How does the lifting problem look in general? For simplicity let us take $j - 1728$:
- One is given an element $a + bi + cj + dk$ and an integer N and we need x, y, z, u such that

$$(a + Nx)^2 + (b + Ny)^2 + p(c + Nz)^2 + p(d + Nu)^2$$

  is powersmooth
- If $a, b = 0$, this looks a lot nicer, in general pretty scary
- First idea: lifting is multiplicative, so if we lift elements in $j\mathbb{Z}[i]$, maybe they generate O/NO
- $(aj + bk) \cdot (cj + dk) = (-pac - pbd) + i(ad - bc)$, thus is in $\mathbb{Z}[i]$ and can be shown that it won't generate everything

Lifting problem II

- Second idea: powersmooth endomorphisms do not need lifting!
- Third idea: Fix a powersmooth endomorphism γ and given σ, try to write it as $\sigma = \gamma_1 \gamma \gamma_2 \gamma \gamma_3 \pmod{NO}$ where $\gamma_i \in j\mathbb{Z}[i]$
- By a counting argument there is a good chance that this is solvable and if it fails you can try again with a different γ
- How can we solve an equation of this type? For simplicity we stay with $j - 1728$ but easily adaptable to any other maximal order

Lifting problem III

- Let $\sigma = A + Bj$ and $\gamma = C + Dj$ where $A, B, C, D \in R$ where $R = \mathbb{Z}[i]$
- We write $\gamma_i = jx_i$ and thus our variables are $x_i \in R$

$$\begin{cases} (n(C)^{-1}p^{-1})(pA\bar{D}x_3 - pB\bar{C}\bar{x}_3) = x_1\bar{x}_2 \bmod NR, \\ (n(D)^{-1}p^{-1})(ACx_3 + pBD\bar{x}_3) = x_1x_2 \bmod NR. \end{cases} \tag{1}$$

- The right hand sides of the equation system have the same norm
- One can show (using an adaptation of Hilbert's theorem 90) that if we can find x_3 such that the norms of $(n(C)^{-1}p^{-1})(pA\bar{D}x_3 - pB\bar{C}\bar{x}_3)$ and $(n(D)^{-1}p^{-1})(ACx_3 + pBD\bar{x}_3)$, then we can solve the equation system
- This leads to a quadratic equation that has a good chance of having a solution and it can be found easily

Open questions

- The approach I outlined works well for prime degree isogenies. For certain other degree complications can arise, several approaches for this are outlined in our Appendix
- Is there some way of combining this approach with the SIDH attacks? If so, can that be used to break M-SIDH
- As mentioned before, being able to evaluate this group action can aslo be considered more generally (without isogeny representations) when there is a bijection between cyclic subgroups of order N and N-isogenous curves. In these cases can this approach be used for cryptanalysis
- Are there any applications of the new lifting algorithm, e.g., to improve KLPT?