How not to break SIDH: Martindale and Panny

Shahed Sharif

October 31, 2019

The paper I will discuss covers a variety of mostly unsuccessful attacks on the SIDH protocol. There are some ideas for future attacks, including open questions.

1 SIDH protocol

SIDH is a key exchange protocol (Supersingular Isogeny Diffie-Hellman). The set-up is as follows. Fix a large prime p and a supersingular curve E over $\mathbb{F}_p$. Choose large integers n, m, and choose points $P_1, P_2, Q_1, Q_2 \in E$ such that P_1, P_2 generate $E[2^n]$ and Q_1, Q_2 generate $E[3^m]$. We want these points to be rational over $\mathbb{F}_{p^2}$; by choosing $p \equiv 1 \pmod{2^n 3^m}$, we can force this to be true. The tuple $(p, E, P_1, P_2, Q_1, Q_2)$ are made public.

To generate a key, Alice chooses a random integer a and computes the elliptic curve $E_A = E/\langle P_1 + aP_2 \rangle$. She computes the images $Q_{A,1}, Q_{A,2}$ of Q_1, Q_2 in E_A and publishes the triple $E_A, Q_{A,1}, Q_{A,2}$. Bob similarly chooses random b, $E_B = E/\langle Q_1 + bQ_2 \rangle$, and the images $P_{B,1}, P_{B,2}$ of P_1, P_2 in E_B. He publishes $E_B, P_{A,1}, P_{A,2}$. The shared key is the j-invariant of

$$E_{AB} = E_B/\langle P_{B,1} + aP_{B,2} \rangle = E_A/\langle Q_{A,1} + bQ_{A,2} \rangle .$$

That is, E_{AB} is the pushout

$$\begin{array}{ccc} E & \longrightarrow & E_A \\ \downarrow & & \downarrow \\ E_B & \longrightarrow & E_{AB} \end{array}$$

The security of the protocol depends on the difficulty of determining a given E and E_A. It turns out that as long as we can find *some* isogeny $E \to E_A$, we can find a efficiently. Thus we pose the following problems:

Problem 1 (Supersingular Isogeny Problem)**.** *Given supersingular elliptic curves E, E' which are isogenous over $\mathbb{F}_{p^2}$, find an isogeny between them.*

Problem 2 (Supersingular Isogeny Problem with auxiliary points)**.** *Given supersingular elliptic curves E, E' which are isogenous over $\mathbb{F}_{p^2}$, and given $Q_1, Q_2 \in$*

E and their respective images $Q'_1, Q'_2 \in E'$ under some isogeny, find an isogeny between them.

Certainly the second problem should be easier than the first, but it is difficult to see this in practice.

2 Attacks: no auxiliary points

Graph attacks. For the Supersingular Isogeny Problem, an equivalent statement is as follows. Let Γ be the graph whose vertices are isomorphism classes of supersingular elliptic curves over $\mathbb{F}_{p^2}$, and whose edges are isogenies, except we identify an isogeny with its dual (so edges are undirected). Then given two vertices lying in a connected component of Γ, we wish to find a path between them. Typically we instead use the ℓ-isogeny graph $\Gamma(\ell)$, which has the same vertex set, but now isogenies are those of degree ℓ. (Of course, in our case $\ell = 2$ or 3.) In fact, most attacks use this version of the problem, by implementing a "meet-in-the-middle" algorithm. These attacks are $O(\sqrt[d]{p})$, where $d = 4$ (classical) or $d = 6$ (quantum, though the memory requirements in this case are prohibitive).

Endomorphism rings. The (full) endomorphism ring of a supersingular curve is a maximal order in a known quaternion algebra. It has been shown that if we can compute the maximal order, even as an abstract ring, then we can solve the isogeny problem. However, it has been shown that under certain assumptions, computing endomorphism rings is computationally equivalent to solving the isogeny problem. One way to see this is to observe that the best method for computing endomorphism rings uses the graph Γ. Specifically, one takes a random walk from a vertex v_0 and hopes to end up back at v_0. Once this happens, the resulting loop yields an endomorphism of the corresponding elliptic curve. If one repeats this enough time, one hopes to get a generating set for the endomorphism ring.

$\mathbb{F}_p$-spine. Let $G(\ell) \subset \Gamma(\ell)$ be the full subgraph whose vertices are isomorphism classes of supersingular elliptic curves over $\mathbb{F}_p$. Note that isogenies between them need not be $\mathbb{F}_p$-rational. Then one can hope to find a path via $G(\ell)$; that is, given $E, E' \in \Gamma(\ell)$, we wish to find $C, C' \in G(\ell)$ and paths $E \to C$, $C \to C'$, and $C' \to E'$. The composition of these paths solves the isogeny problem. This approach is fruitful only if the problems of

1. finding a path to $G(\ell)$, and
2. finding paths inside $G(\ell)$

are both easier than directly solving the full isogeny problem. For the 1st problem, there are no known methods. One idea is, for $E \in \Gamma(\ell)$, to compute an ℓ-power isogeny between E and its quadratic twist and hope that it passes through $G(\ell)$; but the data suggests that this is not feasible in general.

Delfs-Galbraith tackled the second problem. Their algorithm is, heuristically, $\widetilde{O}(\sqrt[4]{p})$.

Lifting. Deuring showed that if one fixes a pair (E, φ) where φ is an endomorphism of the elliptic curve E, then there is a canonical lift of the pair to the appropriate p-adic ring. One can then base-extend to $\mathbb{C}$ and solve the isogeny problem there. However, this process does not work if $\varphi = [n]$, and we don't have a good way of finding a nontrivial endomorphism for a generic supersingular elliptic curve. Furthermore, lift computations typically must be done over a high degree number field.

2.1 Weil restrictions

The following idea seems to be relatively unexplored, and Martindale-Panny list several related open problems.

The main idea is to replace $E/\mathbb{F}_{p^2}$ with its Weil restriction $W(E)/\mathbb{F}_p$. The latter will be a principally polarized supersingular abelian surface. Let $A = W(E)$. Martindale-Panny assume that $\mathrm{End}_{\mathbb{F}_p}(A) \otimes \mathbb{Q}$ is the number field $\mathbb{Q}(\pi)$, where π is the Frobenius endomorphism. Since we expect $j(E) \notin \mathbb{F}_p$, π will be a nontrivial endomorphism of A.

We consider the isogeny graph of principally polarized supersingular abelian surfaces. Isogenies between two such must be maximal isotropic with respect to the Weil pairing, and so we consider the graph G_ℓ whose edges correspond to (ℓ, ℓ) isogenies defined over $\mathbb{F}_p$; that is, isogenies with kernel isomorphic to $\mathbb{Z}/\ell \times \mathbb{Z}/\ell$. Let $L = (\ell_1, \ldots, \ell_n)$ where the ℓ_i are distinct primes, and let $G_L = \cup_{\ell_i} G_{\ell_i}$; that is, two surfaces are adjacent if and only if they are adjacent in one of the G_{ℓ_i}.

Given E, E' supersingular, let $A = W(E), A' = W(E')$. We would like to solve the isogeny problem for A, A' in G_L for some choice of L. A necessary condition to do so is that A, A' must lie in the same connected component of G_L.

Conjecture 2.1. *For most ℓ, G_ℓ is a union of cycles of length $O(\sqrt{p})$.*

The idea is that under our assumption that $\mathrm{End}(A) \cong \mathbb{Q}(\pi)$, the isogeny graph G_ℓ should resemble the isogeny graph of ordinary elliptic curves; that is, an isogeny volcano. The volcano has a cycle of the prescribed length (the *crater*) and some trees attached to vertices of the crater. We would like to show that there are no such trees. If B were an abelian surface corresponding to a vertex on one of these trees, then $\mathrm{End}(B) \subset \mathrm{End}(A)$, and the index would be divisible by ℓ. For most ℓ, $[\mathrm{End}(A) : \mathbb{Z}[\pi]]$ will be coprime to ℓ. But $\mathbb{Z}[\pi] \subset \mathrm{End}(B)$, so there should be no such B.

If the conjecture is true, then we almost certainly need to pick L large in order for A, A' to lie in the same component.

Question 1. *In order for the probability that A, A' lie in the same connected component of G_L to be high, how large should L be?*

Ideally, the number of primes should only need to be polynomial in $\log p$.

We could also implement the Delfs-Galbraith plan; that is, find a path to an $\mathbb{F}_p$-curve.

Question 2. *For L small, given A, is there a surface of the form $W(E_0)$, with E_0 an elliptic curve defined over $\mathbb{F}_p$, in the same connected component as A?*

In order to utilize the graph to solve the isogeny problem, we would likely need to be able to compute (ℓ, ℓ)-isogenies.

Question 3. *What is the complexity of computing (ℓ, ℓ)-isogenies?*

Currently, we only know how to compute $(2, 2)$-isogenies efficiently.

3 Attacks: auxiliary points

Interpolation. Recall that in SIDH, we not only know E, E' isogenous, we also know a basis for $E[m]$ for some m coprime to the degree of an isogeny $\varphi : E \to E'$, and we know the image of the basis under that isogeny. Furthermore, using the fact that E is supersingular, one can show that φ is of the form

$$\varphi(x, y) = (f(x), c_0 y f'(x))$$

for some rational map f over $\mathbb{F}_{p^2}$. We could use our auxiliary point data to deduce f. However, f has a very long description, so this is likely inefficient.

Tate modules. Perhaps we can lift the action on m to a map $T_\ell(E) \to T_\ell(E')$ for some $\ell \mid m$ ($\ell = 3$ in practice). Petit has an attack that does this, but it is only feasible when (say) Alice's subgroup is much smaller than Bob's.