On the Degree-Insensitive SI-GDH problem and assumption

Samuel Dobson and Steven D. Galbraith

Mathematics Department, University of Auckland, New Zealand.
samuel.dobson.nz@gmail.com, s.galbraith@auckland.ac.nz

August 15, 2019

Abstract

Fujioka, Takashima, Terada and Yoneyama, in their 2018 work on an authenticated key exchange protocol using supersingular isogenies, use new assumptions in their security proof of the scheme. In particular, they define the degree-sensitive and degree-insensitive SI-GDH assumptions and problems. These assumptions include a decision oracle that is used in the security proofs. We give evidence that those assumptions are not well defined. Hence, the security proofs in their paper do not seem to be correct.

1 Introduction

Consider an isogeny between two supersingular curves $\phi : E(\mathbb{F}_{p^2}) \to E'(\mathbb{F}_{p^2})$, where $p = \ell_A^{e_A} \cdot \ell_B^{e_B} \cdot f \pm 1$ is prime. In SIDH [JDF11, DFJP14] and similar schemes, the public key of a participant in the scheme consists of both the target curve E', as well as the image of two specific points P', Q' under ϕ. The secret isogeny of participant A and B in the key exchange will have degree $\ell_A^{e_A}$ or $\ell_B^{e_B}$ respectively, and the points P_A, Q_A, P_B, Q_B are some publicly defined bases for the $E[\ell_A^{e_A}]$ and $E[\ell_B^{e_B}]$ torsion subgroups of E (respectively). That is, $E[\ell_A^{e_A}] = \langle P_A, Q_A \rangle$ and likewise for B.

In this work, we are interested in the commutative diagram Figure 1.

$$\begin{tikzcd}
E \arrow[r, "\phi_A"] \arrow[d, "\phi_B"'] & E_A \arrow[d, "\phi_{AB}"] \\
E_B \arrow[r, "\phi_{BA}"'] & E_{AB}
\end{tikzcd}$$

Figure 1: Commutative diagram of SIDH, where $\ker(\phi_{BA}) = \phi_B(\ker(\phi_A))$ and $\ker(\phi_{AB}) = \phi_A(\ker(\phi_B))$. Figure 3 of [FTTY19]

Figure 1 depicts the two public key curves E'_A and E'_B of participants A and B, along with the fourth curve E'_{AB}. In SIDH, the isomorphism class of this fourth curve is uniquely determined by the choice of secret kernels by participants A and B. In fact, an important characteristic of the isogenies used in SIDH is that the degrees of these isogenies ϕ_A, ϕ_B is much less than the number of isomorphism classes of supersingular elliptic curves (roughly $p/12$). This means that the public curves (E, E_A, E_B) uniquely determine the shared curve E_{AB} (of course, this is hard to compute without secret information). Thus, the j-invariant of the final curve produced by both parties will function as a shared secret. Throughout the remainder of this paper, we shall define $i \in \{A, B\}$ to represent one participant in the protocol, and $\bar{i} \in \{B, A\}$ to represent the other ($\bar{i} = A$ iff $i = B$). The participants provide images of basis points so that their counterpart can efficiently compute the curve E_{AB} - the public key points $P'_i = \phi(P_i)$ and $Q'_i = \phi(Q_i)$ allow the isogenies to be "composed", giving ϕ'_{AB} from ϕ'_B and similarly for A.

If isogenies of larger degree are allowed to be used, then eventually (the isomorphism class of) E_{AB} is no longer uniquely determined by E_A and E_B. The natural question we will be investigating in this short note, directly related to the degree-insensitive oracle of [FTTY19], is whether the additional provision of torsion generator images provide enough additional restriction to uniquely define E_{AB}.

1.1 Acknowledgements

We thank Katsuyuki Takashima for his helpful feedback and comments.

2 Definitions and conjectures

In the ensuing discussion, we shall work with the finite field $\mathbb{F}_{p^2}$ for a fixed prime p. We shall begin by defining various sets which will be used in the subsequent discussion. The first, is the set of triples

$$PK_i = \{(E', P', Q') \,|\, E' \text{ supersingular, } P', Q' \in E'(\mathbb{F}_{p^2}), \langle P', Q' \rangle = E'[\ell_{\bar{i}}^{e_{\bar{i}}}]\} \tag{1}$$

Note that this definition is completely independent of any isogeny from E to E'.

We then define the sets of **valid** SIDH public keys. There are two important cases which correspond respectively to the degree-sensitive and degree-insensitive SI-GDH problems [FTTY19]. The first is the exact case described above:

$$PK_i^{ds} = \{(E', P', Q') \,|\, \exists \phi : E \to E', P' = \phi(P_{\bar{i}}), Q' = \phi(Q_{\bar{i}}), \deg \phi = \ell_i^{e_i}\} \tag{2}$$

The second case is similar, but the restriction on the degree of ϕ is loosened:

$$PK_i^{di} = \{(E', P', Q') \,|\, \exists \phi : E \to E', P' = \phi(P_{\bar{i}}), Q' = \phi(Q_{\bar{i}}), \deg \phi = \ell_i^{m}, m \in \mathbb{Z}^+\} \tag{3}$$

As we shall soon discuss, in the first of these two sets, the degree uniquely determines the ϕ for each tuple. In the second case, however, it is one of our main conjectures that the ϕ are not uniquely determined by the triples in PK_i^{di}.

Now that we have defined these three sets, we shall define corresponding "SIDH square" sets. The first of these is the weakest case:

$$\chi = \{(pk_A, pk_B, j(E')) \,|\, pk_A \in PK_A, pk_B \in PK_B, E'(\mathbb{F}_{p^2}) \text{ supersingular}\} \tag{4}$$

Then we have the degree-sensitive and degree-insensitive restricted versions of this set:

$$\begin{aligned} \chi^{ds} = \{(pk_A, pk_B, j(E_{AB})) \,|\, & pk_A \in PK_A^{ds}, pk_B \in PK_B^{ds}, \\ & \text{there exists a supersingular elliptic curve } E_{AB} \\ & \text{ and isogenies between } pk_A, pk_B, E_{AB} \text{ which} \\ & \text{ satisfy the conditions in Figure 1}\} \end{aligned}$$

$$\begin{aligned} \chi^{di} = \{(pk_A, pk_B, j(E_{AB})) \,|\, & pk_A \in PK_A^{di}, pk_B \in PK_B^{di}, \\ & \text{there exists a supersingular elliptic curve } E_{AB} \\ & \text{ and isogenies between } pk_A, pk_B, E_{AB} \text{ which} \\ & \text{ satisfy the conditions in Figure 1}\} \end{aligned}$$

These two sets both correspond to valid SIDH squares in the two different settings, with the second simply loosening the restriction on the degrees - $\deg \phi_A = \deg \phi_{BA} = \ell_A^m$ for any integer m, and $\deg \phi_B = \deg \phi_{AB} = \ell_B^n$ for any integer n.

Fujioka et al. [FTTY19] use an oracle in their security proof which distinguishes between the set χ, and the set of all **valid** public key tuples and final j-invariants χ^{ds} or χ^{di} which fit a commutative diagram as in the scheme above. We conjecture, though, that in the degree-insensitive case, $\chi = \chi^{di}$ - that is, all possible pairs of basis points on all possible supersingular elliptic curves, and all final shared j-invariants, can be reached by a suitable choice of degree-insensitive ϕ_A and ϕ_B. The aim of this short note is to give some evidence for this conjecture.

Fujioka et al. hints toward this problem, stating

> Therefore, as an extreme possible case, any tuple of supersingular elliptic curves (E_A, E_B, E_{AB}) might form the commutative diagram in [Figure 1], that is, any tuple of such curves would be true instances in the hypothetical case. We cannot exclude such possibility from our present knowledge of the di-SI-GDH problem.

We conjecture a much stronger result, however. We proceed in two stages. In the first, we will give evidence that all possible public key tuples PK_i of such schemes can arise as valid public key tuples (when considering all possible choices of ϕ_i). This is Conjecture 1.

Conjecture 1. $PK_i = PK_i^{di}$

We then give evidence that, given any two such public key tuples $pk_A \in PK_A, pk_B \in PK_B$, and for any choice of supersingular curve E', $(pk_A, pk_B, j(E')) \in \chi^{di}$. In other words, any supersingular j-invariant is a valid shared secret and may be produced in a degree-insensitive key exchange with those keys. This is because the loosened restriction on the degree of the isogenies ϕ_i is not enough to uniquely determine the isomorphism class of the fourth curves E_{AB}, there exist many different isogenies with different kernels which produce the same public key tuples. This is summarised in Conjecture 2.

Conjecture 2. $\chi = \chi^{di}$

3 Uniqueness of isogenies from public keys

In the SIDH protocol, the public keys used by each participant uniquely determine the secret isogenies used [MP19], and thus also the shared secret (although this is, of course, hard to compute without the secret knowledge).

We now show that even in the degree-insensitive case, if one participant uses an isogeny of the correct degree, the public keys uniquely determine the shared secret.

Lemma 1. *In the degree-insensitive case, if participant i uses an isogeny of the correct (degree-sensitive) degree,* $\deg \phi_i = \ell_i^{e_i}$*, then $j(E_{AB})$ is uniquely determined regardless of* $\deg \phi_{\bar{i}}$.

Proof. Without loss of generality, assume that it is participant B who uses an isogeny ϕ_B of correct degree. Refer to Figure 2. As usual, we have an elliptic curve E along with a chosen $\ell_B^{e_B}$-torsion basis P_B, Q_B. ϕ_B thus has kernel $\langle K = P_B + \alpha Q_B \rangle$ for some α. Suppose that we have two isogenies $\phi_A, \phi_A' : E \to E_A$ such that

$$P' = \phi_A(P_B) = \phi_A'(P_B) \qquad Q' = \phi_A(Q_B) = \phi_A'(Q_B)$$

Denote the kernels of these maps by G_A, G_A' respectively (so clearly $E/G_A \cong E/G_A'$). Now irrespective of which isogeny participant A used, B will compute the isogeny ϕ_{AB} with kernel

$$\ker \phi_{AB} = \langle P' + \alpha Q' \rangle$$

And thus E_{AB} is uniquely determined (up to isomorphism)

$$E/\langle \ker \phi_B, G_A\rangle \cong E/\langle \ker \phi_B, G'_A\rangle \cong E_{AB}$$

□

$$\begin{tikzcd}
E \arrow[r, bend left, "\phi_A"] \arrow[r, bend right, "\phi'_A"'] \arrow[d, "\phi_B"'] & E_A \arrow[d, "\phi_{AB}"] \\
E_B \arrow[r, bend left, "\phi_{BA}"] \arrow[r, bend right, "\phi'_{BA}"'] & E_{AB}
\end{tikzcd}$$

Figure 2: Commutative diagram of Lemma 1, where $\ker(\phi_{BA}) = \phi_B(\ker(\phi_A))$, $\ker(\phi'_{BA}) = \phi_B(\ker(\phi'_A))$ and $\ker(\phi_{AB}) = \phi_A(\ker(\phi_B)) = \phi'_A(\ker(\phi_B))$.

We thus require, for Conjecture 2, that both isogenies be of arbitrary-power degree, it is not sufficient for only one to be degree-insensitive.

4 Weil pairing restriction

As discussed in [GV18], following from Proposition 8.2 of Silverman [Sil09], the Weil pairing invokes the condition that, for an isogeny $\phi : E \to E'$,

$$e_N(\phi(P), \phi(Q)) = e_N(P, Q)^{\deg(\phi)} \tag{5}$$

Where $N = \ell_B^{e_B}$. This is a simple additional condition that can be applied to distinguish between χ and the χ^{ds} or χ^{di} in some cases. In many cases, such as those we will see in Section 5, this in fact provides no extra restriction on χ when $\deg(\phi)$ can be arbitrary powers of 2. In some cases where it does, though, this additional restriction can be incorporated easily into the definition of χ above, limiting the possible public key tuples. Then, we consider a distinguisher between this new χ and the set of valid public keys/j-invariants in exactly the same manner. We thus ignore it for the sake of simplicity, merely observing that the pairing is easily computed.

5 Experimental evidence

5.1 All public key tuples are valid

In this section we exhibit the experimental evidence we have collected for Conjecture 1.

In the case that $p = 2^3 3^2 - 1 = 71$, we have shown using `MAGMA`, that using arbitrary 2-isogenies, we can reach any pair of points P, Q which generate $E[3^2]$ on any elliptic curve in the isogeny graph (up to isomorphism). There are exactly 3888 unique ordered tuples of points P, Q on each elliptic curve $E(\mathbb{F}_{p^2})$ such that both P and Q have order 3^2, and $\langle P, Q\rangle = E[3^2]$. In order to accomodate for isomorphism classes of the curves, one particular representative curve was (arbitrarily) chosen for each j-invariant. Then, for all subsequent curves with the same j-invariant found by the algorithm, the isomorphism to the representative curve was computed and used to translate the points to this original curve. This allowed for removal of duplicates public key tuples. We found that all 3888 unique ordered pairs on all 7 isogenous supersingular curves were reached from the starting P, Q on the curve with j-invariant 0.

We have also verified this result with high probability on a larger case, where $p = 2^2 3^3 - 1 = 107$, in which case there are exactly $648 \times 486 = 314,928$ possible ordered pairs P, Q on each supersingular elliptic curve E, generating $E[3^3]$. We allowed our simulation to run until the points reached on the curve with j-invariant 94 totalled $314,673$, which is approximately 99.92% of the expected total number of points. Due to the probabilistic nature of the algorithm, the discovery of new pairs of points decreases rapidly as the number of duplicates increases, so we decided to end the simulation early (after a total of 20 million 2-isogenies had been traversed in the supersingular isogeny graph), deciding that this was overwhelming evidence that all points were likely reachable as in the smaller case. We see no reason that these results would not extend to supersingular curves over finite fields of any choice of p as required by the assumption.

In both of these cases, the Weil pairing imposes no extra restriction on the validity of a randomly chosen pair of linearly independent points for each choice of isogeny. Observe that for $N = 3^2$, 2 has order 6 modulo 9, and for $N = 3^3$, 2 has order $18 = \varphi(3^3)$, so there is no apparent theoretical reason why not all choices would be valid, and we observe this in practice.

5.2 All j-invariants are valid given any public keys

We now discuss Conjecture 2. Clearly Conjecture 2 relies on Conjecture 1, because if it were possible to distinguish PK_i from PK_i^{di}, the same distinguisher could be applied just to the public keys in χ to distinguish from χ^{di}. But Conjecture 2 also requires that the j-invariant $j(E_{AB})$ should not provide any advantage in distinguishing between the two sets.

We make an important observation, in that because the degree of the isogeny is allowed to be an arbitrary power of ℓ_i, the image of points $P_{\bar{i}}, Q_{\bar{i}}$ no longer uniquely determines the isogeny used. That is, not only does there exist a power-of-ℓ_i isogeny ϕ_i for any pair P', Q' such that $P' = \phi(P_{\bar{i}}), Q' = \phi(Q_{\bar{i}})$, but also that there exist many such isogenies, each with different kernels.

In order to demonstrate this in practice using `MAGMA`, we used an extension field such as $\mathbb{F}_{p^6}$ (where $p = 71$ as above) so that we can find a point of order 27 to function as the kernel of ϕ_B. Let $\alpha \in \mathbb{F}_{p^6}$ denote the element which generates the extension $\mathbb{F}_{p^6}$ over the base field $\mathbb{F}_p$. We begin with elliptic curve $E : y^2 + y = x^3$ with j-invariant 0. In the simulation we selected at random the points

$$P_B = (7\alpha^5 + 24\alpha^4 + 49\alpha^3 + 68\alpha^2 + 2\alpha + 5 : 46\alpha^5 + 36\alpha^4 + 38\alpha^3 + 31\alpha^2 + 3\alpha + 38 : 1)$$
$$Q_B = (41\alpha^5 + 29\alpha^4 + 3\alpha^3 + 23\alpha^2 + 32\alpha + 56 : 9\alpha^5 + 41\alpha^4 + 63\alpha^3 + 57\alpha^2 + 33\alpha + 1 : 1)$$

We also selected a point of order 27 to function as the kernel for the isogeny chosen by participant B (which must be of higher degree than 9 by Lemma 1)

$$K = (3\alpha^5 + 41\alpha^4 + 18\alpha^3 + 4\alpha^2 + 13\alpha + 45 : 27\alpha^5 + 57\alpha^4 + 49\alpha^3 + 11\alpha^2 + 65\alpha + 64 : 1)$$

We then proceeded via breadth first search along non-backtracking 2-isogenies in the graph to find two distinct isogenies $\phi_A, \phi'_A : E \to E'$, such that $\phi_A(P_B) = \phi'_A(P_B)$ and $\phi_A(Q_B) = \phi'_A(Q_B)$. We present here an example where $E' : y^2 + y = x^3 + 46x + 60$ (so $j(E') = 66$), and $\deg \phi_A = \deg \phi'_A = 2^{10}$. Non-backtracking means that no isogeny returned along its dual in the next step, ensuring that distinct paths will compose to produce isogenies with different kernels.

$$\phi_A(P_B) = (28\alpha^5 + 25\alpha^4 + 54\alpha^3 + 59\alpha^2 + 8\alpha + 66 : 66\alpha^5 + 64\alpha^4 + 36\alpha^3 + 63\alpha^2 + 29\alpha + 23 : 1)$$
$$\phi_A(Q_B) = (21\alpha^5 + \alpha^4 + 5\alpha^3 + 62\alpha^2 + 6\alpha + 66 : 58\alpha^5 + 67\alpha^4 + 51\alpha^3 + 36\alpha^2 + 47\alpha + 48 : 1)$$

Simply showing that isogenies with different kernels exist which produce the same public keys is an interesting observation. But to properly support Conjecture 2, we wish to demonstrate that these different kernels can produce different curves E_{AB}. The image of K under each of these isogenies is

$$\phi_A(K) = (44\alpha^5 + 39\alpha^4 + 59\alpha^3 + 41\alpha^2 + 55\alpha + 64 : 7\alpha^5 + 39\alpha^4 + 61\alpha^3 + 64\alpha^2 + 14\alpha + 47 : 1)$$
$$\phi'_A(K) = (67\alpha^5 + 49\alpha^4 + 11\alpha^3 + 19\alpha^2 + 53\alpha + 49 : 40\alpha^5 + 65\alpha^4 + 13\alpha^3 + 24\alpha^2 + 12\alpha + 67 : 1)$$

Finally, each of these images of degree 27 are used to create an isogeny ϕ_{AB}, ϕ'_{AB} to complete the SIDH square. The first determines an isogeny to the isomorphism class of curves with j-invariant 17, while the second gives j-invariant 48. Thus, despite both ϕ_A, ϕ'_A giving the same public key triple, each gives a different curve E_{AB} in this degree-insensitive key exchange. This shows that E_{AB} is not uniquely determined and strongly supports Conjecture 2. To demonstrate that there exist such "collisions" which produce any supersingular j-invariant would be computationally intensive in practice but the presence of at least one such case is strong evidence for our conjecture.

6 The di-SI-GDH oracle

Above we have discussed a particular problem of distinguishing between the set of all valid SIDH commutative diagrams χ^{ds}/χ^{di}, and a set of all tuples of supersingular elliptic curves with all possible choices of points (subject to the easy-to-compute restrictions above) on them and all possible shared-secret j-invariants, χ. In this section we briefly relate this to the specific working of the di-SI-GDH oracle of Fujioka et al. [FTTY19]. The oracle recieves public SIDH parameters including the curve E, points $P_A, Q_A, P_B, Q_B \in E$, and (candidate) public key tuples of party A and B, along with a j-invariant representing the shared secret obtained through the SIDH protocol with these keys. The oracle then returns true if isogenies exist between E, E_A, E_B, and a curve E_{AB} such that the public points are mapped in the correct way and the j-invariant of E_{AB} is equal to the one provided (see Figure 1). This oracle is used in the security proof to allow a correct simulation in the random oracle model.

Consider, firstly, the public key triples (E', P', Q') provided. Assuming the points obey the subgroup generation and Weil pairing restrictions, Conjecture 1 claims that these provide no way to distinguish between PK_i and PK_i^{di}, which are equal sets. But in addition to this, we give evidence to support the claim (Conjecture 2) that even by fixing a choice of two public keys, any choice of j-invariant $j(E')$ is still valid for some degree-insensitive choice of isogenies. We have given experimental evidence that there exist many different isogenies that produce any public key, each with a different kernel. We conjecture that because the kernels of these isogenies uniquely determine the final elliptic curve E_{AB} in the SIDH protocol, but because these kernels are not determined by the public keys, that any j-invariant would be a valid shared secret for any choice of public keys.

Thus we conjecture that the degree-insensitive SI-GDH oracle as a distinguisher between χ and χ^{di} cannot exist, because these sets are equal.

7 Conclusion

Our experiments give evidence to support our conjectures that all valid triples (E', P'_B, Q'_B) can arise in the degree-insensitive case (Conjecture 1), and that any j-invariant of the final shared curve isomorphism class is valid (Conjecture 2). Hence it does not make sense to consider a distinguisher between this set and a set of all points on all curves (subject to the subgroup generation and Weil pairing restrictions). Such a distinguisher - the di-SI-GDH oracle - is used in the security proof of the authenticated key exchange protocol in [FTTY19]. Hence, we believe that the security proof of Fujioka et al. [FTTY19] is not correct. We stress that this does not mean the protocol in [FTTY19] is broken, only that its security is not justified by the computational assumptions in the paper.

References

[DFJP14] Luca De Feo, David Jao, and Jérôme Plût, *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies*, Journal of Mathematical Cryptology **8** (2014), no. 3, 209–247.

[FTTY19] Atsushi Fujioka, Katsuyuki Takashima, Shintaro Terada, and Kazuki Yoneyama, *Supersingular isogeny Diffie–Hellman authenticated key exchange*, Information Security and Cryptology – ICISC 2018 (Cham) (Kwangsu Lee, ed.), Springer International Publishing, 2019, pp. 177–195.

[GV18] Steven D. Galbraith and Frederik Vercauteren, *Computational problems in supersingular elliptic curve isogenies*, Quantum Information Processing **17** (2018), no. 10, 265.

[JDF11] David Jao and Luca De Feo, *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies*, Post-Quantum Cryptography (Berlin, Heidelberg) (Bo-Yin Yang, ed.), Springer Berlin Heidelberg, 2011, pp. 19–34.

[MP19] Chloe Martindale and Lorenz Panny, *How to not break SIDH*, Cryptology ePrint Archive, Report 2019/558, 2019, `https://eprint.iacr.org/2019/558`.

[Sil09] Joseph H Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, Springer, Dordrecht, 2009.