Masked-degree SIDH

Tomoki Moriya

Department of Mathematical Informatics, The University of Tokyo, Japan
tomoki_moriya@mist.i.u-tokyo.ac.jp

Abstract. Isogeny-based cryptography is one of the candidates for post-quantum cryptography. SIDH is a compact and efficient isogeny-based key exchange, and SIKE, which is the SIDH-based key encapsulation mechanism, remains the NIST PQC Round 4. However, by the brilliant attack provided by Castryck and Decru, the original SIDH is broken in polynomial time (with heuristics). To break the original SIDH, there are three important pieces of information in the public key: information about the endomorphism ring of a starting curve, some image points under a cyclic hidden isogeny, and the degree of the isogeny.
In this paper, we proposed the new isogeny-based scheme named *masked-degree SIDH*. This scheme is the variant of SIDH that masks most information about degrees of hidden isogenies, and the first trial against Castryck–Decru attack. The main idea to cover degrees is to use many primes to compute isogenies that allow the degree to be more flexible. Though the size of the prime p for this scheme is slightly larger than that of SIDH, this scheme resists current attacks using degrees of isogenies like the attack of Castryck and Decru. The most effective attack for masked-degree SIDH has $\tilde{O}(p^{1/(8\log_2(\log_2 p))})$ time complexity with classical computers and $\tilde{O}(p^{1/(16\log_2(\log_2 p))})$ time complexity with quantum computers in our analysis.

Keywords: SIDH · isogeny-based cryptography · masked-degree SIDH

1 Introduction

Because Shor found the quantum algorithm to solve Prime Factorization and Discrete Logarithm Problem in [Sho94], we need some investigations for post-quantum cryptography. Isogeny-based cryptography is considered one of the candidates for post-quantum cryptography, and the compactness of isogeny-based cryptosystems is received a high evaluation.

SIDH is an isogeny-based Diffie-Hellman type key exchange scheme proposed in [JDF11]. SIDH has supported the world of isogeny-based cryptography for about 12 years due to its compactness and efficiency. However, Castryck and Decru proposed the breakthrough attack for SIDH in 2022 [CD22]. This attack breaks the original SIDH in polynomial time (with heuristics). The main vulnerability of SIDH is the following three points:

1. The structure of the endomorphism ring of a starting elliptic curve is revealed.

2. Public key needs the image of a subgroup of the starting curve under the hidden cyclic isogeny.
3. The degree of the hidden isogeny is fixed.

The attack of Castryck and Decru uses these pieces of information. Moreover, there are some other attacks for SIDH using these informations (*e.g.*, the torsion point attack [Pet17]).

In this paper, we propose the novel SIDH variation that resists the attack of Castryck and Decru. The main idea to resist this attack is to hide the degree of a secret isogeny. In other words, we try to eliminate the third weak point. To realize this idea, we refer to another isogeny-based key exchange named CSIDH [CLM$^+$18] in which the degrees of isogenies are not revealed. The reason why CSIDH successes covering the information of degrees is that one uses many primes to compute isogenies in CSIDH. To be more precise, in the CSIDH setting, one uses primes $\ell_1, \ldots, \ell_n$, and computes an isogeny of degree $\ell_1^{e_1} \cdots \ell_n^{e_n}$. Therefore, degrees of isogenies in CSIDH are flexible, while in the SIDH setting, one uses only one prime ℓ, and the degree of the isogeny must be a power of ℓ. From this idea, we take the prime p that has the form

$$p = \ell_{A,1}^{e_{A,1}} \ell_{B,1}^{e_{B,1}} \ell_{A,2}^{e_{A,2}} \ell_{B,2}^{e_{B,2}} \cdots \ell_{A,t}^{e_{A,t}} \ell_{B,t}^{e_{B,t}} - 1.$$

Here, $\ell_{A,1}, \ldots, \ell_{A,t}$ are primes for Alice, and $\ell_{B,1}, \ldots, \ell_{B,t}$ are primes for Bob. Using this type of prime, we construct the new isogeny-based scheme named *masked-degree SIDH.* This scheme can hide degrees of target isogenies sacrificing compactness.

Moreover, we analyze the security of masked-degree SIDH. In our analysis, the most effective attack for masked-degree SIDH is the brute force approach to find the degree of the hidden isogeny, and its complexity is $\tilde{O}(p^{1/(8\log_2(\log_2 p))})$ via classical computers and $\tilde{O}(p^{1/(16\log_2(\log_2 p))})$ via quantum computers. According to our analysis, the size of parameters and public keys of masked-degree SIDH is extremely huge. See Table 1 for the precise sizes of public keys.

2 Preliminaries

2.1 Elliptic curves and isogenies

In this subsection, we introduce some mathematical concepts and facts corresponding to isogeny-based cryptography. Refer to [Sil09] for the detailed explanation.

Let k be a field, and E a genus-1 curve. A pair of E and a point O_E in $E(k)$ is called an elliptic curve over k. An elliptic curve has an abelian group structure such that the identity is O_E. We often represent an elliptic curve by a genus-1 curve. Denote the n-torsion group of E by $E[n]$. If n is coprime to the characteristic of k, then there is a group isomorphism $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$. The j-invariant is an invariant for isomorphism classes of elliptic curves. For two elliptic curves E_0 and E_1 over k, it holds that $j(E_0) = j(E_1)$ if and only if

$E_0 \cong E_1$ over the algebraic closure of k. Let p be a prime, and k a finite field of characteristic p. If an elliptic curve E satisfies $\#E(k) \equiv 1 \pmod{p}$, then E is called supersingular. A supersingular elliptic curve over k is isomorphic to a curve over $\mathbb{F}_{p^2}$.

A surjective morphism between two elliptic curves that is also a group morphism is called an isogeny. For an isogeny $\phi\colon E \to E'$, there is the isogeny $\hat{\phi}\colon E' \to E$ such that $\hat{\phi} \circ \phi = [\deg \phi]$ in E and $\phi \circ \hat{\phi} = [\deg \phi]$ in E'. We call $\hat{\phi}$ the dual isogeny of ϕ. If an isogeny is separable as a morphism of curves, then the isogeny is called separable. For any finite subgroup G of E, there is a separable isogeny outgoing from E whose kernel is G. A cyclic isogeny is an isogeny whose kernel is a cyclic group. If there are two separable isogenies $\phi\colon E \to E_1$ and $\psi\colon E \to E_2$ with $\ker \phi = \ker \psi$, then it holds that $E_1 \cong E_2$ over the algebraic closure of k. A representative of an isomorphism class of E_1 is denoted by E/G. From a smooth-order subgroup G of E, there is an efficient formula to compute a separable isogeny $\phi\colon E \to E/G$ with $\ker \phi = G$ [Vél71]. Let n be an integer coprime to the characteristic of p. The n-Weil pairing e_n is the non-degenerate pairing $e_n\colon E[n] \times E[n] \to \mu_n$, where μ_n is the group of n-th roots of unity in the algebraic closure of k. It holds that $e_n(\phi(P), \phi(Q)) = e_n(P, Q)^{\deg \phi}$ for an isogeny ϕ.

2.2 SIDH

SIDH is a Diffie-Hellman key exchange scheme that uses pieces of information of torsion points for completing a (pseudo) commutative diagram:

$$\begin{tikzcd}
(E_0, P_A, Q_A, P_B, Q_B) \arrow[r] \arrow[d] & (E_A, \phi_A(P_B), \phi_A(Q_B)) \arrow[d] \\
(E_B, \phi_B(P_A), \phi_B(Q_A)) \arrow[r] & E_{AB} \cong E_{BA}
\end{tikzcd}$$

The precise scheme is as follows:

Public parameter: Let E_0 be the elliptic curve of j-invariant 1728. Set a prime p as $p = 2^{e_A}3^{e_B} - 1$. Let P_A and Q_A (resp. P_B and Q_B) be points generating $E_0[2^{e_A}] \cong (\mathbb{Z}/2^{e_A}\mathbb{Z})^2$ (resp. $E_0[3^{e_B}] \cong (\mathbb{Z}/3^{e_B}\mathbb{Z})^2$).

Public key (Alice): Alice first generates a random value $k_A \in (\mathbb{Z}/2^{e_A}\mathbb{Z})^\times$ as her secret key. Let $R_A = P_A + k_A Q_A$. Alice computes an isogeny $\phi_A\colon E_0 \to E_A := E_0/\langle R_A \rangle$ and image points $\phi_A(P_B), \phi_A(Q_B)$. Alice sends to Bob E_A and these image points as a public key.

Public key (Bob): Bob first generates a random value $k_B \in (\mathbb{Z}/3^{e_B}\mathbb{Z})^\times$ as his secret key. Let $R_B = P_B + k_B Q_B$. Bob computes an isogeny $\phi_B\colon E_0 \to E_B := E_0/\langle R_B \rangle$ and image points $\phi_A(P_B), \phi_A(Q_B)$. Bob sends to Alice E_B and these image points as a public key. Let k_B be his secret key.

Shared key: Let $R'_A = \phi_B(P_A) + k_A \phi_B(Q_A)$, and let $R'_B = \phi_A(P_B) + k_B \phi_A(Q_B)$. Alice computes $E_{AB} := E_B/\langle R'_A \rangle$, and Bob computes an isogeny $E_{BA} := E_A/\langle R'_B \rangle$. The value $j(E_{AB}) = j(E_{BA})$ is the shared key.

2.3 Castryck–Decru attack

In this subsection, we briefly explain Castryck–Decru attack for SIDH.

Some notations in this subsection come from the previous subsection. The core of their attack is to determine, from given κ and public information of SIDH, whether there is an isogeny ϕ' of degree 3^{e_B-b} with $\phi_B = \phi' \circ \kappa$ or not, where κ is an isogeny of degree 3^b outgoing from E_0. If the determination successes with high probability, we can reveal the secret isogeny ϕ_B as follows:

1. Compute all isogenies of degree 3^b outgoing from E_0 for some b.
2. Find an isogeny $\kappa\colon E_0 \to E_1$ of degree 3^b such that there is an isogeny ϕ' of degree 3^{e_B-b} such that $\phi_B = \phi' \circ \kappa$.
3. If $\deg \phi'$ is not 1, then set the target isogeny to ϕ', and repeat 1 and 2.
4. If $\deg \phi'$ is 1, then ϕ_B can be revealed from all κ's.

The problem is how to judge the existence of ϕ'. The key is Kani's theorem [Kan97, Theorem 2.6]. Before explaining this theorem, we define some important mathematical concepts. Let C and E be elliptic curves, $\psi\colon C \to E$ a separable isogeny, and H_1, H_2 subgroups of $\ker \psi$ such that $H_1 \cap H_2 = \{O_C\}$, $\#H_1 \cdot \#H_2 = \deg \psi$, and $\#H_1 + \#H_2 = N$. We call the set (ψ, H_1, H_2) an isogeny diamond configuration of order N between C and E. An anti-isometry with respect to the N-Weil pairing is a map $\iota\colon E[N] \to C[N]$ such that $e_N(\iota(R), \iota(S)) = e_N(R, S)^{-1}$ for all $R, S \in C[N]$. Let ω be the (N, N)-isogeny outgoing from $C \times E$ whose kernel is $\langle (R, \iota(R)), (S, \iota(S)) \rangle$, where $\{R, S\}$ is a generator of $C[N]$. If the codomain 2-dimension variety of ω is a product of two elliptic curves, we call ι a reducible anti-isometry. Kani's theorem claims that for an isogeny diamond configuration (ψ, H_1, H_2) of order N between C and E, there is a unique reducible anti-isometry $\iota\colon C[N] \to E[N]$ such that

$$\iota\left(\frac{\#H_1}{d} R_1 + \frac{\#H_2}{d} R_2\right) = \psi'(R_2 - R_1) \text{ for all } R_i \in [N/d]^{-1} H_i \ (i = 1, 2),$$

where $d = \gcd(\#H_1, \#H_2)$, and ψ' is an isogeny such that $\psi = \psi' \circ [d]$.

The way to judge the existence of ϕ' when E_0 is the curve of j-invariant 1728 is as follows:

1. Set $c = 2^{e_A-a} - 3^{e_B-b}$ such that c is positive, and only has prime factors congruent to 1 mod 4.
2. Compute an isogeny $\gamma\colon E_1 \to C$ of degree c by using the construction of the endomorphism ring of E_0.
3. Compute $P_c = \gamma(\kappa(2^a P_A))$ and $Q_c = \gamma(\kappa(2^a Q_A))$.
4. Compute the $(2^{e_A-a}, 2^{e_A-a})$-isogeny outgoing from $C \times E_B$ whose kernel is $\langle (P_c, 2^a \phi_B(P_A)), (Q_c, 2^a \phi_B(Q_A)) \rangle$.
5. If the codomain of the above $(2^{e_A-a}, 2^{e_A-a})$-isogeny is a product of two elliptic curves, there is an isogeny ψ' of degree 3^{e_B-b} such that $\phi_B = \psi' \circ \kappa$.

We now explain why the above method guarantees the existence of ψ'. If there is ψ' of degree 3^{e_B-b} such that $\phi_B = \psi' \circ \kappa$, there is an isogeny diamond configuration $(\psi' \circ \hat{\gamma}, H_1(:= \ker \hat{\gamma}), H_2(:= \hat{\gamma}(\ker \psi')))$ of order $2^{e_A - a}$ such that $\# H_1 = 2^{e_A - a} - 3^{e_B - b}$ and $\# H_2 = 3^{e_B - b}$. Therefore, from Kani's theorem, the isogeny $\psi' \circ \hat{\gamma}$ corresponds to a reducible anti-isometry, and the codomain of the $(2^{e_A - a}, 2^{e_A - a})$-isogeny is a product of two elliptic curves. On the contrary, if ψ' does not exist, then heuristically the codomain of the $(2^{e_A - a}, 2^{e_A - a})$-isogeny is not a product of two elliptic curves with a high probability because the ratio of products of two supersingular elliptic curves is negligible in Jacobian varieties of superspecial curves.

3 Construction of masked-degree SIDH

In this section, we explain the construction of masked-degree SIDH.

The heart of hiding degrees of isogenies is to expand the space of degrees via many primes. The main difference between masked-degree SIDH and the original SIDH is that in masked-degree SIDH, we set p as

$$p = \ell_{A,1}^{e_{A,1}} \ell_{B,1}^{e_{B,1}} \ell_{A,2}^{e_{A,2}} \ell_{B,2}^{e_{B,2}} \cdots \ell_{A,t}^{e_{A,t}} \ell_{B,t}^{e_{B,t}} - 1,$$

and consider a $\prod_{i=1}^{t} \ell_{A,i}^{e'_{A,i}}$-isogeny for random $e'_{A,i}$'s (resp. a $\prod_{i=1}^{t} \ell_{B,i}^{e'_{B,i}}$-isogeny for random $e'_{B,i}$'s) instead of a 2^{e_A}-isogeny (resp. a 3^{e_B}-isogeny). Here, some astute readers may notice that this construction is not sufficient to let degrees of isogenies hidden. We may find the degrees of isogenies by using Weil pairings and image points P', Q' in the public key. To avoid this, it is enough to take a random integer $\alpha \in (\mathbb{Z}/\prod_{i=1}^{t} \ell_{B,i}^{e_{B,i}} \mathbb{Z})^\times$ and compute $\alpha P', \alpha Q'$. Note that since $\deg [\alpha]$ is square, we may know $\prod_{i=1}^{t} \ell_{A,i}^{e'_{A,i}}$ is square or non-square in mod $\ell_{B,i}^{e_{B,i}}$ for all $i = 1, \ldots, t$ via the Weil pairing. The precise scheme of masked-degree SIDH is as follows:

Public parameter: Let E_0 be the elliptic curve of j-invariant 1728. Set a prime p as

$$p = \ell_{A,1}^{e_{A,1}} \ell_{B,1}^{e_{B,1}} \ell_{A,2}^{e_{A,2}} \ell_{B,2}^{e_{B,2}} \cdots \ell_{A,t}^{e_{A,t}} \ell_{B,t}^{e_{B,t}} - 1,$$

where $\ell_{A,1} = 2$, and $\ell_{A,2}, \ldots, \ell_{A,t}, \ell_{B,1}, \ldots, \ell_{B,t}$ are distinct odd primes. Let P_A and Q_A (resp. P_B and Q_B) be points generating $E_0[\prod_{i=1}^{t} \ell_{A,i}^{e_{A,i}}] \cong (\mathbb{Z}/\prod_{i=1}^{t} \ell_{A,i}^{e_{A,i}} \mathbb{Z})^2$ (resp. $E_0[\prod_{i=1}^{t} \ell_{B,i}^{e_{B,i}}] \cong (\mathbb{Z}/\prod_{i=1}^{t} \ell_{B,i}^{e_{B,i}} \mathbb{Z})^2$).

Public key (Alice): Alice first generates the following three randoms as her secret key:

$$(e'_{A,1}, \ldots, e'_{A,t}) \in \{0, 1, \ldots, e_{A,1}\} \times \cdots \times \{0, 1, \ldots, e_{A,t}\},$$
$$\alpha \in (\mathbb{Z}/\prod_{i=1}^{t} \ell_{B,i}^{e_{B,i}} \mathbb{Z})^\times, \quad k_A \in (\mathbb{Z}/\prod_{i=1}^{t} \ell_{A,i}^{e_{A,i}} \mathbb{Z})^\times.$$

Let $R_A = (\prod_{i=1}^{t} \ell_{A,i}^{e'_{A,i}})(P_A + k_A Q_A)$. Alice computes an isogeny $[\alpha] \circ \phi_A \colon E_0 \to E_A := E_0/\langle R_A \rangle$ and image points $\alpha\phi_A(P_B), \alpha\phi_A(Q_B)$. Alice sends to Bob E_A and these image points as a public key.

Public key (Bob): Bob first generates the following three randoms as his secret key:

$$(e'_{B,1}, \dots, e'_{B,t}) \in \{0, 1, \dots, e_{B,1}\} \times \cdots \times \{0, 1, \dots, e_{B,t}\},$$
$$\beta \in (\mathbb{Z}/\prod_{i=1}^{t} \ell_{A,i}^{e_{A,i}}\mathbb{Z})^{\times}, \quad k_B \in (\mathbb{Z}/\prod_{i=1}^{t} \ell_{B,i}^{e_{B,i}}\mathbb{Z})^{\times}.$$

Let $R_B = (\prod_{i=1}^{t} \ell_{B,i}^{e'_{B,i}})(P_B + k_B Q_B)$. Bob computes an isogeny $[\beta] \circ \phi_B \colon E_0 \to E_B := E_0/\langle R_B \rangle$ and image points $\beta\phi_A(P_B), \beta\phi_A(Q_B)$. Bob sends to Alice E_B and these image points as a public key.

Shared key: Let $R'_A = (\prod_{i=1}^{t} \ell_{A,i}^{e'_{A,i}})(\phi_B(P_A) + k_A\phi_B(Q_A))$, and let $R'_B = (\prod_{i=1}^{t} \ell_{B,i}^{e'_{B,i}})(\phi_A(P_B) + k_B\phi_A(Q_B))$. Alice computes $E_{AB} := E_B/\langle R'_A \rangle$, and Bob computes an isogeny $E_{BA} := E_A/\langle R'_B \rangle$. The value $j(E_{AB}) = j(E_{BA})$ is the shared key.

Theorem 1. *Masked-degree SIDH is correct.*

Proof. It is easy to check that $\ker(\phi'_A \circ \phi_B) = \ker(\phi'_B \circ \phi_A) = \langle R_A, R_B \rangle$. Therefore, it holds that $E_{AB} \cong E_{BA}$. □

4 Security analysis

In this section, we discuss the security of masked-degree SIDH.

4.1 Attacks for masked-degree SIDH

Solution to general Isogeny Problem. There are some studies about solving algorithms for Isogeny Problem. Using classical computers, Delfs and Galbraith proposed the algorithm for solving Isogeny Problem in $\tilde{O}(p^{1/2})$ [DG16]. Biasse, Jao, and Sankar provided the quantum algorithm with the complexity $\tilde{O}(p^{1/4})$ [BJS14]. These attacks can be adapted to masked-degree SIDH.

Meet in the middle attack. Meet in the middle attack was a basic attack for the original SIDH that computes all possible isogenies outgoing from E_0 and E_A and finds the collision of these isogenies. In the setting of SIDH, the degree of the target isogeny is 2^{e_A}; hence, we only need to consider computing 2-isogenies in $e_{A,i}/2$ steps. Although the degree of the secret isogeny is not revealed in the setting of masked-degree SIDH, this attack can be adapted to masked-degree SIDH because we know the upper bound of degrees. The difference of the attack between the masked case and the original case is that we need to check all elliptic curves of degree $\prod_{i=1}^{t} \ell_{A,i}^{e'_{A,i}}$ in the masked case, where $e'_{A,i}$ is a value in $\{0, \dots, \lfloor e_{A,i}/2 \rfloor\}$. Therefore, the number of candidates for a middle curve is about

$$\prod_{i=1}^{t} \sum_{j_i=0}^{\lfloor e_{A,i}/2 \rfloor} \ell_{A,i}^{\lfloor e_{A,i}/2 \rfloor - j_i} = \prod_{i=1}^{t} \frac{\ell_{A,i}^{\lfloor e_{A,i}/2 \rfloor + 1} - 1}{\ell_{A,i} - 1} \approx \prod_{i=1}^{t} \ell_{A,i}^{\lfloor e_{A,i}/2 \rfloor} \approx p^{\frac{1}{4}}$$

Therefore, the complexity of this attack is $\tilde{O}(p^{1/4})$ via classical computers. For quantum computers, there is a famous algorithm named Craw finding algorithm [Tan09]. By using this algorithm, the complexity is $\tilde{O}(p^{1/6})$.

Brute force approach to find the degree of the isogeny. To attack masked-degree SIDH, it is a natural approach to identify the degree of the secret isogeny because of Castryck–Decru attack. The complexity of the brute force approach relies on the size of the space of degrees, that is $\prod_{i=1}^{t} e_{A,i}$ and $\prod_{i=1}^{t} e_{B,i}$. As noted in Section 3, the Weil pairing leaks the squareness of the degree modulo $\prod_{i=1}^{t} \ell_{A,i}^{e'_{A,i}}$ or $\prod_{i=1}^{t} \ell_{B,i}^{e'_{B,i}}$. Moreover, a little bit more information of the secret key of Bob is leaked because the cardinality of $(\mathbb{Z}/2^e\mathbb{Z})^\times/((\mathbb{Z}/2^e\mathbb{Z})^\times)^2$ is 4 for $e \geq 3$, while that of $(\mathbb{Z}/\ell^e\mathbb{Z})^\times/((\mathbb{Z}/\ell^e\mathbb{Z})^\times)^2$ is 2 for an odd prime ℓ. Therefore, the Weil pairing reduces the space of secret degrees to at most $1/2^{t+1}$. Hence, the size of the space of all degrees must be about $2^{\lambda+t+1}$ in classical security (resp. $2^{2\lambda+t+1}$ in quantum security by Grover algorithm [Gro96]). We estimate the size of the prime p under this situation. We analyze the complexity in the classical world because the complexity with quantum computers is easily derived from that with classical computers. It is clear that the size of the space of degrees depends on parameters that constitute p (*i.e.*, t and $e_{A,1}, \dots, e_{A,t}, e_{B,1}, \dots, e_{B,t}$). Therefore, in this paper, we assume some properties of these parameters to make the analysis clear. First, assume that $e_{A,1} = \cdots = e_{A,t} = e_{B,1} = \cdots = e_{B,t}$, and denote this value by e_0. Second, fix $t = \lambda/2$. By Prime number theorem, the $\ell_{A,i}$'s and $\ell_{B,i}$'s are estimated to satisfy $\prod_{i=1}^{t}(\ell_{A,i}/\log \ell_{A,i}) \approx (2t)^t$ and $\prod_{i=1}^{t}(\ell_{B,i}/\log \ell_{B,i}) \approx (2t)^t$. From the assumption of the size of the space of the degrees, it holds that $(e_0+1)^t \approx 2^{\lambda+t+1}$. Therefore, we have

$$\log_2 p = e_0 \sum_{i=1}^{t} (\log_2 \ell_{A,i} + \log_2 \ell_{B,i}) \approx 2e_0 t(\log_2 t + 1) \approx 2^{\frac{\lambda}{t}+2} t(\log_2 t + 1).$$

As we suppose that $t = \lambda/2$, it holds that $\log_2 p \approx 8\lambda \log_2 \lambda$. Hence, the prime p satisfies $p \approx 2^{8\lambda \log_2 \lambda}$, and the complexity of the brute force attack on the degree of the isogeny is $\tilde{O}(p^{1/(8 \log_2 (\log_2 p))})$ via classical computers. The complexity with quantum computers is $\tilde{O}(p^{1/(16 \log_2 (\log_2 p))})$.

Castryck–Decru attack. If we know the degree of the target isogeny, Castryck–Decru attack may be able to be adapted to masked-degree SIDH. However, it seems to be hard to find the degree of the target isogeny as in the above subsection. Here, we discuss Castryck–Decru attack without information about the target degree. The important part of their attack is to construct an expected isogeny diamond configuration $(\psi' \circ \hat{\gamma}, \ker \hat{\gamma}, \hat{\gamma}(\ker \psi'))$ of order N, where N is an integer dividing the order of P_A, Q_A. This provides an expected reducible anti-isometry $\iota \colon C[N] \to E_B[N]$ that is given by P_A, Q_A and $\phi_B(P_A), \phi_B(Q_A)$, and we can compute a proper (N,N)-isogeny to check whether ι is reducible. However, if it is hard to decide the degree of ψ', then it is also hard to take integers c and N such that $N = c + \deg \psi'$ and N divides the order of P_A, Q_A. This means that it is hard to compute an expected reducible anti-isometry $\iota \colon C[N] \to E_B[N]$. Although they mentioned more flexible conditions about c and N in [CD22], we cannot adapt the attack to masked-degree SIDH because we need to know c and N. Therefore, we think the current Castryck–Decru attack cannot be adapted to masked-degree SIDH without information about the degree of the hidden isogeny.

Isogeny Problem vs Isogeny Problem with image points. In this subsection, we discuss the relationship between Isogeny Problem and Isogeny Problem with Image Points. These problems are defined as follows:

Problem 2 (Isogeny Problem). Let p be a prime, and E_1 and E_2 supersingular elliptic curves over $\mathbb{F}_{p^2}$. Compute a separable isogeny $\phi \colon E_1 \to E_2$.

Problem 3 (Isogeny Problem with Image Points). Let p be a prime, and E_1 and E_2 supersingular elliptic curves. Let N be a smooth integer such that $E_1[N] \subset E_1(\mathbb{F}_{p^2})$ and $E_2[N] \subset E_2(\mathbb{F}_{p^2})$, and let $P_1, Q_1 \in E_1[N]$ and $P_2, Q_2 \in E_2[N]$ be points such that P_i, Q_i generate $E_i[N]$ for $i = 1, 2$ and there is a separable isogeny $\phi(P_1) = P_2$ and $\phi(Q_1) = Q_2$. Compute a separable isogeny between E_1 and E_2.

Isogeny Problem with Image Points is an important problem for the security of masked-degree SIDH. It is clear that if Isogeny Problem is solved, then Isogeny Problem with Image Points is also solved. On the contrary, the following theorem holds:

Theorem 4. *Let p be a prime, and N a smooth integer such that $E[N] \subset E(\mathbb{F}_{p^2})$ for a supersingular elliptic curve E. Then Isogeny Problem is reduced to Isogeny Problem with Image Points.*

Proof. The main strategy for the reduction is as follows:

1. Generate random points $P_1, Q_1 \in E_1[N]$ and $P_2, Q_2 \in E_2[N]$ such that P_i, Q_i generate $E_i[N]$ for $i = 1, 2$.
2. Solve Isogeny Problem with Image Points for $(E_1, E_2, P_1, P_2, Q_1, Q_2)$, and get a separable isogeny between E_1 and E_2.

This strategy does not seem to work because there is no guarantee of the existence of a separable isogeny ϕ such that $\phi(P_1) = P_2$ and $\phi(Q_1) = Q_2$. Let $\phi' \colon E_1 \to E_2$ be a separable isogeny such that $\deg \phi'$ is coprime to N. Note that $\phi'(P_1)$ and $\phi'(Q_1)$ generate $E_2[N]$. The following claim guarantees the existence of a separable isogeny ϕ:

Claim. There is a separable endomorphism of E_2 such that $\phi'(P_1) \mapsto P_2$ and $\phi'(Q_1) \mapsto Q_2$.

Proof of Claim. Let $\mathcal{O}$ be an endomorphism ring of E_2. Since $\mathcal{O}$ is a maximal order of a quaternion algebra, there is a $\mathbb{Z}$-basis $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ of $\mathcal{O}$. By using a generator of $E_2[N]$, we can represent $\alpha_1|_{E_2[N]}, \ldots, \alpha_4|_{E_2[N]}$ as 2×2-matrices. Therefore, there is a $\mathbb{Z}/N\mathbb{Z}$-module homomorphism

$$\begin{array}{rccc} \varPhi\colon & (\mathbb{Z}/N\mathbb{Z})^4 & \longrightarrow & M_2(\mathbb{Z}/N\mathbb{Z}) \\ & (n_1, n_2, n_3, n_4) & \longmapsto & n_1\alpha_1|_{E_2[N]} + \cdots + n_4\alpha_4|_{E_2[N]} \end{array},$$

where $M_2(\mathbb{Z}/N\mathbb{Z})$ is the $\mathbb{Z}/N\mathbb{Z}$-module of 2×2-matrices over $\mathbb{Z}/N\mathbb{Z}$. If a point (n'_1, n'_2, n'_3, n'_4) is in the kernel of $\varPhi$, then the kernel of $n'_1\alpha_1 + \cdots + n'_4\alpha_4$ contains $E_2[N]$. Therefore, there is an endomorphism ψ with $n'_1\alpha_1 + \cdots + n'_4\alpha_4 = \psi \circ [N]$. As $\{\alpha_1, \ldots, \alpha_4\}$ is a basis, we have $N \mid n'_1, \ldots, n'_4$. This means that $n'_1, \ldots, n'_4$ are zero, and $\varPhi$ is injective. Since $\#(\mathbb{Z}/N\mathbb{Z})^4 = \#M_2(\mathbb{Z}/N\mathbb{Z}) = N^4$, the homomorphism $\varPhi$ is the isomorphism. Hence, there is an endomorphism γ such that $\gamma(\phi'(P_1)) = P_2$ and $\gamma(\phi'(Q_1)) = Q_2$. From [Sil09, Proof of Corollary 5.5], at least one of γ and $[N] + \gamma$ is separable. This completes the proof of Claim. ■

From the above claim, there is a separable isogeny ϕ such that $\phi(P_1) = P_2$ and $\phi(Q_1) = Q_2$. Therefore, Isogeny Problem can be reduced to Isogeny Problem with Image Points. □

As above discussions, Isogeny Problem with Image Points is equivalent to Isogeny Problem; however, masked-degree SIDH can be attacked in sub-exponential time. It is because we know the upper bound of the degree of the target isogeny in the setting of masked-degree SIDH.

4.2 Parameter for masked-degree SIDH

In this subsection, we discuss the size of the proper parameter of masked-degree SIDH under NIST security levels.

From Subsection 4.1, the most effective attack for masked-degree SIDH is brute force approach to find the degree of the isogeny; the complexity of this attack is $\tilde{O}(p^{1/(8\log_2(\log_2 p))})$ via classical computers and $\tilde{O}(p^{1/(16\log_2(\log_2 p))})$ via quantum computers. The size of p is about $\log_2 p \approx 2^{\frac{\lambda}{t}+2}t(\log_2 t + 1)$ in classical security. We now consider the size of t which makes the size of p as small as possible. Let $f(t) = 2^{\frac{\lambda}{t}+2}t(\log_2 t + 1)$. Considering the minimum value of $f(t)$, we get a proper t. By using computers, we have $t = 74$ for $\lambda = 128$, $t = 112$ for $\lambda = 192$, and $t = 151$ for $\lambda = 256$. Since $e_0 \approx 2^{\frac{\lambda+1}{t}+1} - 1$, we can also estimate e_0.

Under this estimation, we propose three primes: p_{6806}, p_{11191}, and p_{15747}. The prime p_{6806} is a 6806-bit prime such that

$$p_{6806} = 2^6 \cdot \ell_1^6 \cdots \ell_{142}^6 \ell_{143} \cdots \ell_{148} - 1,$$

where $\ell_1, \ldots, \ell_{147}$ are the smallest distinct odd primes, and $\ell_{148} = 4903$. The prime p_{11191} is a 11191-bit prime such that

$$p_{11191} = 2^6 \cdot \ell_1^6 \cdots \ell_{214}^6 \ell_{215} \cdots \ell_{224} - 1,$$

where $\ell_1, \ldots, \ell_{223}$ are the smallest distinct odd primes, and $\ell_{224} = 4099$. The prime p_{15747} is a 15747-bit prime such that

$$p_{15747} = 2^6 \cdot \ell_1^6 \cdots \ell_{284}^6 \ell_{285} \cdots \ell_{302} - 1,$$

where $\ell_1, \ldots, \ell_{301}$ are the smallest distinct odd primes, and $\ell_{302} = 11257$. These primes correspond to NIST security levels 1, 3, and 5, respectively. The size of the public key of masked-degree SIDH is 6 times the bit length of p. In [CJL+17], there is a method to compress the size of the public key of SIDH that can also be adapted to masked-degree SIDH. By this method, Alice's public key is in $\mathbb{F}_{p^2} \times \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/\prod_{i=1}^{t} \ell_{B,i}^{e_{B,i}}\mathbb{Z})^3$, and Bob's public key is in $\mathbb{F}_{p^2} \times \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/\prod_{i=1}^{t} \ell_{A,i}^{e_{A,i}}\mathbb{Z})^3$. We summarize the sizes of the public keys of masked-degree SIDH under these security levels in Table 1. Here, we let $2, \ell_2, \ell_4, \ldots$ be Alice's primes (*i.e.*, $\ell_{A,1}, \ldots, \ell_{A,t}$), and $\ell_1, \ell_3, \ldots$ Bob's primes (*i.e.*, $\ell_{B,1}, \ldots, \ell_{B,t}$). As shown in this table, masked-degree SIDH needs extremely huge size parameters.

Table 1. Key sizes of masked-degree SIDH in NIST security levels

λ	NIST	p	public key	compressed pk (Alice)	compressed pk (Bob)
128	level 1	6,806 bit	5,105 byte	2,984 byte	2,973 byte
192	level 3	11,191 bit	8,394 byte	4,902 byte	4,892 byte
256	level 5	15,747 bit	11,811 byte	6,896 byte	6,884 byte

5 Conclusion

In this paper, we proposed the new isogeny-based scheme, masked-degree SIDH. This is the first trial to revive SIDH that was broken by Castryck–Decru attack. The base idea to resist their attack is to cover the degree of the secret isogeny. To get rid of the information about degrees, we use many primes to compute isogenies and extend the space of the degrees of the target isogenies.

Moreover, we analyzed the security of masked-degree SIDH. By hiding the degrees, it seems hard to adapt Castryck–Decru attack to masked-degree SIDH directly. The most efficient attack for masked-degree SIDH in our analysis is the brute force approach to find the degree of the isogeny. The time complexity of this attack is $\tilde{O}(p^{1/(8\log_2(\log_2 p))})$ with classical computers and $\tilde{O}(p^{1/(16\log_2(\log_2 p))})$ with quantum computers. Although this is a sub-exponential time, the actual size of parameters of masked-degree SIDH adapted to NIST security levels is extraordinarily large (Table 1).

References

BJS14. Jean-François Biasse, David Jao, and Anirudh Sankar. A quantum algorithm for computing isogenies between supersingular elliptic curves. In *Progress in Cryptology – INDOCRYPT 2014*, pages 428–442. Springer, 2014.

CD22. Wouter Castryck and Thomas Decru. An efficient key recovery attack on SIDH (preliminary version). `https://eprint.iacr.org/2022/975`, 2022.

CJL$^+$17. Craig Costello, David Jao, Patrick Longa, Michael Naehrig, Joost Renes, and David Urbanik. Efficient compression of sidh public keys. In *Advances in Cryptology – EUROCRYPT 2017*, pages 679–706. Springer, 2017.

CLM$^+$18. Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: an efficient post-quantum commutative group action. In *Advances in Cryptology – ASIACRYPT 2018*, pages 395–427. Springer, 2018.

DG16. Christina Delfs and Steven D Galbraith. Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$. *Designs, Codes and Cryptography*, pages 425–440, 2016.

Gro96. Lov K Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 212–219, 1996.

JDF11. David Jao and Luca De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In *Post-Quantum Cryptography*, pages 19–34. Springer, 2011.

Kan97. Ernst Kani. The number of curves of genus two with elliptic differentials. *Journal für die reine und angewandte Mathematik*, 1997(485):93–122, 1997.

Pet17. Christophe Petit. Faster algorithms for isogeny problems using torsion point images. In *Advances in Cryptology – ASIACRYPT 2017*, pages 330–353. Springer, 2017.

Sho94. Peter W Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. Ieee, 1994.

Sil09. Joseph H Silverman. *The arithmetic of elliptic curves*, volume 106. Springer Science & Business Media, 2009.

Tan09. Seiichiro Tani. Claw finding algorithms using quantum walk. *Theoretical Computer Science*, 410(50):5285–5297, 2009.

Vél71. Jacques Vélu. Isogénies entre courbes elliptiques. *CR Acad. Sci. Paris Sér. A*, 273(5):238–241, 1971.