Zero-Knowledge Proofs for SIDH variants with Masked Degree or Torsion

Youcef Mokrani, David Jao

Department of Combinatorics and Optimization
University of Waterloo, Waterloo, Ontario, N2L 3G1, Canada
{ymokrani,djao}@math.uwaterloo.ca

Abstract. The polynomial attacks on SIDH by Castryck, Decru, Maino, Martindale and Robert have shown that, while the general isogeny problem is still considered unfeasible to break, it is possible to efficiently compute a secret isogeny when given its degree and image on enough torsion points.
A natural response from many researchers has been to propose SIDH variants where one or both of these possible extra pieces of information is masked in order to obtain schemes for which a polynomial attack is not currently known. Example of such schemes are M-SIDH, MD-SIDH and FESTA.
However, by themselves, theses SIDH variants are vulnerable to the same adaptive attacks where the adversary sends public keys whose associated isogeny is either unknown or inexistent. For the original SIDH scheme, one possible defense against these attacks is to use zero-knowledge proofs that a secret isogeny has been honestly computed. However, such proofs do not currently exist for most SIDH variants.
In this paper, we present new zero-knowledge proofs for isogenies whose degree or torsion points have been masked. The security of these proofs mainly relies on the hardness of DSSP.

Keywords: Elliptic curves · Supersingular isogenies · Zero-knowledge proofs

1 Introduction

Since polynomial time attacks on SIDH have been discovered [5,13,14], there have been multiple attempts in creating SIDH variants that resist the known attacks. It is important to note that these attacks only work on SIDH and not the general isogeny problem. This is because they require the extra information that is leaked by SIDH, namely its degree and its mapping for a large enough set of auxiliary points.

Therefore, the core idea behind these new variants is to mask the degree or the auxiliary points such that a shared secret can still be generated between honest parties without leaking information that can be used by an attacker to break the scheme. While these new variants are resistant to the currently known

attacks on SIDH, there are still vulnerable to adaptive attacks [10,11] where an attacker sends invalid public keys in order to gain information about a victim's secret key if a key exchange is attempted.

In the context of SIDH, one way to protect against such attacks is to have the parties prove the validity and knowledge of their secret using a Fiat-Shamir signature based on a zero-knowledge proof for their secret isogeny. However, the new masking techniques of the variants make the old zero-knowledge proofs unusable, hence the need of new proofs. In this paper, we present multiple new zero-knowledge proofs for multiple SIDH variants. The collection of proofs shown here can do any combination of the following.

- Either mask or prove the degree of the secret isogeny.
- Reveal no information about the mapping of torsion points or prove the honesty of the masked torsion point information when each torsion point is scaled by the same constant (as in M-SIDH [10]) or different ones (as in binSIDH [3] of the diagonal variant of FESTA [4]).

It is worth noting that none of the proofs in this paper require knowledge of any endomorphism rings, making compatible with schemes that require these rings to be unknown to all. For security, the zero-knowledge proofs in this paper only require the DSSP assumption as well as a computationally binding and statistically hiding commitment scheme.

In Sections 2 and 3, we present the theorems, assumptions and notations used in our protocols. The zero-knowledge proofs of this paper are presented in Sections 4, 5, 6 and 7.

1.1 Related papers

In cases where the prover has access to the endomorphism ring of the domain curve, they can prove their knowledge of an isogeny between the claimed curves using SQISign [9] or SQISignHD [6]. Since the isogeny revealed in the associated zero-knowledge proof is independent of the secret isogeny, including its degree, it stays zero-knowledge even when the degree of the secret isogeny is part of the secret. However, in the context of using it to prove honest public keys for SIDH variant, this technique cannot be used to prove that the claimed torsion point information is correct. Also, there are protocols where the endomorphism ring has to be kept unknown from all participants, in which case SQISign cannot be used.

There is already a zero-knowledge proof proposed for M-SIDH [10]. However, this proof relies on a stronger assumption than DSSP. In this paper, we present zero-knowledge proofs able to show the same properties while only needing DSSP at the cost of a slight loss in efficiency.

2 Background Knowledge and Assumptions

The security of the zero-knowledge proofs we are proposing in this paper rely on the following two theorems. The first give us an upper bound on the probability

to distinguish the codomain of a random isogeny from a random supersingular curve, while the second gives a similar bound on the probability of distinguishing the parallel isogeny in an SIDH square from a random one.

Theorem 1 ([12]). *Let p, ℓ be a prime numbers, e be a positive integer and E_0 be a supersingular elliptic curve of $\mathbb{F}_{p^2}$. Let E be the codomain of a random cyclic isogeny of degree ℓ^e and domain E_0. Let Γ be the set of supersingular elliptic curves over $\mathbb{F}_{p^2}$. For every $E' \in \Gamma$, we have that*

$$\left| \mathbb{P}(E = E') - \frac{1}{|\Gamma|} \right| \leq \left(\frac{2\sqrt{\ell}}{\ell + 1} \right)^e$$

Theorem 2 (Corollary of Theorem 11 of [2]). *Let p, ℓ be a prime numbers, A be a positive integer not divisible by ℓ, and $\phi : E_0 \to E_1$ be cyclic isogeny of degree A between two supersingular elliptic curves over $\mathbb{F}_{p^2}$.*

Let ψ be a random cyclic isogeny of degree ℓ^e and ϕ' be the isogeny parallel to ϕ in an SIDH square between ϕ and ψ.

As e grows to infinity, the domain E_2 of ϕ' converges towards a uniformly random curve in Γ and ϕ' converges towards a uniformly random cyclic isogeny of degree A and domain E_2. The convergence rate is exponential.

It is worth noting that Theorems 1 and 2 can be generalized so that we still obtain exponential convergence towards uniform distributions when ℓ^e is replaced with a positive integer B increasing to infinity. With the above results, given large enough parameter sets, we can assume that the following problem is hard.

Assumption 1 (DSSP) *Let A and B be two large, relatively prime integers. Given a cyclic isogeny $\phi : E_0 \to E_1$ of degree A, the decisional supersingular product problem is to distinguish between the following two distributions:*

1. *$\mathcal{D}_0 = \{(E_2, E_3, \phi')\}$ such that there exists a cyclic subgroup $G \subseteq E_0[B]$ of order B and $E_2 \cong E_0/G$ and $E_3 \cong E_1/\phi(G)$, and $\phi' : E_2 \to E_3$ is a degree A cyclic isogeny.*
2. *$\mathcal{D}_1 = \{(E_2, E_3, \phi')\}$ such that E_2 is a random supersingular elliptic curve with the same cardinality as E_0 and E_3 is the codomain of a random cyclic isogeny $\phi' : E_2 \to E_3$ of degree A.*

We assume that this problem is hard.

We also need to assume the existence of a function with the following security properties.

Assumption 2 ([2]) *We assume the existence of a function H which is a statistically hiding and computationally binding commitment scheme on the set of binary strings. Denote by $\mathcal{H}$ the codomain of H.*

In cases where we use H on arbitrary data, we implicitly assume that this data is encoded in the form of a binary string using a suitable encoding scheme.

3 Additional Definitions and Notations

The protocols presented in this paper use multiple functions and mathematical objects, many of these being used for more than one protocol. In order to avoid repeating these definitions every time, we present them once in this section.

Definition 1. *Given a cyclic isogeny $\phi : E \to F$,* $\textsc{GeneratingPoint}(\phi)$ *return a point K generating the kernel of ϕ. Given an elliptic curve point $K \in E$,* $\textsc{IsogenyFromKernel}(K)$ *returns an isogeny whose kernel is generated by K.*

Definition 2. *Given a supersingular elliptic curve E and a positive integer n,* $\textsc{CyclicIsogeny}(E, n)$ *returns a random cyclic isogeny whose domain is E and degree is n.*

Definition 3. *Given two isogenies $\phi : E \to E_1$ and $\psi : E \to E_2$ of relatively prime degrees,* $\textsc{ParallelIsogeny}(\phi, \psi)$ *returns the isogeny parallel to ϕ in the isogeny square generated by ϕ and ψ.*

Definition 4. *Given an elliptic curve E and a positive integer n, $E[n]$ is the subgroup formed of the points of order dividing n while $E[[n]]$ is the subset of the points of order exactly n.*

Definition 5. *Given an elliptic curve E and a positive integer n,* $\textsc{RandomBasis}(E, n)$ *returns a uniformly random basis (P, Q) of $E[n]$.*

Definition 6. *Given three elliptic curve points P, Q, R,* $\mathrm{DDLOG}(P, Q, R)$ *returns a pair of integers (e, f) such that $[e]P + [f]Q = R$. Note that we only use this function where a solution exists and is unique modulo a known integer. Also note that we only use this function in groups whose order is smooth, making the function efficient.*

Definition 7. *Given an isogeny $\phi : E \to F$,* $\textsc{Codomain}(\phi)$ *returns F.*

Definition 8. *Given a positive integer A and two integers (a, b),* $\textsc{InverPair}(a, b, A)$ *returns a pair of integers (a', b') such that $a'b - b'a$ is invertible modulo A. Note that we only use this function in cases where a valid solution exists.*

Definition 9. *Given a positive integer A, FacSet(A) is the set of positive factors of A. Given two positive integers A and B, FacSetTwo(A, B) is the set of integers d such that $A \mid D \mid B$.*

Definition 10. *Given a possibly non-cyclic isogeny ϕ, Cycliphy(ϕ) return a cyclic isogeny with the same domain and codomain. This can be easily obtained by seeing ϕ as a walk on the isogeny graph and removing the backtracking.*

Definition 11. *The function IsoValid(E, F, ϕ) returns* **true** *if ϕ is a valid isogeny from E to F and* **false** *otherwise.*

Definition 12. *In this paper, we work on elliptic curves defined over a known field $\mathbb{F}$. Also, we consider to elliptic curves with the same j-invariant to be the same. Let Γ be the set of supersingular elliptic curves defined over that field.*

Definition 13. *During the Verification step of the zero-knowledge proofs in this paper, we use* **accept** *to note that the Verifier accepts and $\perp$ to note refusal.*

4 Masking the Degree

Suppose that we want to prove knowledge of an isogeny between two supersingular elliptic curves without revealing its degree. When possible, the most efficient solution would be to use SQISign [9] or SQISignHD [6]. However, these protocols both require the prover to know the endomorphism ring of the starting curve, which limits the possible applications.

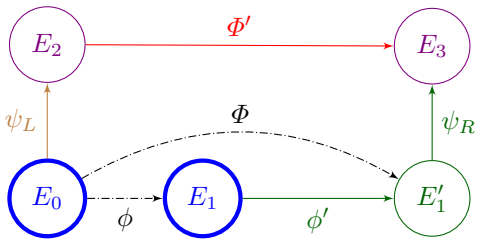
In protocols where the degree of an isogeny is part of the secret, a multiple of said degree is usually publicly known. That is the case for both MD-SIDH [10] and terSIDH [3]. In such cases, we can use rejection sampling first introduced in the context of isogenies in SeaSign [8] in order to mask the degree during a normal SIDH proof.

The core idea of MDISOZKP, when trying to prove knowledge of an isogeny $\phi : E_0 \to E_1$, is to start by computing an isogeny $\phi' : E_1 \to E_1'$ of random and potentially large degree with the same prime factors as the degree of ϕ.

We can then remove the backtracking appearing in $\phi'\phi$ in order to obtain the cyclic isogeny $\Phi : E_0 \to E_1'$. The step is necessary to make sure that the adversary does not learn anything about the secret isogeny since the degree of backtracking is a non-trivial factor of the degree of ϕ.

We can then compute an isogeny $\psi_L : E_0 \to E_2$ of degree relatively prime to Φ and compute the SIDH square between the two in order to obtain the isogenies $\Phi' : E_2 \to E_3$ and $\psi_R : E_1' \to E_3$. For the commitment, the prover can publish a hash of E_2 and E_3 and, depending on the challenge, the prover either reveals ψ_L, Φ' or $\psi_R\phi'$.

Since we use rejection sampling, in cases where the challenge asks for Φ' to be revealed, the prover needs to check that the degree respects some additional conditions. Otherwise, the proof is aborted. Later in this section, we prove that the probability of requiring an abort is low enough for a Fiat-Shamir signature to be feasible.



Definition 14 (MDISOZKP). *Let $\mathcal{A} = \prod_{i=1}^{s} q_i^{f_i}$ be a large integer such that the q_is are distinct primes dividing $p+1$. Let B be a large positive integer relatively prime to A. Let $\phi : E_0 \to E_1$ be a secret cyclic isogeny of degree $A \mid \mathcal{A}$.*

n is a positive integer representing the number of times the following proof will be repeated. The challenge is a random chall $\in \{-1, 0, 1\}$.

Commitment

$A' \leftarrow\!\$\ FacSet(\mathcal{A}^{sn})$
$\phi' \leftarrow CyclicIsogeny(E_1, A')$
$E_1' \leftarrow Codomain(\phi')$
$\Phi \leftarrow Cycliphy(\phi'\phi)$
$K_{\psi_L} \leftarrow\!\$\ E_0[[B]]$
$\psi_L \leftarrow \textsc{IsogenyFromKernel}(K_{\psi_L})$
$E_2 \leftarrow Codomain(\psi_L)$
$\Phi' \leftarrow ParallelIsogeny(\Phi, \psi_L)$
$K_{\psi_R} \leftarrow \Phi(K_{\psi_L})$
$\psi_R \leftarrow \textsc{IsogenyFromKernel}(K_{\psi_R})$
$E_3 \leftarrow Codomain(\psi_R)$
$r_2, r_3 \leftarrow\!\$\ N$
$C_2 \leftarrow H(E_2, r_2)$
$C_3 \leftarrow H(E_3, r_3)$
return (C_2, C_3)

Response

if $chall = -1$:
  return (E_2, r_2, ψ_L)
if $chall = 0$:
  return $(E_3, r_3, \psi_R\phi')$
if $chall = 1$:
  if $\deg(\Phi) \notin FacSetTwo(\mathcal{A}, \mathcal{A}^{sn})$: **abort**
  return $(E_2, E_3, r_2, r_3, \Phi')$

Verification

if $chall = -1$:
  if $C_2 \neq H(E_2, r_2)$:$\perp$
  if $\neg IsoValid(E_0, E_2, \psi_L)$:$\perp$
if $chall = 0$:
  if $C_3 \neq H(E_3, r_3)$:$\perp$
  if $\neg IsoValid(E_1, E_3, \psi_R\phi')$:$\perp$
if $chall = 1$:
  if $(C_2, C_3) \neq (H(E_2, r_2), H(E_3, r_3))$:$\perp$
  if $\neg IsoValid(E_2, E_3, \Phi')$:$\perp$
return true

Theorem 3. *Given Assumption 2, MDISOZKP is 3-special sound for the knowledge of an isogeny from E_0 to E_1.*

Proof. Since H is computationally binding, the commitments are equivalent to obtaining E_2 and E_3 directly when it comes to soundness. Given valid ψ_L, $\psi_R\phi'$ and Φ' for the same commitment (E_2, E_3), $\hat{\psi_R}\phi'\Phi'\psi_L$ is an isogeny from E_0 to E_1.

Theorem 4. *If MDISOZKP does not abort when $chall = 1$, then the degree of Φ' is a uniformly random element of $FacSetTwo(A, A^{sn})$.*

Proof. Let $d = \frac{\deg(\phi'\phi)}{\deg(\Phi)}$. For any value of d, $\frac{\deg(\phi)}{d}$ divides $\mathcal{A}$. If we fix the value of d, ϕ' can have any degree dividing $\mathcal{A}^{ns}$. We also have that the degree of ϕ' must divide $\mathcal{A}^{ns}$. Hence, since we are conditioning on the fact that MDISOZKP does not abort and chall $= 1$, for any possible degree of ϕ and value of d, there is a unique degree of ϕ' for every target degree of Φ. This makes the degree of Φ uniform, and since Φ and Φ' have the same degree, the same holds for Φ'.

Theorem 5. *Given Assumptions 1 and 2, if MDISOZKP does not abort, then it is honest verifier zero-knowledge.*

Proof. For the proof, we can create a simulator $\mathcal{S}$ for outputting a commitment-challenge-answer triple indistinguishable from that of honest parties. To do so, we describe the simulator for each possible challenge. When chall $= -1$, $\mathcal{S}$ can generate $(K_{\psi_L}, \psi_L, E_2, r_2)$ as would an honest party and generate an honest commitment C_2. Since H is statistically hiding, randomly sampling C_3 from $\mathcal{H}$ is indistinguishable from an honest computation. If chall $= 0$, $\mathcal{S}$ can generate (A', ϕ', E_1') as would an honest party. Since there is a bijection between $E_0[[B]]$ and $E_1'[[B]]$ in addition to the fact that K_{ψ_L} is never revealed, directly sampling K_{ψ_R} is indistinguishable from an honest output. Using this value, $\mathcal{S}$ can generate (ψ_R, E_3, r_3, C_3) as normal and randomly sample C_2. When chall $= -1$, $\mathcal{S}$ can sample a random $A'' \in \text{FacSetTwo}(\mathcal{A}, \mathcal{A}^{sn})$, a random supersingular elliptic curve E_2 and then a random cyclic isogeny Φ' using $\text{CyclicIsogeny}(E_2, A'')$. Given Assumption 1, This construction is indistinguishable from an honest one. $\mathcal{S}$ can then compute the other values as normal.

Theorem 6. *Given n rounds of MDISOZKP, the probability that no abort happens is at least* $\frac{1}{e}$.

Proof. For fixed ϕ and any value of $d = \frac{\deg(\phi'\phi)}{\deg(\Phi)}$, there is always at least $\prod_{i=1}^{s}(ns-2)f_i$ possible degrees of ϕ' that do not cause an abort. Hence, the probability of the protocol not aborting in a given round can be lower bounded by

$$\frac{2}{3} + \frac{1}{3}\frac{\prod_{i=1}^{s}(ns-2)f_i}{\prod_{i=1}^{s}(ns+1)f_i} = \frac{2}{3} + \frac{1}{3}\left(\frac{ns-2}{ns+1}\right)^s$$

The probability of having no abort in any round can then be lower bounded by

$$\left(\frac{2}{3} + \frac{1}{3}\left(\frac{ns-2}{ns+1}\right)^s\right)^n = \frac{1}{e} + \frac{2s-1}{2ens} + O\left(\frac{1}{n^2}\right) > \frac{1}{e}$$

5 Masked Torsion

M-SIDH [10] has been proposed as a possible fix for the attacks on SIDH [5,13,14]. The main difference being that, for a secret isogeny $\phi : E_0 \to E_1$ of degree A between two publicly known supersingular elliptic curve, M-SIDH also reveals $([\alpha]\phi(P_0), [\alpha]\phi(Q_0))$ for an unknown random α where (P_0, Q_0) is a basis of $E_0[B]$.

This protocol creates the need of being to prove knowledge of an isogeny with the above properties without leaking extra information. Basso [1] published a 3-sound zero-knowledge proof that does just that. However, that protocol relies on a stronger assumption than DSSP. A 6-sound variation only relying on DSSP is mentioned in the same paper but is dismissed for being too inefficient.

For the original SIDH protocol, De Feo et al. [7] proposed a 3-sound zero-knowledge proof that relied on the double-DSSP assumption. Such an assumption is too strong, as it can be broken by the same attacks as SIDH. However,

we can modify the protocol to only rely on the DSSP assumption at the cost of now being 4-sound. Masking the torsion can be done easily by adding a random scalar in the protocol.

The core idea of MTISOZKP consists in generating two cyclic isogenies $\psi_{L,i} : E_0 \to E_{2,i}$ of degree B whose kernel generators form a basis of $E[B]$. These isogenies can be used with ϕ to construct two SIDH squares sharing an edge. In order to not leak information by doing so, we work with the dual of the isogenies of degree B as well as random bases of $E_{2,i}$. Also, we use H in order to force the commitments to be honest without leaking information.

Definition 15 (MTISOZKP). *Let A and B be two relatively prime positive integers. Let $\phi : E_0 \to E_1$ be a secret isogeny of degree A such that $\phi(P_0) = P_1$ and $\phi(Q_0) = Q_1$ where P_0 and Q_0 are a basis of the $E_0[B]$. Let $\alpha \leftarrow\$ (\mathbb{Z}/B\mathbb{Z})^*$ be secret and $(E_0, E_1, P_0, Q_0, [\alpha]P_1, [\alpha]Q_1)$ be public. The challenge is a random $chall \in \{-1, 0, 1, 2\}$.*

Commitment

$(P'_1, Q'_1) \leftarrow ([\alpha]P_1, [\alpha]Q_1)$
$K_\phi \leftarrow \text{GeneratingPoint}(\phi)$
$(K_{\psi_{L,0}}, K_{\psi_{L,1}}) \leftarrow \text{RandomBasis}(E_0, B)$
$\beta \leftarrow\$ (\mathbb{Z}/B\mathbb{Z})^*$
$(U, V) \leftarrow \text{RandomBasis}(E_0, A)$
$(e, f) \leftarrow \text{DDLOG}(U, V, K_\phi)$
for $i \in \{0, 1\}$:
  $\psi_{L,i} \leftarrow \text{IsogenyFromKernel}(K_{\psi_{L,i}})$
  $E_{2,i} \leftarrow \text{Codomain}(\psi_{L,i})$
  $(P_{2,i}, Q_{2,i}) \leftarrow \text{RandomBasis}(E_{2,i}, B)$
  $K_{\phi_i} \leftarrow \psi_i(K_\phi)$
  $\phi_i \leftarrow \text{IsogenyFromKernel}(K_{\phi_i})$
  $\psi_{R,i} \leftarrow \text{IsogenyFromKernel}(\phi(K_{\psi_{L,i}}))$
  $E_{3,i} \leftarrow \text{Codomain}(\phi_i)$
  $(P_{3,i}, Q_{3,i}) \leftarrow ([\beta]\phi_i(P_{2,i}), [\beta]\phi_i(Q_{2,i}))$
  $K_{\hat{\psi_{L,i}}} \leftarrow \text{GeneratingPoint}(\hat{\psi_{L,i}})$
  $(c_i, d_i) \leftarrow \text{DDLOG}(P_{2,i}, Q_{2,i}, K_{\hat{\psi_{L,i}}})$
  $(c'_i, d'_i) \leftarrow \text{InverPair}(c_i, d_i, B)$
  $R_{0,i} \leftarrow \hat{\psi_{L,i}}([c'_i]P_{2,i} + [d'_i]Q_{2,i})$
  $(a_i, b_i) \leftarrow \text{DDLOG}(P_0, Q_0, R_{0,i})$
  $U'_i \leftarrow \psi_{L,i}(U)$
  $V'_i \leftarrow \psi_{L,i}(V)$
  $r_{L,i}, r_{R,i}, r_{m,i}, r_{w,i} \leftarrow\$ N$
  $C_{L,i} \leftarrow H(E_{2,i}, P_{2,i}, Q_{2,i}, r_{L,i})$
  $C_{R,i} \leftarrow H(E_{3,i}, P_{3,i}, Q_{3,i}, r_{R,i})$
  $C_{m,i} \leftarrow H(c_i, d_i, c'_i, d'_i, a_i, b_i, r_{m,i})$
  $C_{w,i} \leftarrow H(U'_i, V'_i, r_{w,i})$

Commitment (cont.)

$r_A, r_B, r_E \leftarrow\$ N$
$\gamma \leftarrow \alpha\beta^{-1}$
$C_A \leftarrow H(\gamma, r_A)$
$C_B \leftarrow H(\beta, r_B)$
$C_E \leftarrow H(e, f, r_E)$
$C_1 \leftarrow (C_{L,0}, C_{R,0}, C_{m,0}, C_{w,0})$
$C_2 \leftarrow (C_{L,1}, C_{R,1}, C_{m,1}, C_{w,1})$
$C_3 \leftarrow (C_A, C_B, C_E)$
return (C_1, C_2, C_3)

Response

$z_{L,0} \leftarrow (E_{2,0}, P_{2,0}, Q_{2,0}, r_{L_0})$
$z_{L,1} \leftarrow (E_{2,1}, P_{2,1}, Q_{2,1}, r_{L_1})$
$z_{R,0} \leftarrow (E_{3,0}, P_{3,0}, Q_{3,0}, r_{R_0})$
$z_{R,1} \leftarrow (E_{3,1}, P_{3,1}, Q_{3,1}, r_{R_1})$
$z_{w,0} \leftarrow (U'_0, V'_0, r_{w,0})$
$z_{w,1} \leftarrow (U'_1, V'_1, r_{w,1})$
$z_{m,0} \leftarrow (c_0, d_0, c_1, d_1, c'_0, d'_0, a_0, b_0, r_{m,0})$
$z_{m,1} \leftarrow (c'_1, d'_1, a_1, b_1, r_{m,1})$
if $chall = -1$:
  return $(z_{L,0}, z_{L,1}, z_{m,0}, z_{m,1}, z_{w,0}, z_{w,1})$
if $chall = 0$:
  return $(z_{R,0}, z_{R,1}, z_{m,0}, z_{m,1}, (\gamma, r_A))$
if $chall = 1$:
  return $(z_{w,0}, (e, f, r_E), z_{L,0}, z_{R,0}, (\beta, r_B))$
if $chall = 2$:
  return $(z_{w,1}, (e, f, r_E), z_{L,1}, z_{R,1}, (\beta, r_B))$

Verification

if $chall = -1$:
  for $i \in \{0,1\}$:
    if $C_{L,i} \neq H(E_{2,i}, P_{2,i}, Q_{2,i}, r_{L,i})$:$\perp$
    if $(C_{m,i}, C_{w,i}) \neq (H(c_i, d_i, c_i', d_i', a_i, b_i, r_{m,i}), H(U_i', V_i', r_{w,i}))$:$\perp$
    $K_{\hat{\psi_{L,i}}} \leftarrow [c_i]P_{2,i} + [d_i]Q_{2,i}$
    if $K_{\hat{\psi_{L,i}}} \notin E_{2,i}[[B]]$:$\perp$
    $\hat{\psi_{L,i}} \leftarrow \textsc{IsogenyFromKernel}(K_{\hat{\psi_{L,i}}})$
    $E_{0,i}' \leftarrow \textsc{Codomain}(\hat{\psi_{L,i}})$
    if $E_{0,i}' \neq E_0$:$\perp$
    $R_{0,i}' \leftarrow \hat{\psi_{L,i}}([c_i']P_{2,i} + [d']Q_{2,i})$
    if $R_{0,i}' \neq [a_i]P_0 + [b_i]Q_0$:$\perp$
    if $(\textsc{gcd}(a_0b_1 - a_1b_0, B), \textsc{gcd}(c_i'd_i - d_i'c_i, B)) \neq (1,1)$:$\perp$
  if $(\hat{\psi_{L,0}}(U_0'), \hat{\psi_{L,0}}(V_0')) \neq (\hat{\psi_{L,1}}(U_1'), \hat{\psi_{L,1}}(V_1'))$:$\perp$
if $chall = 0$:
  for $i \in \{0,1\}$:
    if $(C_{R,i}, C_A) \neq (H(E_{3,i}, P_{3,i}, Q_{3,i}, r_{R,i}), H(\gamma, r_A))$:$\perp$
    if $C_{m,i} \neq H(c_i, d_i, c_i', d_i', a_i, b_i, r_{m,i})$:$\perp$
    $K_{\hat{\psi_{R,i}}} \leftarrow [c_i]P_{3,i} + [d_i]Q_{3,i}$
    if $K_{\hat{\psi_{R,i}}} \notin E_{3,i}[[B]]$:$\perp$
    $\hat{\psi_{R,i}} \leftarrow \textsc{IsogenyFromKernel}(K_{\hat{\psi_{R,i}}})$
    $E_{1,i}' \leftarrow \textsc{Codomain}(\hat{\psi_{R,i}})$
    if $E_{1,i}' \neq E_1'$:$\perp$
    $R_{1,i}' \leftarrow \hat{\psi_{R,i}}([c_i']P_{3,i} + [d']Q_{3,i})$
    if $[\gamma]\, R_{1,i}' \neq [a_i]P_1' + [b_i]Q_1'$:$\perp$
    if $(\textsc{gcd}(a_0b_1 - a_1b_0, B), \textsc{gcd}(c_i'd_i - d_i'c_i, B)) \neq (1,1)$:$\perp$
else :
  $i \leftarrow chall - 1$:
  $K_{\Phi_i'} \leftarrow [e]U_i' + [f]V_i'$
  if $(C_{L,i}, C_{R,i}) \neq (H(E_{2,i}, P_{2,i}, Q_{2,i}, r_{L,i}), H(E_{3,i}, P_{3,i}, Q_{3,i}, r_{R,i}))$:$\perp$
  if $(C_{w,i}, C_E, C_B) \neq (H(U_i', V_i', r_{w,i}), H(e, f, r_E), H(\beta, r_B))$:$\perp$
  if $K_{\phi_i'} \notin E_{2,i}[[A]]$:$\perp$
  $\phi_i' \leftarrow \textsc{IsogenyFromKernel}(K_{\phi_i'})$
  $E_{3,i}' \leftarrow \textsc{Codomain}(\Phi_i')$
  if $(E_{3,i}', [\beta]\phi_i'(P_{2,i}), [\beta]\phi_i'(Q_{2,i})) \neq (E_{3,i}, P_{3,i}, Q_{3,i})$:$\perp$
return true

Theorem 7 (Correctness). *If the prover is honest, then the verification algorithm will always return* **true**.

Proof. If chall $= -1$, the properties checked by the verification algorithm were directly computed by the prover. Hence, this case will always be correct.

If chall $\in \{1, 2\}$, the properties checked by the verification algorithm are all respected by an honest $[\beta]\phi_{\text{chall}-1}$. Hence, this case will always be correct.

If chall $= 0$, we are working with almost the same SIDH square as in [7]. The main difference being that $(P_{3,i}, Q_{3,i})$ have an extra β factor and (P'_1, Q'_1) have an extra α factor. This is dealt by multiplying $\hat{\psi_{R,i}}$ by $[\alpha\beta^{-1}]$.

Theorem 8 (Soundness). *Given Assumption 2, MTISOZKP is 4-special sound for the knowledge of a cyclic isogeny of the claimed degree between the claimed curves with the claimed torsion point information.*

Proof. We show that for a fixed commitment, if one obtains valid answers to all 4 possible challenges, then they can compute an isogeny with the claimed properties. Since H is a computationally binding commitment scheme, we can assume that the four answers agree on the committed values.

The goal is to use the possible answers in order to compute and isogeny $\rho : E_0 \to E_1$ of degree A and an integer α such that $(P'_1, Q'_1) = ([\alpha]\rho(P_0), [\alpha]\rho(Q_0))$.

Looking at the isogeny square for each $i \in \{0, 1\}$, we are given the pair (c_i, d_i) which define the point $K_{\hat{\psi_{L,i}}} = [c_i]P_{2,i} + [d_i]Q_{2,i}$ which in turn defines the isogeny $\hat{\psi_{L,i}} : E_{2,i} \to E_0$ of degree B. We are also given $K_{\phi'_i} = [e]U'_i + [f]V'_i$ which defines an isogeny $\phi'_i : E_{2,i} \to E_{3,i}$ of degree A. We can then complete the $(\hat{\psi_{L,i}}, \phi'_i)$-isogeny square to obtain a ρ candidate of degree A that we name $\rho_i : E_0 \to E_1$.

Next, we show that ρ_0 and ρ_1 have the same kernel and are therefore equivalent. It is the case since

$$\begin{aligned}\ker(\rho_0) = \hat{\psi_{L,0}}(\ker(\phi'_0)) &= \left\langle \hat{\psi_{L,0}}([e]U'_0 + [f]V'_0) \right\rangle = \left\langle \hat{\psi_{L,1}}([e]U'_1 + [f]V'_1) \right\rangle \\ &= \hat{\psi_{L,1}}(\ker(\phi'_1)) = \ker(\rho_1)\end{aligned}$$

We also have an α candidate in $\gamma\beta$. All that remains is to show that $\rho = \rho_0 = \rho_1$ has the correct torsion point images.

Recall that we are given pairs (a_i, b_i) such that $R_{0,i} = [a_i]P_0 + [b_i]Q_0$ and the matrix $M := \begin{pmatrix} a_0 & b_0 \\ a_1 & b_1 \end{pmatrix}$ is invertible.

Hence, $\{R_{0,0}, R_{0,1}\}$ is a basis of $E_0[B]$.

Also recall that $R_{0,i} = \hat{\psi_{L,i}}([c'_i]P_{2,i} + [d'_i]Q_{2,i})$, $R_{1,i} = \hat{\psi_{R,i}}([c'_i]P_{3,i} + [d'_i]Q_{3,i})$ and $(P_{3,i}, Q_{3,i}) = ([\beta]\phi_i(P_{2,i}), [\beta]\phi_i(Q_{2,i}))$. Since $\rho\hat{\psi_{L,i}} = \hat{\psi_{R,i}}\phi_i$, we have that $\rho(R_{0,i}) = [\beta^{-1}]R_{1,i}$. Hence:

$$\begin{aligned}&\begin{pmatrix} R_{0,0} \\ R_{0,1} \end{pmatrix} = M \begin{pmatrix} P_0 \\ Q_0 \end{pmatrix} \implies \begin{pmatrix} \rho(R_{0,0}) \\ \rho(R_{0,1}) \end{pmatrix} = M \begin{pmatrix} \rho(P_0) \\ \rho(Q_0) \end{pmatrix} \\ \implies &\begin{pmatrix} [\beta^{-1}]R_{1,0} \\ [\beta^{-1}]R_{1,1} \end{pmatrix} = M \begin{pmatrix} \rho(P_0) \\ \rho(Q_0) \end{pmatrix} \implies M^{-1} \begin{pmatrix} [\beta^{-1}]R_{1,0} \\ [\beta^{-1}]R_{1,1} \end{pmatrix} = \begin{pmatrix} \rho(P_0) \\ \rho(Q_0) \end{pmatrix} \\ \implies &\begin{pmatrix} [\gamma^{-1}\beta^{-1}]P'_1 \\ [\gamma^{-1}\beta^{-1}]Q'_1 \end{pmatrix} = \begin{pmatrix} \rho(P_0) \\ \rho(Q_0) \end{pmatrix} \implies \begin{pmatrix} P'_1 \\ Q'_1 \end{pmatrix} = \begin{pmatrix} [\beta\gamma]\rho(P_0) \\ [\beta\gamma]\rho(Q_0) \end{pmatrix}\end{aligned}$$

and this completes the proof.

Theorem 9 (Zero-knowledge). *Given Assumptions 1 and 2, MTISOZKP is zero-knowledge.*

Proof. We prove it by showing a simulator $\mathcal{S}$ outputting valid a commitment-challenge-answer tuple with the same distribution as an honest prover for each possible challenge.

When the challenge is -1, value that is published without being masked by H can be computed honestly. $C_{R,0}$, $C_{R,1}$, C_A, and C_B can be randomly sampled from $\mathcal{H}$ while being indistinguishable from an honest output by Assumption 2.

When the challenge is 0, the simulator can use the homomorphism property of isogenies to work on the right side of the SIDH squares instead of the left. The masked values can once again be sampled randomly.

When the challenge is 1 or 2, the simulator can sample a random ϕ_i and β and compute the rest using these values. The masked values are, again, sampled randomly. Distinguishing this simulator from an honest output is equivalent to solving the DSSP, which we assume to be hard.

6 Double Masked Subgroup

Instead of multiplying both torsion points images by the same constant, binSIDH, terSIDH [3] and the diagonal variant of FESTA [4] multiply each point by independent random scalars. This has the consequence of making MTISOZKP hard to adapt in this case, as the correctness of the previous protocol relies on the fact that the isogeny multiplying every point by the same constant commutes with every isogeny. Needing to multiply each basis point by a different scalar looses this commutative property, which means that we must look elsewhere for a zero-knowledge proof.

DMSISOZKP is a zero-knowledge proving that a party known an isogeny $\phi : E_0 \to E_1$ such that $([\alpha_P]\phi(P_0), [\alpha_Q]\phi(Q_0)) = (P_1, Q_1)$ for some unknown values of α_P and α_Q. Similarly to MTISOZKP, DMSISOZKP consist of building an SIDH square and using dual isogenies and hashed commitments to maintain zero-knowledge and soundness. The main difference being that, in DMSISOZKP, the generated isogenies are of degree C and the random basis is of order BC. This is so that we can prove information on the B torsion. While only requiring Assumptions 2 and 1 for its security, DMSISOZKP requires some additional conditions on the field for it to be efficient. We need a field such that isogenies of degree C can be efficiently computed while, at the same time, points of order BC can be efficiently be computed and used in other computations. In practice, this requires the chosen prime to be about 50% larger, as isogenies of degree C must also be hard to attack.

Definition 16 (DMSISOZKP). *Let A, B and C be two relatively prime positive integers. Let $\phi : E_0 \to E_1$ be a secret isogeny of degree A such that $(\phi(P_0), \phi(Q_0)) = (P_1, Q_1)$ where (P_1, Q_1) form a basis of $E_0[B]$. Let $\alpha_P, \alpha_Q \leftarrow\!\!\$\ (\mathbb{Z}/(BC)\mathbb{Z})^*$ be secret and $(E_0, E_1, P_0, Q_0, [\alpha_P]P_1, [\alpha_Q]Q_1)$ be public. The challenge is a random chall $\in \{-1, 0, 1\}$.*

Commitment

$(P'_1, Q'_1) \leftarrow ([\alpha_P]P_1, [\alpha_Q]Q_1)$
$K_\phi \leftarrow \text{GeneratingPoint}(\phi)$
$K_{\psi_L} \leftarrow\!\!\$\ E[[C]]$
$K_{\psi_R} \leftarrow \phi(K_{\psi_L})$
$\psi_L \leftarrow IsogenyFromKernel(K_{\psi_L})$
$\psi_R \leftarrow IsogenyFromKernel(K_{\psi_R})$
$E_2 \leftarrow Codomain(\psi_L)$
$E_3 \leftarrow Codomain(\psi_R)$
$(P_{2,P}, Q_{2,P}) \leftarrow RandomBasis(E_2, BC)$
$(P_{2,Q}, Q_{2,Q}) \leftarrow RandomBasis(E_2, BC)$
$\beta_P, \beta_Q \leftarrow\!\!\$\ (\mathbb{Z}/(BC)\mathbb{Z})^*$
$K_{\phi'} \leftarrow \psi_L(K_\phi)$
$\phi' \leftarrow IsogenyFromKernel(K_{\phi'})$
$(P_{3,P}, Q_{3,P}) \leftarrow ([\beta_P]\phi'(P_{2,P}), [\beta_P]\phi'(Q_{2,P}))$
$(P_{3,Q}, Q_{3,Q}) \leftarrow ([\beta_Q]\phi'(P_{2,Q}), [\beta_Q]\phi'(Q_{2,Q}))$
$K_{\hat{\psi_L}} \leftarrow GeneratingPoint(\hat{\psi_L})$
$(c, d) \leftarrow DDLOG(P_{2,P}, Q_{2,P}, K_{\hat{\psi_L}})$
$(a_P, b_P) \leftarrow DDLOG(\hat{\psi_L}(P_{2,P}), \hat{\psi_L}(Q_{2,P}), P_0)$
$(a_Q, b_Q) \leftarrow DDLOG(\hat{\psi_L}(P_{2,Q}), \hat{\psi_L}(Q_{2,Q}), Q_0)$
$\gamma_P \leftarrow \alpha_P \beta_P^{-1}$
$\gamma_Q \leftarrow \alpha_Q \beta_Q^{-1}$
$r_L, r_R, r_m, r_A, r_B \leftarrow\!\!\$\ N$
$C_L \leftarrow H(E_2, P_{2,P}, Q_{2,P}, P_{2,Q}, Q_{2,Q}, r_L)$
$C_R \leftarrow H(E_3, P_{3,P}, Q_{3,P}, P_{3,Q}, Q_{3,Q}, r_R)$
$C_m \leftarrow H(a_P, b_P, a_Q, b_Q, c, d, r_m)$
$C_A \leftarrow H(\gamma_P, \gamma_Q, r_A)$
$C_B \leftarrow H(\beta_P, \beta_Q, r_B)$
return $(C_L, C_R, C_m, C_A, C_B)$

Response

$z_L \leftarrow (E_2, P_{2,P}, Q_{2,P}, P_{2,Q}, Q_{2,Q}, r_L)$
$z_R \leftarrow (E_3, P_{3,P}, Q_{3,P}, P_{3,Q}, Q_{3,Q}, r_R)$
$z_m \leftarrow (a_P, b_P, a_Q, b_Q, c, d, r_m)$
if $chall = -1$:
  return (z_L, z_m)
if $chall = 0$:
  return $(z_R, z_m, \gamma_P, \gamma_Q, r_A)$
if $chall = 1$:
  return $(z_L, z_R, \beta_P, \beta_Q, r_B, K_{\phi'})$

Verification

if $chall = -1$:
  if $C_L \neq H(E_2, P_{2,P}, Q_{2,P}, P_{2,Q}, Q_{2,Q}, r_L)$:$\perp$
  if $C_m \neq H(a_P, b_P, a_Q, b_Q, c, d, r_m)$:$\perp$
  if $\neg IsBasis(P_{2,P}, Q_{2,P}, E_2, BC)$:$\perp$
  if $\neg IsBasis(P_{2,Q}, Q_{2,Q}, E_2, BC)$:$\perp$
  $K_{\hat{\psi_L}} \leftarrow [c]P_{2,P} + [d]Q_{2,P}$
  if $K_{\hat{\psi_L}} \notin E_2[[C]]$:$\perp$
  $\hat{\psi_L} \leftarrow IsogenyFromKernel(K_{\hat{\psi_L}})$
  $E'_0 \leftarrow Codomain(\hat{\psi_L})$
  if $E'_0 \neq E_0$:$\perp$
  if $P_0 \neq [a_P]\hat{\psi_L}(P_{2,P}) + [b_P]\hat{\psi_L}(Q_{2,P})$:$\perp$
  if $Q_0 \neq [a_Q]\hat{\psi_L}(P_{2,Q}) + [b_Q]\hat{\psi_L}(Q_{2,Q})$:$\perp$
if $chall = 0$:
  if $C_R \neq H(E_3, P_{3,P}, Q_{3,P}, P_{3,Q}, Q_{3,Q}, r_R)$:$\perp$
  if $C_m \neq H(a_P, b_P, a_Q, b_Q, c, d, r_m)$:$\perp$
  if $C_A \neq H(\gamma_P, \gamma_Q, r_A)$:$\perp$
  if $\neg IsBasis(P_{3,P}, Q_{3,P}, E_3, BC)$:$\perp$
  if $\neg IsBasis(P_{3,Q}, Q_{3,Q}, E_3, BC)$:$\perp$
  $K_{\hat{\psi_R}} \leftarrow [c]P_{3,P} + [d]Q_{3,P}$
  if $K_{\hat{\psi_R}} \notin E_3[[C]]$:$\perp$
  $\hat{\psi_R} \leftarrow IsogenyFromKernel(K_{\hat{\psi_R}})$
  $E'_1 \leftarrow Codomain(\hat{\psi_R})$
  if $E'_1 \neq E_1$:$\perp$
  if $P'_1 \neq [a_P\gamma_P]\hat{\psi_R}(P_{3,P}) + [b_P\gamma_P]\hat{\psi_R}(Q_{3,P})$:$\perp$
  if $Q'_1 \neq [a_Q\gamma_Q]\hat{\psi_R}(P_{3,Q}) + [b_Q\gamma_Q]\hat{\psi_R}(Q_{3,Q})$:$\perp$
if $chall = 1$:
  if $C_L \neq H(E_2, P_{2,P}, Q_{2,P}, P_{2,Q}, Q_{2,Q}, r_L)$:$\perp$
  if $C_R \neq H(E_3, P_{3,P}, Q_{3,P}, P_{3,Q}, Q_{3,Q}, r_R)$:$\perp$
  if $C_B \neq H(\beta_P, \beta_Q, r_B)$:$\perp$
  if $K_{\phi'} \notin E_2[[A]]$:$\perp$
  $\phi' \leftarrow IsogenyFromKernel(K_{\phi'})$
  $E'_3 \leftarrow Codomain(\phi')$
  if $E'_3 \neq E_3$:$\perp$
  if $P_{3,P} \neq [\beta_P]\phi'(P_{2,P})$:$\perp$
  if $Q_{3,P} \neq [\beta_P]\phi'(Q_{2,P})$:$\perp$
  if $P_{3,Q} \neq [\beta_Q]\phi'(P_{2,Q})$:$\perp$
  if $Q_{3,Q} \neq [\beta_Q]\phi'(Q_{2,Q})$:$\perp$
accept

Theorem 10 (Correctness). *If the prover is honest, then the verification algorithm will always return* **true**.

Proof. If chall $= -1$, the properties checked by the verification algorithm were directly computed by the prover. Hence, this case will always be correct.

If chall = 1, the properties checked by the verification algorithm are all respected by honest $[\beta_P]\phi'$ and $[\beta_Q]\phi'$. Hence, this case will always be correct.

If chall = 0, we have that $\hat{\psi_R}\phi' = \phi\hat{\psi_L}$ since the four isogenies form an SIDH square. Hence:

$$\begin{aligned}
P'_1 &= [\alpha_P]\phi(P_0) \\
&= [\alpha_P]\phi([a_P]\hat{\psi_L}(P_{2,P}) + [b_P]\hat{\psi_L}(Q_{2,P})) \\
&= [a_P\alpha_P]\phi\hat{\psi_L}(P_{2,P}) + [b_P\alpha_P]\phi\hat{\psi_L}(Q_{2,P}) \\
&= [a_P\alpha_P]\hat{\psi_R}\phi'(P_{2,P}) + [b_P\alpha_P]\hat{\psi_R}\phi'(Q_{2,P}) \\
&= [a_P\gamma_P]\hat{\psi_R}(P_{3,P}) + [b_P\gamma_P]\hat{\psi_R}(Q_{3,P})
\end{aligned}$$

which is the checked equation. The same argument holds for $Q'_1 = [a_Q\gamma_Q]\hat{\psi_R}(P_{3,Q}) + [b_Q\gamma_Q]\hat{\psi_R}(Q_{3,Q})$.

Theorem 11 (Zero-knowledge). *Given Assumptions 2 and 1, DMSISOZKP is zero-knowledge.*

Proof. We prove it by showing a simulator outputting valid a commitment-challenge-answer tuple with the same distribution as an honest prover for each possible challenge.

When the challenge is -1, the simulator can compute the revealed values honestly and sample random values for the masked data, which is indistinguishable from random by Assumption 2.

When the challenge is 0, the simulator can use the homomorphism property of isogenies to work on the right side of the SIDH squares instead of the left. The masked values can one again be sampled randomly.

When the challenge is 1, the simulator can sample a random ϕ' and (β_P, β_Q) and compute the rest using these values. The masked values are, again, sampled randomly. Distinguishing this simulator from an honest output is equivalent to solving the DSSP, which we assume to be hard.

Theorem 12 (Soundness). *Given Assumption 2, DMSISOZKP is 3-special sound for the knowledge of a cyclic isogeny of the claimed degree between the claimed curves with the claimed torsion point information.*

Proof. We show that for a fixed commitment, if one obtains valid answers to all 3 possible challenges, then they can compute an isogeny with the claimed properties.

Since H is a computationally binding commitment scheme, we can assume that the three answers agree on the committed values.

The goal is to use the possible answers in order to compute and isogeny $\rho : E_0 \to E_1$ of degree A and a pair of integers (α_P, α_P) such that $(P'_1, Q'_1) = ([\alpha_P]\rho(P_0), [\alpha_Q]\rho(Q_0))$.

We are given the pair (c, d) which define the point $K_{\hat{\psi_L}}$, which in turn defines the isogeny $\hat{\psi_L} : E_2 \to E_0$ of degree C. We are also given the point $K_{\phi'}$ which

defines the isogeny $\phi' : E_2 \to E_3$. We can then complete the $(\hat{\psi_L}, \phi')$-isogeny square to obtain our ρ candidate.

We also have a (α_P, α_Q) candidate in $(\gamma_P\beta_P, \gamma_Q\beta_Q)$.

We have that $\rho : E_0 \to E_1$ is of degree A, so we only need to check that it respects the claimed mapping. Since ρ is constructed by completing an SIDH square, we have that $\rho\hat{\psi_L} = \hat{\psi_R}\phi'$. Hence:

$$\begin{aligned}
\rho(P_0) &= \rho([a_P]\hat{\psi_L}(P_{2,P}) + [b_P]\hat{\psi_L}(Q_{2,P})) \\
&= [a_P]\rho\hat{\psi_L}(P_{2,P}) + [b_P]\rho\hat{\psi_L}(Q_{2,P}) \\
&= [a_P]\hat{\psi_R}\phi'(P_{2,P}) + [b_P]\hat{\psi_R}\phi'(Q_{2,P}) \\
\rho(P_0) &= [\beta_P^{-1}\gamma_P^{-1}]P_1' \\
[\alpha_P]\rho(P_0) &= P_1'
\end{aligned}$$

The same arguments holds for $[\alpha_Q]\rho(Q_0) = Q_1'$. Therefore, ρ is a valid secret isogeny and this completes the proof.

7 Masked Degree and Double Subgroup

Section 4's technique used to prove knowledge of an isogeny while masking its degree can be combined with any of zero-knowledge proof in this paper in order to prove the desired torsion point information. Since the combination method and security proofs of every case are almost identical, we only explicitly present one of them in this paper.

For applications such as terSIDH [3], we require a zero-knowledge proof that that can prove knowledge of an isogeny with the given subgroup images without leaking information about either the isogeny itself or its degree. In order to do this, we start DMSISOZKP and add the random sampling technique presented in MDISOZKP.

Definition 17 (MDTISOZKP).

Let $\mathcal{A} = \prod_{i=1}^{s} q_i^{f_i}$ be a large integer such that the q_is are distinct primes dividing $p+1$. Let B and C be large positive integers relatively prime to $\mathcal{A}$. Let $\phi : E_0 \to E_1$ be a secret cyclic isogeny of degree $A \mid \mathcal{A}$ such that $(\phi(P_0), \phi(Q_0)) = (P_1, Q_1)$ where (P_1, Q_1) form a basis of $E_0[B]$. Let $\alpha_P, \alpha_Q \leftarrow\$ (\mathbb{Z}/(BC)\mathbb{Z})^*$ be secret and $(E_0, E_1, P_0, Q_0, [\alpha_P]P_1, [\alpha_Q]Q_1)$ be public.

Let $(P_1', Q_1') := ([\alpha_P]P_1, [\alpha_Q]Q_1)$ and let n be a positive integer representing the number of times the following proof will be repeated. The challenge is a random chall $\in \{-1, 0, 1\}$.

Commitment

$A' \leftarrow\!\$\ FacSet(\mathcal{A}^{sn})$
$\phi' \leftarrow CyclicIsogeny(E_1, A')$
$E'_1 \leftarrow Codomain(\phi')$
$\Phi \leftarrow Cycliphy(\phi'\phi)$
$A'' \leftarrow \deg(\Phi)$
$\xi \leftarrow A''/(A \times A')$
$K_{\psi_L} \leftarrow\!\$\ E[[C]]$
$K_{\psi_R} \leftarrow \Phi(K_{\psi_L})$
$\psi_L \leftarrow IsogenyFromKernel(K_{\psi_L})$
$\psi_R \leftarrow IsogenyFromKernel(K_{\psi_R})$
$E_2 \leftarrow Codomain(\psi_L)$
$E_3 \leftarrow Codomain(\psi_R)$
$(P_{2,P}, Q_{2,P}) \leftarrow RandomBasis(E_2, BC)$
$(P_{2,Q}, Q_{2,Q}) \leftarrow RandomBasis(E_2, BC)$
$\beta_P, \beta_Q \leftarrow\!\$\ (\mathbb{Z}/(BC)\mathbb{Z})^*$
$\Phi' \leftarrow ParallelIsogeny(\Phi, \psi_L)$
$(P_{3,P}, Q_{3,P}) \leftarrow ([\beta_P]\Phi'(P_{2,P}), [\beta_P]\Phi'(Q_{2,P}))$
$(P_{3,Q}, Q_{3,Q}) \leftarrow ([\beta_Q]\Phi'(P_{2,Q}), [\beta_Q]\Phi'(Q_{2,Q}))$
$K_{\hat{\psi_L}} \leftarrow GeneratingPoint(\hat{\psi_L})$
$(c, d) \leftarrow DDLOG(P_{2,P}, Q_{2,P}, K_{\hat{\psi_L}})$
$(a_P, b_P) \leftarrow DDLOG(\hat{\psi_L}(P_{2,P}), \hat{\psi_L}(Q_{2,P}), P_0)$
$(a_Q, b_Q) \leftarrow DDLOG(\hat{\psi_L}(P_{2,Q}), \hat{\psi_L}(Q_{2,Q}), Q_0)$
$\gamma_P \leftarrow \alpha_P \beta_P^{-1} \xi^{-1}$
$\gamma_Q \leftarrow \alpha_Q \beta_Q^{-1} \xi^{-1}$
$r_L, r_R, r_m, r_A, r_B \leftarrow\!\$\ N$
$C_L \leftarrow H(E_2, P_{2,P}, Q_{2,P}, P_{2,Q}, Q_{2,Q}, r_L)$
$C_R \leftarrow H(E_3, P_{3,P}, Q_{3,P}, P_{3,Q}, Q_{3,Q}, r_R)$
$C_m \leftarrow H(a_P, b_P, a_Q, b_Q, c, d, r_m)$
$C_A \leftarrow H(\gamma_P, \gamma_Q, r_A)$
$C_B \leftarrow H(\beta_P, \beta_Q, r_B)$
return $(C_L, C_R, C_m, C_A, C_B)$

Verification

if $chall = -1$:
  if $C_L \neq H(E_2, P_{2,P}, Q_{2,P}, P_{2,Q}, Q_{2,Q}, r_L)$:$\perp$
  if $C_m \neq H(a_P, b_P, a_Q, b_Q, c, d, r_m)$:$\perp$
  if $\neg IsBasis(P_{2,P}, Q_{2,P}, E_2, BC)$:$\perp$
  if $\neg IsBasis(P_{2,Q}, Q_{2,Q}, E_2, BC)$:$\perp$
  $K_{\hat{\psi_L}} \leftarrow [c]P_{2,P} + [d]Q_{2,P}$
  if $K_{\hat{\psi_L}} \notin E_2[[C]]$:$\perp$
  $\hat{\psi_L} \leftarrow IsogenyFromKernel(K_{\hat{\psi_L}})$
  $E'_0 \leftarrow Codomain(\hat{\psi_L})$
  if $E'_0 \neq E_0$:$\perp$
  if $P_0 \neq [a_P]\hat{\psi_L}(P_{2,P}) + [b_P]\hat{\psi_L}(Q_{2,P})$:$\perp$
  if $Q_0 \neq [a_Q]\hat{\psi_L}(P_{2,Q}) + [b_Q]\hat{\psi_L}(Q_{2,Q})$:$\perp$
if $chall = 0$:
  if $C_R \neq H(E_3, P_{3,P}, Q_{3,P}, P_{3,Q}, Q_{3,Q}, r_R)$:$\perp$
  if $C_m \neq H(a_P, b_P, a_Q, b_Q, c, d, r_m)$:$\perp$
  if $C_A \neq H(\gamma_P, \gamma_Q, r_A)$:$\perp$
  if $\neg IsBasis(P_{3,P}, Q_{3,P}, E_3, BC)$:$\perp$
  if $\neg IsBasis(P_{3,Q}, Q_{3,Q}, E_3, BC)$:$\perp$
  $K_{\hat{\psi_R}} \leftarrow [c]P_{3,P} + [d]Q_{3,P}$
  if $K_{\hat{\psi_R}} \notin E_3[[C]]$:$\perp$
  $\hat{\psi_R} \leftarrow IsogenyFromKernel(K_{\hat{\psi_R}})$
  $E'_1 \leftarrow Codomain(\hat{\psi_R})$
  if $\neg IsoValid(E_1, E'_1, \phi')$:$\perp$
  if $\deg(\phi') \nmid \mathcal{A}^{sn}$:$\perp$
  if $\phi'(P'_1) \neq [a_P\gamma_P]\hat{\psi_R}(P_{3,P}) + [b_P\gamma_P]\hat{\psi_R}(Q_{3,P})$:$\perp$
  if $\phi'(Q'_1) \neq [a_Q\gamma_Q]\hat{\psi_R}(P_{3,Q}) + [b_Q\gamma_Q]\hat{\psi_R}(Q_{3,Q})$:$\perp$
if $chall = 1$:
  if $C_L \neq H(E_2, P_{2,P}, Q_{2,P}, P_{2,Q}, Q_{2,Q}, r_L)$:$\perp$
  if $C_R \neq H(E_3, P_{3,P}, Q_{3,P}, P_{3,Q}, Q_{3,Q}, r_R)$:$\perp$
  if $C_B \neq H(\beta_P, \beta_Q, r_B)$:$\perp$
  if $\neg IsoValid(E_2, E_3, \Phi')$:$\perp$
  if $\deg(\Phi') \notin FacSetTwo(\mathcal{A}, \mathcal{A}^{sn})$:$\perp$
  if $(P_{3,P}, Q_{3,P}) \neq ([\beta_P]\phi'(P_{2,P}), [\beta_P]\phi'(Q_{2,P}))$:$\perp$
  if $(P_{3,Q}, Q_{3,Q}) \neq ([\beta_Q]\phi'(P_{2,Q}), [\beta_Q]\phi'(Q_{2,Q}))$:$\perp$
return true

Response

if $chall = -1$:
  return $(E_2, P_{2,P}, Q_{2,P}, P_{2,Q}, Q_{2,Q}, r_L, a_P, b_P, a_Q, b_Q, c, d, r_m)$
if $chall = 0$:
  return $(E_3, P_{3,P}, Q_{3,P}, P_{3,Q}, Q_{3,Q}, r_R, a_P, b_P, a_Q, b_Q, c, d, r_m, \gamma_P, \gamma_Q, r_A, \phi')$
if $chall = 1$:
  if $A'' \notin FacSetTwo(\mathcal{A}, \mathcal{A}^{sn})$: **abort**
  return $(E_2, P_{2,P}, Q_{2,P}, P_{2,Q}, Q_{2,Q}, r_L, E_3, P_{3,P}, Q_{3,P}, P_{3,Q}, Q_{3,Q}, r_R, \beta_P, \beta_Q, r_B, \Phi')$

Theorem 13 (Correctness). *If the prover is honest and does not abort, then the verification algorithm will always return* **true**.

Proof. If chall $= -1$, the properties checked by the verification algorithm were directly computed by the prover. Hence, this case will always be correct.

If chall $= 1$, the properties checked by the verification algorithm are all respected by honest $[\beta_P]\Phi'$ and $[\beta_Q]\Phi'$. Hence, this case will always be correct.

If chall $= 0$, we have that $\hat{\psi_R}\Phi' = \Phi\hat{\psi_L}$ since the four isogenies form an SIDH square. We also have that $\phi\phi' = [\xi]\Phi$. Hence:

$$\begin{aligned}
\phi'(P'_1) &= [\alpha_P]\phi\phi'(P_0) \\
&= [\alpha_P\xi]\Phi(P_0) \\
&= [\alpha_P\xi]\Phi([a_P]\hat{\psi_L}(P_{2,P}) + [b_P]\hat{\psi_L}(Q_{2,P})) \\
&= [a_P\alpha_P\xi]\Phi\hat{\psi_L}(P_{2,P}) + [b_P\alpha_P\xi]\Phi\hat{\psi_L}(Q_{2,P}) \\
&= [a_P\alpha_P\xi]\hat{\psi_R}\Phi'(P_{2,P}) + [b_P\alpha_P\xi]\hat{\psi_R}\Phi'(Q_{2,P}) \\
&= [a_P\gamma_P]\hat{\psi_R}(P_{3,P}) + [b_P\gamma_P]\hat{\psi_R}(Q_{3,P})
\end{aligned}$$

which is the checked equation. The same argument hold for $\phi'(Q'_1) = [a_Q\gamma_Q]\hat{\psi_R}(P_{3,Q}) + [b_Q\gamma_Q]\hat{\psi_R}(Q_{3,Q})$.

Before proving the security of MDTISOZKP, it is important to remark that Theorems 4 and 6 also hold for MDTISOZKP as the proof is identical. Hence, the probability of the scheme not aborting during n rounds is at least $\frac{1}{e}$.

Theorem 14 (Zero-knowledge). *Given Assumptions 2 and 1, if MDTISOZKP does not abort, then it is zero-knowledge.*

Proof. We prove it by showing a simulator outputting valid a commitment-challenge-answer tuple with the same distribution as an honest prover for each possible challenge.

When the challenge is -1, the simulator can compute the revealed values honestly and sample random values for the masked data, which is indistinguishable from an honest output by Assumption 2.

When the challenge is 0, the simulator can compute ϕ' honestly. Then, we can use the homomorphism property of isogenies to work on the right side of the SIDH squares instead of the left. The masked values can one again be sampled randomly.

When the challenge is 1, the simulator can sample a random Φ' and (β_P, β_Q) and compute the rest using these values. The masked values are, again, sampled randomly. The degree of Φ' is indistinguishable by Theorem 4. Hence, distinguishing this simulator from an honest output is equivalent to solving the DSSP, which we assume to be hard.

Theorem 15 (Soundness). *Given Assumption 2, MDTISOZKP is 3-special sound for the knowledge of a cyclic isogeny between the claimed curves with the claimed torsion point information.*

Proof. We show that for a fixed commitment, if one obtains valid answers to all 3 possible challenges, then they can compute an isogeny with the claimed properties.

Since H is a computationally binding commitment scheme, we can assume that the three answers agree on the committed values.

We are given an isogeny $\phi' : E_1 \to E_1'$ of degree A'. Let $P_1'' = \phi'(P_1')$ and $Q_1'' = \phi'(Q_1')$. Given an isogeny $\Phi : E_0 \to E_1'$ such that $\Phi(P_0) = [\delta_P]P_1''$ and $\Phi(Q_0) = [\delta_Q]Q_1''$, $\hat{\phi'}\Phi$ is a valid extractor.

Therefore, the goal is to use the possible answers in order to compute and isogeny $\rho : E_0 \to E_1'$ of degree A'' and a pair of integers (δ_P, δ_P) such that $(P_1'', Q_1'') = ([\delta_P]\rho(P_0), [\delta_Q]\rho(Q_0))$.

We are given the pair (c, d) which define the point $K_{\hat{\psi_L}}$, which in turn defines the isogeny $\hat{\psi_L} : E_2 \to E_0$ of degree C. We are also an the isogeny $\Phi' : E_2 \to E_3$ of degree A''. We can then complete the $(\hat{\psi_L}, \Phi')$-isogeny square to obtain our ρ candidate.

We also have a (δ_P, δ_Q) candidate in $(\gamma_P\beta_P, \gamma_Q\beta_Q)$.

We have that $\rho : E_0 \to E_1'$ is of degree A'', so we only need to check that it respects the claimed mapping. Since ρ is constructed by completing an SIDH square, we have that $\rho\hat{\psi_L} = \hat{\psi_R}\Phi'$. Hence:

$$\begin{aligned}
\rho(P_0) &= \rho([a_P]\hat{\psi_L}(P_{2,P}) + [b_P]\hat{\psi_L}(Q_{2,P})) \\
&= [a_P]\rho\hat{\psi_L}(P_{2,P}) + [b_P]\rho\hat{\psi_L}(Q_{2,P}) \\
&= [a_P]\hat{\psi_R}\Phi'(P_{2,P}) + [b_P]\hat{\psi_R}\Phi'(Q_{2,P}) \\
&= [a_P\beta_P^{-1}]\hat{\psi_R}P_{4,P} + [b_P\beta_P^{-1}]\hat{\psi_R}Q_{3,P} \\
\rho(P_0) &= [\beta_P^{-1}\gamma_P^{-1}]P_1'' \\
[\delta_P]\rho(P_0) &= P_1''
\end{aligned}$$

The same arguments hold for $[\delta_Q]\rho(Q_0) = Q_1''$. Therefore, ρ can be used to generate a valid secret isogeny and this completes the proof.

8 Conclusion

Using the schemes in this paper, we can prove knowledge of isogenies with masked torsion-point information while either proving the degree or masking it, as desired.

The fact that the security of our scheme relies mainly on DSSP allows us to obtain statistical zero-knowledge using large enough parameters as a consequence of Theorems 1 and 2.

For further research, it is worth mentioning that some variants of FESTA use non-diagonal matrices to masked their torsion point information. In those cases, the schemes in this paper do not apply. However, the technique in DMSISOZKP can probably be generalized for non-diagonal, but abelian families of matrices.

9 Acknowledgments

This preprint has not undergone peer review or any post-submission improvements or corrections. The Version of Record of this contribution is published in Security, Privacy, and Applied Cryptography Engineering, and is available online at https://doi.org/10.1007/978-3-031-51583-5_3

This research was supported by NSERC Alliance Consortia Quantum Grant ALLRP 578463–2022.

References

1. Basso, A.: A post-quantum round-optimal oblivious PRF from isogenies. Cryptology ePrint Archive, Paper 2023/225 (2023), https://eprint.iacr.org/2023/225
2. Basso, A., Codogni, G., Connolly, D., De Feo, L., Fouotsa, T.B., Lido, G.M., Morrison, T., Panny, L., Patranabis, S., Wesolowski, B.: Supersingular curves you can trust. In: Hazay, C., Stam, M. (eds.) Advances in Cryptology – EUROCRYPT 2023. pp. 405–437. Springer Nature Switzerland, Cham (2023)
3. Basso, A., Fouotsa, T.B.: New SIDH countermeasures for a more efficient key exchange. Cryptology ePrint Archive, Paper 2023/791 (2023), https://eprint.iacr.org/2023/791
4. Basso, A., Maino, L., Pope, G.: FESTA: Fast encryption from supersingular torsion attacks. Cryptology ePrint Archive, Paper 2023/660 (2023), https://eprint.iacr.org/2023/660
5. Castryck, W., Decru, T.: An efficient key recovery attack on SIDH. In: Hazay, C., Stam, M. (eds.) Advances in Cryptology – EUROCRYPT 2023. pp. 423–447. Springer Nature Switzerland, Cham (2023)
6. Dartois, P., Leroux, A., Robert, D., Wesolowski, B.: SQISignHD: New dimensions in cryptography. Cryptology ePrint Archive, Paper 2023/436 (2023), https://eprint.iacr.org/2023/436
7. De Feo, L., Dobson, S., Galbraith, S.D., Zobernig, L.: SIDH proof of knowledge. In: Advances in Cryptology – ASIACRYPT 2022: 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5–9, 2022, Proceedings, Part II. p. 310–339. Springer-Verlag, Berlin, Heidelberg (2023). https://doi.org/10.1007/978-3-031-22966-4˙11
8. De Feo, L., Galbraith, S.D.: Seasign: Compact isogeny signatures from class group actions. In: Ishai, Y., Rijmen, V. (eds.) Advances in Cryptology – EUROCRYPT 2019. pp. 759–789. Springer International Publishing, Cham (2019)
9. De Feo, L., Kohel, D., Leroux, A., Petit, C., Wesolowski, B.: Sqisign: Compact post-quantum signatures from quaternions and isogenies. In: Moriai, S., Wang, H. (eds.) Advances in Cryptology – ASIACRYPT 2020. pp. 64–93. Springer International Publishing, Cham (2020)
10. Fouotsa, T.B., Moriya, T., Petit, C.: M-SIDH and MD-SIDH: countering sidh attacks by masking information. Cryptology ePrint Archive, Paper 2023/013 (2023), https://eprint.iacr.org/2023/013
11. Galbraith, S.D., Petit, C., Shani, B., Ti, Y.B.: On the security of supersingular isogeny cryptosystems. In: Cheon, J.H., Takagi, T. (eds.) Advances in Cryptology – ASIACRYPT 2016. pp. 63–91. Springer Berlin Heidelberg, Berlin, Heidelberg (2016)

12. Galbraith, S.D., Petit, C., Silva, J.: Identification protocols and signature schemes based on supersingular isogeny problems. J. Cryptol. **33**(1), 130–175 (jan 2020)
13. Maino, L., Martindale, C.: An attack on SIDH with arbitrary starting curve. Cryptology ePrint Archive, Paper 2022/1026 (2022), https://eprint.iacr.org/2022/1026
14. Robert, D.: Breaking SIDH in polynomial time. In: Hazay, C., Stam, M. (eds.) Advances in Cryptology – EUROCRYPT 2023. pp. 472–503. Springer Nature Switzerland, Cham (2023)