A New Isogeny-Based Signature Scheme Using Degree Challenges

Kohei Nakagawa[1,a)] Ryo Yoshizumi[2,b)]

Abstract: Isogeny-based cryptography is cryptographic schemes whose security is based on the hardness of a mathematical problem called the isogeny problem, and is attracting attention as one of the candidates for post-quantum cryptography. A representative isogeny-based cryptography is the signature scheme called SQIsign, which was submitted to the NIST PQC standardization competition. In this paper, we introduce a new isogeny-based signature scheme, which represents a significant departure from existing isogeny-based signatures such as SQIsign. The key distinction in our proposed scheme lies in its use of the degree of isogeny as a challenge within the underlying Σ-protocol. Then, the prover outputs an isogeny of the given degree as a response. While PRISM, another signature scheme, also employs degrees as challenges, it diverges from our approach by not being based on the hardness of endomorphism ring problem, which is well-known problem in the field of isogeny-based cryptography. In this paper, we describe the algorithm, security analysis, and efficiency of our protocol.

Keywords: Post-Quantum Cryptography, Isogeny-based Signature, SQIsign

1. Introduction

With the progression of quantum computing, a considerable threat is posed to traditional public-key cryptographic schemes like RSA and elliptic curve cryptography. In response, the area of *post-quantum cryptography* (PQC) has developed, focusing on cryptography that remains secure even in the presence of quantum adversaries. To address the pressing need for standardized PQC, the National Institute of Standards and Technology (NIST) initiated a multi-phase competition to evaluate and select PQC candidates for standardization.

Within the various categories of PQC, *isogeny-based cryptography* has attracted attention because of its compact data sizes. One of the representative isogeny-based cryptography is the signature scheme called SQIsign [11], which was submitted to the NIST PQC standardization competition for additional signature [8]. Although SIKE [16] was also representative isogeny-based cryptography, several attacks on SIKE [7], [19], [24] were reported in 2022. These attacks show that any isogeny can be efficiently recovered from its evaluation on sufficiently large torsion subgroup by computing high-dimensional isogenies.

Recently, a lot of cryptography using high-dimensional isogenies have been studied: encryption schemes such as FESTA [6], QFESTA [20], and POKÉ [5], and variants of SQIsign such as SQIsignHD [9], SQIsign2D-West [4], SQIsign2D-East [21], and SQIPrime [14]. In particular, SQIsign2D-West has been adopted as the SQIsign specification in Round 2 of the NIST competition [1].

1.1 Contributions

In this paper, we present a novel signature scheme using high-dimensional isogeny which represents a significant departure from existing isogeny-based signatures such as SQIsign. The key distinction in our proposed scheme lies in its use of the degree of isogeny as a challenge within the underlying Σ-protocol. Then, the prover outputs an isogeny of the given degree as a response. While PRISM [3], another signature scheme, also employs degrees as challenges, it diverges from our approach by not being based on the hardness of endomorphism ring problem, which is well-known problem in the field of isogeny-based cryptography.

2. Preliminaries

In this section, we give some notations and background knowledge used in this paper.

2.1 Notations

For integers a, b, n, we denote the set of all integers x satisfying $a < x < b$ and $\gcd(x, q) = 1$ by $(a, b)_n$. For an odd prime N and an integer M, $\left(\frac{M}{N}\right)$ denotes the Legendre symbol.

2.2 Quaternion Algebras.

A *quaternion algebra* over $\mathbb{Q}$ is a division algebra defined by $\mathbb{Q} + \mathbb{Q}\mathbf{i} + \mathbb{Q}\mathbf{j} + \mathbb{Q}\mathbf{k}$ and $\mathbf{i}^2 = a, \mathbf{j}^2 = b, \mathbf{ij} = -\mathbf{ji} = \mathbf{k}$ for

[1] NTT Social Informatics Laboratories
[2] Kyushu University
[a)] kohei.nakagawa@ntt.com
[b)] yoshizumi.ryo.483@s.kyushu-u.ac.jp

$a, b \in \mathbb{Q}^*$. We denote it by $H(a,b)$. We say $H(a,b)$ is *ramified* at a place v of $\mathbb{Q}$ if $H(a,b) \otimes_{\mathbb{Q}} \mathbb{Q}_v$ is not isomorphic to the algebra of the 2×2 matrices over $\mathbb{Q}_v$. There exists a quaternion algebra ramified exactly at p and ∞. Such an algebra is unique up to isomorphism. We denote it by $\mathcal{B}_{p,\infty}$.

Let $\alpha = x + y\mathbf{i} + z\mathbf{j} + t\mathbf{k} \in H(a,b)$ with $x, y, z, t \in \mathbb{Q}$. The *conjugate* of α is $x - y\mathbf{i} - z\mathbf{j} - t\mathbf{k}$ and denoted by $\bar{\alpha}$. The *reduced norm* of α is $\alpha\bar{\alpha}$ and denoted by $n(\alpha)$.

An *order* $\mathcal{O}$ of $H(a,b)$ is a subring of $H(a,b)$ that is also a $\mathbb{Z}$-lattice of rank 4. This means that $\mathcal{O} = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \mathbb{Z}\alpha_3 + \mathbb{Z}\alpha_4$ for a basis $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ of $H(a,b)$. We denote such an order by $\mathbb{Z}\langle\alpha_1, \alpha_2, \alpha_3, \alpha_4\rangle$. An order $\mathcal{O}$ is said to be *maximal* if there is no larger order that contains $\mathcal{O}$.

For a maximal order $\mathcal{O}$, an (integral) *left $\mathcal{O}$-ideal* I is a $\mathbb{Z}$-lattice of rank 4 satisfying $I \subset \mathcal{O}$ and $\mathcal{O} \cdot I \subset I$. A *right $\mathcal{O}$-ideal* is similarly defined. For an ideal I, we denote its conjugate by $\bar{I} = \{\bar{\alpha} \mid \alpha \in I\}$. We denote by $n(I)$ the *reduced norm* of the ideal I, defined as (the unique positive generator of) the $\mathbb{Z}$-module generated by the reduced norms of the elements of I. A left $\mathcal{O}$-ideal I of integer norm can be written as $I = \mathcal{O}\alpha + \mathcal{O}n(I)$ for some $\alpha \in I$. We denote such I by $I = \mathcal{O}\langle\alpha, n(I)\rangle$. The *ideal equivalence* denoted by $I \sim J$ means that there exists $\beta \in \mathcal{B}^*_{p,\infty}$ such that $I = J\beta$.

2.3 Deuring Correspondence.

Deuring [13] showed that the endomorphism ring of a supersingular elliptic curve over $\mathbb{F}_{p^2}$ is isomorphic to a maximal order of $\mathcal{B}_{p,\infty}$ and gave a correspondence (the *Deuring correspondence*) where a supersingular elliptic E curve over $\mathbb{F}_{p^2}$ corresponds to a maximal order isomorphic to $\mathrm{End}(E)$.

Suppose $p \equiv 3 \pmod 4$. This is the setting we use in our protocol. Then we can take $\mathcal{B}_{p,\infty} = H(-1,-p)$ and an elliptic curve over $\mathbb{F}_{p^2}$ with j-invariant 1728 is supersingular. Let E_0 be the elliptic curve over $\mathbb{F}_{p^2}$ defined by $y^2 = x^3 + x$. Then $j(E_0) = 1728$, so E_0 is supersingular. We define endomorphisms $\iota : (x,y) \mapsto (-x, \sqrt{-1}y)$ and $\pi : (x,y) \mapsto (x^p, y^p)$ of E_0, where $\sqrt{-1}$ is a fixed square root of -1 in $\mathbb{F}_{p^2}$. The endomorphism ring of E_0 is isomorphic to $\mathcal{O}_0 \coloneqq \mathbb{Z}\langle 1, \mathbf{i}, \frac{\mathbf{i}+\mathbf{j}}{2}, \frac{1+\mathbf{k}}{2}\rangle$. This isomorphism is given by $\iota \mapsto \mathbf{i}$ and $\pi \mapsto \mathbf{j}$. From now on, we identify $\mathrm{End}(E_0)$ with $\mathcal{O}_0$ by this isomorphism.

Some isogeny-based protocols, e.g., SQISign [11], need to compute the image under an element in $\mathcal{O}_0$ represented by the coefficients with respect to the basis $(1, \mathbf{i}, \frac{\mathbf{i}+\mathbf{j}}{2}, \frac{1+\mathbf{k}}{2})$. Let $P \in E_0(\mathbb{F}_{p^2})$ and $\alpha = x + y\mathbf{i} + z\frac{\mathbf{i}+\mathbf{j}}{2} + t\frac{1+\mathbf{k}}{2}$ for $x, y, z, t \in \mathbb{Z}$. Given P and x, y, z, t, one can compute $\alpha(P)$ in $O(\log \max\{|x|, |y|, |z|, |t|\})$ operations on $\mathbb{F}_{p^2}$ and $O(\log p)$ operations on $\mathbb{F}_{p^4}$. The latter operations in $\mathbb{F}_{p^4}$ are necessary only for the case when the order of P is even. We need to compute $\alpha(P_0)$ and $\alpha(Q_0)$ for a fixed basis P_0, Q_0 of $E_0[2^a]$ for some integer a in our protocol. In this case, by precomputing the images of P_0 and Q_0 under $\mathbf{i}$, $\frac{\mathbf{i}+\mathbf{j}}{2}$, and $\frac{1+\mathbf{k}}{2}$, we can compute $\alpha(P_0)$ and $\alpha(Q_0)$ by scalar multiplications by x, y, z, t and additions.

The Deuring correspondence also gives a correspondence between isogenies and ideals. Let E_1 be a supersingular elliptic curve over $\mathbb{F}_{p^2}$ and let $\mathcal{O}_1$ be a maximal order of $\mathcal{B}_{p,\infty}$ such that $\mathcal{O}_1 \cong \mathrm{End}(E_1)$. Let $\phi : E_1 \to E_2$ be an N-isogeny, then the isogeny ϕ can be associated to a left $\mathcal{O}_1$-ideal I_ϕ. This ideal I_ϕ is also a right $\mathcal{O}_2$-ideal for a maximal order $\mathcal{O}_2$ satisfying $\mathcal{O}_2 \cong \mathrm{End}(E_2)$. Such an ideal I_ϕ is called a *connecting ideal* from $\mathcal{O}_1$ to $\mathcal{O}_2$. Furthermore, it is known that its norm $n(I_\phi)$ is equal to the degree N of ϕ. The order $\mathfrak{O}$ denoted by $\mathfrak{O} = \mathcal{O}_1 \cap \mathcal{O}_2$ is called the *Eichler order* and $\mathfrak{O} = \mathbb{Z} + I_\phi$ holds. Moreover, two isogenies $\phi, \psi : E_1 \to E_2$ that have the same domain and codomain correspond to equivalent ideals $I_\phi \sim I_\psi$.

2.4 On the Use of 2-Dimensional Isogenies

Since the attack on SIDH using 2-dimensional isogenies [7], [19], [24], there have been widespread efforts to incorporate 2-dimensional isogenies into the design of isogeny-based cryptography. In this section, we explain the use of 2-dimensional isogenies.

First, we introduce an important lemma known as Kani's lemma [17], which is used in the attack on SIDH.

Lemma 1. *([19], Theorem 1) Let d_1 and d_2 be coprime integers and let $D = d_1 + d_2$. Let E, E_1, E_2, and F be elliptic curves connected by the following commutative diagram of isogenies:*

$$\begin{array}{ccc} E & \xrightarrow{\varphi_1} & E_1 \\ {\scriptstyle\varphi_2}\downarrow & & \downarrow{\scriptstyle\varphi_2'} \\ E_2 & \xrightarrow[\varphi_1']{} & F, \end{array}$$

where $\deg(\varphi_i) = \deg(\varphi_i') = d_i$ for $i \in \{1,2\}$. Then, the map

$$\Phi = \begin{pmatrix} \varphi_1 & -\widehat{\varphi_2'} \\ \varphi_2 & \widehat{\varphi_1'} \end{pmatrix} : E \times F \to E_1 \times E_2 \qquad (1)$$

is a (D,D)-isogeny with respect to the natural product polarizations on $E_1 \times E_2$ and $E \times F$, and has kernel $\{([d_2]P, \varphi_2' \circ \varphi_1(P)) \mid P \in E[D]\}$. Conversely, a (D,D)-isogeny with this kernel is equal to Φ up to isomorphism.

From this lemma, we can evaluate $\hat{\varphi}_1$ and $\widehat{\varphi_2'}$ by computing a (D,D)-isogeny Φ with kernel $\{([d_2]P, \varphi_2' \circ \varphi_1(P)) \mid P \in E_1[D]\}$. Especially when $D = 2^e$ for a positive integer e, we can compute the (D,D)-isogeny with kernel G by the recent formulas proposed by Dartois, Maino, Pope, and Robert [10].

2.5 Existing Subroutines

In our construction, we use some existing algorithms, such as `FullRepresentInteger` [12], `StrongApproxi-`

mation [18], [23], and ShortIdealToIsogenyIQO [22]. In this subsection, we introduce these algorithms briefly. Here, E_0 and $\mathcal{O}_0$ are as defined in Section 2.3. For integers a, b, let (P_0, Q_0) be a basis of $E_0[2^{a+b}]$.

• $\texttt{FullRepresentInteger}_{\mathcal{O}_0}(M) \to \alpha$

Input: An integer $M > p$.

Output: $\alpha \in \mathcal{O}_0$ such that $n(\alpha) = M$.

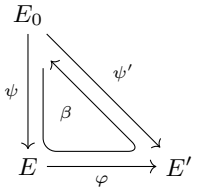
• $\texttt{StrongApproximation}_M(N, C_0, D_0) \to \mu$

Input: A prime number N and integers M, C_0, D_0 satisfying $\left(\frac{M}{N}\right) = \left(\frac{p(C_0^2+D_0^2)}{N}\right)$ and $M > pN^3$.

Output: $\mu \in \mathcal{O}_0$ such that $n(\mu) = M$ and $\mu = m(C_0\mathbf{j} + D_0\mathbf{k}) + N\mu_1$, where $m \in \mathbb{Z}$ and $\mu_1 \in \mathcal{O}_0$.

• $\texttt{ShortIdealToIsogenyIQO}\ (q, E, \psi(P_0), \psi(Q_0), L) \to (q', E', \psi'(P_0), \psi'(Q_0), K_\varphi, \beta)$

For an odd integer q, let $\psi : E_0 \to E$ be a q-isogeny and $\varphi : E \to E'$ be a 2^b-isogeny. Let left-$\mathcal{O}_0$ ideal L be the corresponding ideal to $\varphi \circ \psi$. Then, let $\psi' : E_0 \to E'$ be an isogeny of an odd degree q', and $\beta = \hat{\psi}' \circ \varphi \circ \psi \in \mathcal{O}_0$.



In this notation, ShortIdealToIsogenyIQO is the following algorithm:

Input: $q, E, \psi(P_0), \psi(Q_0), L$.

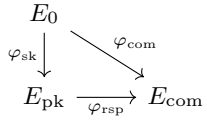
Output: $q', E', \psi'(P_0), \psi'(Q_0), \beta \in \mathcal{O}_0$, and a generator $K_\varphi \in E$ of $\operatorname{Ker}\varphi$.

This algorithm requires the computation of a $(2^a, 2^a)$-isogeny.

Remark 1. *The original* ShortIdealToIsogenyIQO *algorithm is applicable under more general conditions; see* [22].

3. Our New Signature Scheme

In this section, we introduce our signature scheme. Our signature is constructed by applying the Fiat-Shamir transform on a Σ-protocol based on the following diagram.



In this diagram, $(E_{\mathrm{pk}}, \varphi_{\mathrm{sk}})$ is a key pair and E_{com} is a commitment. Against a challenge $d_{\mathrm{chl}} \in \mathbb{Z}$, the prover computes an isogeny $\varphi_{\mathrm{rsp}} : E_{\mathrm{pk}} \to E_{\mathrm{com}}$ of degree $2^{e_1} d_{\mathrm{chl}}(2^{e_2} - d_{\mathrm{chl}})$ for an integer e_1, e_2.

First, in Section 3.1, we give a building block used to compute the response isogeny φ_{rsp}. Second, in Section 3.2, we describe our Σ-protocol.

3.1 Random Pushable Endomorphism

In this subsection, we introduce a new algorithm *Random Pushable Endomorphism* (Algorithm 1), used in our protocol. For the validity of the algorithm, we first show a lemma (Lemma 2) regrading endomorphisms.

Lemma 2. *Let N, M be coprime integers. Let $\alpha_1, \alpha_2 \in \mathcal{O}_0$ be elements satisfying that $\operatorname{nrd}(I_1) = \operatorname{nrd}(I_2) = N$ where $I_i = \langle \alpha_i, N \rangle$ for $i = 1, 2$. We write the corresponding isogenies $\varphi_{I_i} : E_0 \to E_i$ to the ideal I_i.*

Then, for $\alpha \in \mathcal{O}_0$ of the reduced norm M, the following conditions are equivalent:

(i) There exists $\psi : E_1 \to E_2$ such that the following diagram is commutative:

$$\begin{array}{ccc} E_0 & \xrightarrow{\alpha} & E_0 \\ {\scriptstyle \varphi_{I_1}}\downarrow & & \downarrow{\scriptstyle \varphi_{I_2}} \\ E_1 & \xrightarrow[\psi]{} & E_2 \end{array}.$$

(ii) $\alpha_2 \alpha \overline{\alpha_1} \in N\mathcal{O}_0$.

Proof. (i) is equivalent to $\operatorname{Ker}(\varphi_{I_2} \circ \alpha) \supset \operatorname{Ker}(\varphi_{I_1})$. Since the composition $\varphi_{I_2} \circ \alpha$ corresponded to $I_2\alpha$, (i) is equivalent to $I_2\alpha \subset I_1$. Since $I_1 = \langle \alpha_1, N \rangle$ and $I_2 = \langle \alpha_2, N \rangle$, (i) is equivalent to $\alpha_2\alpha \in \langle \alpha_1, N \rangle$ and $N\alpha \in \langle \alpha_1, N \rangle$. Since $N\alpha \in \langle \alpha_1, N \rangle$ always holds, (i) is equivalent to $\alpha_2\alpha \in \langle \alpha_1, N \rangle$. Since $N = \operatorname{nrd}(I_1) = \gcd(n(\alpha_1), n(N))$, we have $n(\alpha_1) = mN$ for $m \in \mathbb{Z}$ such that $\gcd(m, N) = 1$. Thus, we can write $sm + tN = 1$ for $s, t \in \mathbb{Z}$.

We assume (i), and we write $\alpha_2\alpha = \beta_1\alpha_1 + N\beta_2$ for $\beta_1, \beta_2 \in \mathcal{O}_0$, we have $\alpha_2\alpha\overline{\alpha_1} = n(\alpha_1)\beta_1 + N\beta_2\overline{\alpha_1} = N(m\beta_1 + \beta_2\overline{\alpha_1}) \in N\mathcal{O}_0$. Hence, we have (ii). Conversely, we assume (ii), and we write $\alpha_2\alpha\overline{\alpha_1} = N\beta$ for $\beta \in \mathcal{O}_0$, we have $n(\alpha_1)\alpha_2\alpha = N\beta\alpha_1$. By a simple calculation, we have $\alpha_2\alpha = s\beta_1\alpha_1 + Nt\alpha_2\alpha \in \langle \alpha_1, N \rangle$, which is (i). □

Remark 2. *Lemma 2 clearly holds for any supersingular elliptic curve E and a maximal order $\mathcal{O}$ ($\cong \operatorname{End}(E)$) not only for E_0 and $\mathcal{O}_0$.*

Thus, to compute $\alpha \in \mathcal{O}_0$ satisfying condition (i), we construct $\alpha \in \mathcal{O}_0$ by satisfying condition (ii). Since the reduced norm of α is M, we use $\texttt{StrongApproximation}_M(N, C_0, D_0)$ for appropriate $C_0, D_0 \in \mathbb{Z}$. Hence, we need to impose a condition $M > pN^3$. Thus, we obtain $\alpha = m(C_0\ \mathbf{j} + D_0\ \mathbf{k}) + N\mu_1$ of reduced norm M for some $m \in \mathbb{Z}$ and $\mu_1 \in \mathcal{O}_0$. Then, $\alpha_2\alpha\overline{\alpha_1} = m(C_0(\alpha_2\ \mathbf{j}\ \overline{\alpha_1}) + D_0(\alpha_2\ \mathbf{k}\ \overline{\alpha_1})) + N\alpha_2\mu_1\overline{\alpha_1}$. Thus, (ii) is equivalent to

$$C_0(\alpha_2\ \mathbf{j}\ \overline{\alpha_1}) + D_0(\alpha_2\ \mathbf{k}\ \overline{\alpha_1}) \equiv 0 \pmod{N\mathcal{O}_0}. \quad (2)$$

Note that since $\gcd(N, M) = 1$, we have $\gcd(m, N) = 1$. Hence, by solving (2), we have the desired α. In addition, to apply $\texttt{StrongApproximation}$, $\left(\frac{M}{N}\right) = \left(\frac{p(C_0^2+D_0^2)}{N}\right)$ has to be satisfied. If it does not hold, by dividing M by 2 (thus, we assume $2|M$ in advance), the required condition holds. In this case, the reduced norm of α is also

halved. Since $(C_0 : D_0) \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ is uniquely determined, the randomness of this algorithm is the same as one of `StrongApproximation`. Algorithm 1 describes this procedure.

Algorithm 1 `RnadPushEnd`$(M, N, \alpha_1, \alpha_2)$

Require: M, N, α_1, α_2 such that M is even, $\gcd(M, N) = 1$, $M > pN^3$, and $\mathrm{nrd}(\langle \alpha_1, N\rangle) = \mathrm{nrd}(\langle \alpha_2, N\rangle) = N$.
Ensure: $\alpha \in \mathcal{O}_0$ of reduced norm M or $\frac{M}{2}$ such that $\alpha_2 \alpha \overline{\alpha_1} \in N\mathcal{O}_0$.
Compute $(C_0 : D_0) \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ such that $C_0(\alpha_2 \ \mathbf{j} \ \overline{\alpha_1}) + D_0(\alpha_2 \ \mathbf{k} \ \overline{\alpha_1}) \equiv 0 \pmod{N\mathcal{O}_0}$.
if $\left(\frac{M}{N}\right) = \left(\frac{p(C_0^2+D_0^2)}{N}\right)$ **then**
  M, `is_M_halved` $:= M$, `False`.
else
  M, `is_M_halved` $:= \frac{M}{2}$, `True`.
end if
$\alpha := \texttt{StrongApproximation}_M(N, C_0, D_0)$.
return α, M, `is_M_halved`.

3.2 Underlying Σ-Protocol

In this subsection, we introduce the proposed protocol which is constructed by applying the Fiat-Shamir transform [15] on a Σ-protocol.

3.2.1 Parameter setting.

For the security parameter λ, let a, b be positive integers such that $a \approx b \approx \lambda$ and $b < a$. Let $p = 2^{a+b}f - 1$ be a prime number for some small integer f. Here, E_0 and $\mathcal{O}_0$ are as defined in Section 2.3. Let (P_0, Q_0) be a basis of $E_0[2^{a+b}]$ that is $\mathbb{F}_{p^2}$-rational. We write

$$P_0^a := 2^b P_0,\ Q_0^a := 2^b Q_0,\quad P_0^b := 2^a P_0,\ Q_0^b := 2^a Q_0.$$

Note that (P_0^a, Q_0^a) is a basis of $E_0[2^a]$, and (P_0^b, Q_0^b) is a basis of $E_0[2^b]$. In addition, let $N < 2^b$ be an odd prime number satisfying $N \equiv 3 \pmod 8$ or $N \equiv 5 \pmod 8$.

3.2.2 Key generation.

In the key generation step, we construct a random N-isogeny with the domain as E_0; $\varphi_{\mathrm{sk}} : E_0 \to E_{\mathrm{pk}}$. However, since it is *not* satisfied $N > p$, we cannot use `RandIsogImg` [20] directly. Hence, we deal with this problem by adding a 2^a-isogeny at the codomain as follows:

(1) Compute $\alpha_{\mathrm{sk}} \in \mathcal{O}_0$ of reduced norm $N(2^b - N)2^a$ $(> p)$ by `FullRepresentInteger`.

(2) Decompose α_{sk} to three isogenies:

$$E_0 \xrightarrow{\varphi_{\mathrm{sk}}} E_{\mathrm{pk}} \xrightarrow{\rho} F \xrightarrow{\psi} E_0$$

such that $\deg(\varphi_{\mathrm{sk}}) = N, \deg(\rho) = 2^b - N$, and $\deg(\psi) = 2^a$.

(3) Since $\mathrm{Ker}(\hat{\psi}) = \mathrm{Ker}(\hat{\alpha_{\mathrm{sk}}})[2^a]$, we can compute $\hat{\psi}$ and F. Thus, we compute $\hat{\psi}(\alpha_{\mathrm{sk}}(P_0)) = \rho(\varphi_{\mathrm{sk}}(P_0^b)), \hat{\psi}(\alpha_{\mathrm{sk}}(Q_0)) = \rho(\varphi_{\mathrm{sk}}(Q_0^b)) \in F$.

(4) Compute $P_{\mathrm{pk}} := \varphi_{\mathrm{sk}}(P_0), Q_{\mathrm{pk}} := \varphi_{\mathrm{sk}}(Q_0) \in E_{\mathrm{pk}}$ by `KaniCod`.

(5) Compute a left-$\mathcal{O}_0$ ideal $I_{\mathrm{sk}} := \langle \alpha_{\mathrm{sk}}, N\rangle$ corresponding to φ_{sk}.

Then, the verifier treats E_{pk} as the public key and $(P_{\mathrm{pk}}, Q_{\mathrm{pk}}, \alpha_{\mathrm{sk}}, I_{\mathrm{sk}})$ as the secret key. An Algorithm 2 describes the key generation.

Algorithm 2 `KeyGen`

Require: `param` $= (p, a, b, N, E_0, \mathcal{O}_0)$.
Ensure: `pk` $= E_{\mathrm{pk}}$, `sk` $= (P_{\mathrm{pk}}, Q_{\mathrm{pk}}, \alpha_{\mathrm{sk}}, I_{\mathrm{sk}})$
1: $\alpha_{\mathrm{sk}} := \texttt{FullRepresentInteger}_{\mathcal{O}_0}(N(2^b - N)2^a)$.
2: Compute $\alpha_{\mathrm{sk}}(P_0), \alpha_{\mathrm{sk}}(Q_0) \in E_0$.
3: Compute a basis $K_{\hat{\psi}}$ of $\mathrm{Ker}(\hat{\alpha_{\mathrm{sk}}}) \cap E_0[2^a]$.
4: Compute $\hat{\psi}(\alpha_{\mathrm{sk}}(P_0)), \hat{\psi}(\alpha_{\mathrm{sk}}(Q_0)) \in F$ under $\hat{\psi} : E_0 \to F = E_0/K_{\hat{\psi}}$.
5: $\_, E_{\mathrm{pk}}; (P_{\mathrm{pk}}, Q_{\mathrm{pk}}), \emptyset := \texttt{KaniCod}(N, 2^b - N, E_0, F, P_0^b, Q_0^b, \hat{\psi}(\alpha_{\mathrm{sk}}(P_0)), \hat{\psi}(\alpha_{\mathrm{sk}}(Q_0)); (P_0, Q_0), \emptyset)$.
6: $I_{\mathrm{sk}} := \langle \alpha_{\mathrm{sk}}, N\rangle$.
7: **return** `pk` $= E_{\mathrm{pk}}$, `sk` $= (P_{\mathrm{pk}}, Q_{\mathrm{pk}}, \alpha_{\mathrm{sk}}, I_{\mathrm{sk}})$.

3.2.3 Commitment.

The commitment is the same as the key generation explained above. Namely, the prover computes N-isogeny $\varphi_{\mathrm{com}} : E_0 \to E_{\mathrm{com}}$ and returns `com` $= E_{\mathrm{com}}$, `sec` $= (P_{\mathrm{com}}, Q_{\mathrm{com}}, \alpha_{\mathrm{com}}, I_{\mathrm{com}})$.

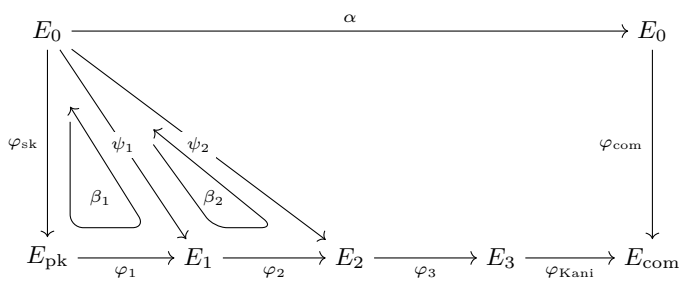
3.2.4 Challenge.

During the challenge phase, the verifier samples an odd integer $d_{\mathrm{chl}} \in (2^{a-2}, 2^{a-1})_2$ uniformly at random and returns `chl` $= d_{\mathrm{chl}}$.

3.2.5 Response.

First, the prover compute $\alpha, M,$ `is_M_halved` $=$ `RandPushEnd`$(2^{3b}d_{\mathrm{chl}}(2^a - d_{\mathrm{chl}}), N, \alpha_{\mathrm{sk}}, \alpha_{\mathrm{com}})$. Then, if `is_M_halved` is `False`, $\deg(\alpha) = 2^{3b}d_{\mathrm{chl}}(2^a - d_{\mathrm{chl}})$, otherwise, $\deg(\alpha) = 2^{3b-1}d_{\mathrm{chl}}(2^a - d_{\mathrm{chl}})$. Then, we push α through the secret key $\varphi_{\mathrm{sk}} : E_0 \to E_{\mathrm{pk}}$. Note that since $p \approx 2^{a+b}$, $b < a$, and $N < 2^b$, the condition $2^{3b}d_{\mathrm{chl}}(2^a - d_{\mathrm{chl}}) > pN^3$ is satisfied.

During the response phase, the prover utilizes the following diagram:



In the above diagram, the horizontal composition below $\varphi_{\mathrm{Kani}} \circ \varphi_3 \circ \varphi_2 \circ \varphi_1$ is the pushout of α through φ_{sk} such that $\deg(\varphi_1) = \deg(\varphi_2) = 2^b$, $\deg(\varphi_{\mathrm{Kani}}) = d_{\mathrm{chl}}(2^a - d_{\mathrm{chl}})$,

and $\deg(\varphi_3) = 2^b$ (or 2^{b-1}).

The response is computed as follows. Here, (P_2, Q_2) is a basis $E_2[2^{a+b}]$ determined only from E_2 uniquely.

(1) Compute $\alpha, M,$ `is_M_halved` $:=$ `RandPushEnd`$(2^{3b} d_{\mathrm{chl}}(2^a - d_{\mathrm{chl}}), N, \alpha_{\mathrm{sk}}, \alpha_{\mathrm{com}})$.

(2) Compute a left-$\mathcal{O}_0$ ideal $L := I_{\mathrm{com}} \cdot \alpha$ which corresponds to $\varphi_{\mathrm{com}} \circ \alpha$.

(3) Compute a left-$\mathcal{O}_0$ ideal $L_1 := L + N2^b\mathcal{O}_0$ which corresponds to $\varphi_1 \circ \varphi_{\mathrm{sk}}$.

(4) Compute $\beta_1 \in L_1, q_1, E_1, \psi_1(P_0), \psi_1(Q_0)$, and K_1 by `ShortIdealToIsogenyIQO` where K_1 is a basis of $\mathrm{Ker}(\varphi_1)$.

(5) Compute a left-$\mathcal{O}_0$ ideal $L_2 := L + N2^{2b}\mathcal{O}_0$ which corresponds to $\varphi_2 \circ \varphi_1 \circ \varphi_{\mathrm{sk}}$.

(6) Compute a left-$\mathcal{O}_0$ ideal $L_2' := L_2 \frac{\overline{\beta_1}}{N2^b}$ which corresponds to $\varphi_2 \circ \psi$.

(7) Compute $\beta_2 \in L_2', q_2, E_2, \psi_2(P_0), \psi_2(Q_0)$, and K_2 by `ShortIdealToIsogenyIQO` where K_2 is a basis of $\mathrm{Ker}(\varphi_2)$.

(8) Compute $M_{\psi_2} \in \mathrm{GL}_2(\mathbb{Z}/2^{a+b}\mathbb{Z})$ such that $(\psi_2(P_0), \psi_2(Q_0)) = (P_2, Q_2)M_{\psi_2}$.

(9) Compute $\beta := \frac{\alpha\overline{\beta_1}\,\overline{\beta_2}}{2^{2b}q_1} \in \mathcal{O}_0$, and $\beta(P_0), \beta(Q_0) \in E_0$.

(10) Compute $M_\beta \in \mathrm{M}_2(\mathbb{Z}/2^{a+b}\mathbb{Z})$ such that $(\beta(P_0), \beta(Q_0)) = (P_0, Q_0)M_\beta$.

(11) Compute $(U_{\mathrm{com}}, V_{\mathrm{com}}) := \frac{1}{N}(P_{\mathrm{com}}, Q_{\mathrm{com}})M_\beta M_{\psi_2}^{-1}$ over $\mathbb{Z}/2^{a+b}\mathbb{Z}$. Note that $N \in (\mathbb{Z}/2^{a+b}\mathbb{Z})^\times$.

At last, the prover returns $K_1 \in E_{\mathrm{pk}}[2^b], K_2 \in E_1[2^b]$ and $U_{\mathrm{com}}, V_{\mathrm{com}} \in E_{\mathrm{com}}[2^{a+b}]$ as the response. We show the following important fact about the response:

Lemma 3. *In the above notation, we have*

$$(U_{\mathrm{com}}, V_{\mathrm{com}}) = ((\varphi_{\mathrm{Kani}} \circ \varphi_3)(P_2), (\varphi_{\mathrm{Kani}} \circ \varphi_3)(Q_2)).$$

Proof. First, we show that $\beta = \widehat{\varphi_{\mathrm{com}}} \circ \varphi_{\mathrm{Kani}} \circ \varphi_3 \circ \psi_2$. By the definitions, we have $\hat{\beta_1} = \widehat{\varphi_{\mathrm{sk}}} \circ \widehat{\varphi_1} \circ \psi_1$, $\hat{\beta_2} = \widehat{\psi_1} \circ \widehat{\varphi_2} \circ \psi_2$, and $\varphi_{\mathrm{Kani}} \circ \varphi_3 \circ \varphi_2 \circ \varphi_1 \circ \varphi_{\mathrm{sk}} = \varphi_{\mathrm{com}} \circ \alpha$. Thus, $[N]\alpha \circ \hat{\beta_1} \circ \hat{\beta_2} = [q_1]\widehat{\varphi_{\mathrm{com}}} \circ \varphi_{\mathrm{com}} \circ \alpha \circ (\widehat{\varphi_{\mathrm{sk}}} \circ \widehat{\varphi_1} \circ \widehat{\varphi_1}) \circ \psi_2 = [2^{2b}Nq_1]\widehat{\varphi_{\mathrm{com}}} \circ \varphi_{\mathrm{Kani}} \circ \varphi_3 \circ \psi_2$. Hence, $\beta = \widehat{\varphi_{\mathrm{com}}} \circ \varphi_{\mathrm{Kani}} \circ \varphi_3 \circ \psi_2$. Then, we have

$$\begin{aligned}(P_{\mathrm{com}}, Q_{\mathrm{com}})M_\beta &= (\varphi_{\mathrm{com}}(P_0), \varphi_{\mathrm{com}}(Q_0))M_\beta \\ &= (\varphi_{\mathrm{com}}(\beta(P_0)), \varphi_{\mathrm{com}}(\beta(Q_0))) \\ &= N(\varphi_{\mathrm{Kani}}(\varphi_3(\psi_2(P_0))), \varphi_{\mathrm{Kani}}(\varphi_3(\psi_2(Q_0)))) \\ &= N(\varphi_{\mathrm{Kani}}(\varphi_3(P_0)), \varphi_{\mathrm{Kani}}(\varphi_3(Q_0)))M_{\psi_2}.\end{aligned}$$

Thus, we have

$$\begin{aligned}(U_{\mathrm{com}}, V_{\mathrm{com}}) &:= \frac{1}{N}(P_{\mathrm{com}}, Q_{\mathrm{com}})M_\beta M_{\psi_2}^{-1} \\ &= (\varphi_{\mathrm{Kani}}(\varphi_3(P_0)), \varphi_{\mathrm{Kani}}(\varphi_3(Q_0))).\end{aligned}$$

Algorithm 3 `Response`

Require: `param` $= (p, a, b, N, E_0, \mathcal{O}_0)$, `pk` $= E_{\mathrm{pk}}$, `sk` $= (P_{\mathrm{pk}}, Q_{\mathrm{pk}}, \alpha_{\mathrm{sk}}, I_{\mathrm{sk}})$, `com` $= E_{\mathrm{com}}$, `sec` $= (P_{\mathrm{com}}, Q_{\mathrm{com}}, \alpha_{\mathrm{com}}, I_{\mathrm{com}})$, `chl` $= d_{\mathrm{chl}}$.

Ensure: `resp`$=(K_1, K_2, (\varphi_{\mathrm{Kani}} \circ \varphi_3)(P_2), (\varphi_{\mathrm{Kani}} \circ \varphi_3)(Q_2),$ `is_M_halved`$)$.

1: $\alpha, \_,$ `is_M_halved` $:=$ `RandPushEnd`$(2^{3b} d_{\mathrm{chl}}(2^a - d_{\mathrm{chl}}), N, \alpha_{\mathrm{sk}}, \alpha_{\mathrm{com}})$.
2: $L := I_{\mathrm{com}} \cdot \alpha$.
3: $L_1 := L + N2^b\mathcal{O}_0$.
4: $(q_1, E_1, \psi_1(P_0), \psi_1(Q_0), K_1, \beta_1)$ $:=$ `ShortIdealToIsogenyIQO` $(N, E_{\mathrm{pk}}, \varphi_{\mathrm{sk}}(P_0), \varphi_{\mathrm{sk}}(Q_0), L_1)$.
5: $L_2 := L + N2^{2b}\mathcal{O}_0$.
6: $L_2' := L_2 \frac{\overline{\beta_1}}{N2^b}$.
7: $(q_2, E_2, \psi_2(P_0), \psi_2(Q_0), K_2, \beta_2)$ $:=$ `ShortIdealToIsogenyIQO` $(q_1, E_1, \psi_1(P_0), \psi_1(Q_0), L_2')$.
8: Compute $M_{\psi_2} \in \mathrm{GL}_2(\mathbb{Z}/2^{a+b}\mathbb{Z})$ such that $(\psi_2(P_0), \psi_2(Q_0)) = (P_2, Q_2)M_{\psi_2}$.
9: $\beta := \frac{\alpha\overline{\beta_1}\,\overline{\beta_2}}{2^{2b}q_1}$.
10: Compute $M_\beta \in \mathrm{M}_2(\mathbb{Z}/2^{a+b}\mathbb{Z})$ such that $(\beta(P_0), \beta(Q_0)) = (P_0, Q_0)M_\beta$.
11: $(U_{\mathrm{com}}, V_{\mathrm{com}}) := \frac{1}{N}(P_{\mathrm{com}}, Q_{\mathrm{com}})M_\beta M_{\psi_2}^{-1}$.
12: **return** `resp` $= (K_1, K_2, U_{\mathrm{com}}, V_{\mathrm{com}},$ `is_M_halved`$)$.

□

An Algorithm 3 shows the response.

3.2.6 Verification.

The verifier computes $E_1 := E_2/K_1$ and $E_2 := E_1/K_2$. Then, the verifier has (P_2, Q_2) and the images $(U_{\mathrm{com}}, V_{\mathrm{com}})$ under $\varphi_{\mathrm{Kani}} \circ \varphi_3$:

$$E_2 \xrightarrow{\varphi_3} E_3 \xrightarrow{\varphi_{\mathrm{Kani}}} E_{\mathrm{com}}.$$

In this condition, as below, the verifier computes E_3 and construct a basis of $E_3[2^a]$ to apply the Kani's lemma to φ_{Kani}.

First, if `is_M_haved` is `False`, we write $(a', b') := (a, b)$, otherwise, $(a', b') := (a+1, b-1)$. Note that $\deg(\varphi_3) = b'$. Then, we take integers $0 \le s_1, t_1 < 2^{b'}$,$(s_1, t_1) \neq (0, 0)$ such that $2^{a'}s_1U_{\mathrm{com}} + 2^{a'}t_1V_{\mathrm{com}} = 0$. Thus, we have $\varphi_3(2^{a'}s_1P_2 + 2^{a'}t_1Q_2) = 0$, and since $\mathrm{Ker}(\varphi_3)$ is cyclic, $\mathrm{Ker}(\varphi_3)$ is generated by $K_3 := 2^{a'}s_1P_2 + 2^{a'}t_1Q_2 \in E_2[2^{b'}]$. We take $0 \le s_2, t_2 < 2^{b'}$ such that $((s_1, t_1), (s_2, t_2))$ is a basis of $(\mathbb{Z}/2^{b'}\mathbb{Z})^2$. Then, for

$$\begin{aligned}P_3 &:= 2^{b-b'}(s_1\varphi_3(P_2) + t_1\varphi_3(Q_2)), \\ Q_3 &:= 2^b(s_2\varphi_3(P_2) + t_2\varphi_3(Q_2)),\end{aligned}$$

(P_3, Q_3) is a basis of $E_3[2^a]$, and we have

$$\begin{aligned}\varphi_{\mathrm{Kani}}(P_3) &= 2^{b-b'}(s_1U_{\mathrm{com}} + t_1V_{\mathrm{com}}), \\ \varphi_{\mathrm{Kani}}(Q_3) &= 2^b(s_2U_{\mathrm{com}} + t_2V_{\mathrm{com}}).\end{aligned}$$

We apply Kani's lemma to $d_{\mathrm{chl}}(2^a - d_{\mathrm{chl}})$-isogeny $\varphi_{\mathrm{Kani}} : E_3 \to E_{\mathrm{com}}$. Thus, the quotient $\Phi : E_3 \times E_{\mathrm{com}} \to F_1 \times F_2$ by K is a $(2^a, 2^a)$ -isogeny to a product of elliptic curves. Then, $\varphi_{\mathrm{Kani}} : E_3 \to E_{\mathrm{com}}$ is decomposed to a d_{chl}-isogeny $f : E_3 \to F_1$ or a $(2^a - d_{\mathrm{chl}})$-isogeny $f : E_3 \to F_1$. If

$(R,*) := \Phi((P_3,0))$ or $(S,*) := \Phi((Q_3,0))$ for $R, S \in F_1$, it holds that $R = f(P_3)$ and $S = f(Q_3)$. Hence, we have

$$e_{2^a}^{F_1}(R,S) = e_{2^a}^{F_1}(f(P_3), f(Q_3)) = e_{2^a}^{E_3}(P_3,Q_3)^{\deg(f)}. \tag{3}$$

Since $d_{\mathrm{chl}} < 2^{a-1}$, the condition $d'_{\mathrm{chl}} \in \{d_{\mathrm{chl}}, 2^a - d_{\mathrm{chl}}\}$ characterizes $d'_{\mathrm{chl}} = d_{\mathrm{chl}}$.

The verifier confirms whether $(E_3 \times E_{\mathrm{com}})/K$ is a product of elliptic curves and equation (3) holds. An Algorithm 4 describes the verification.

Algorithm 4 `Verify`

Require: `param` $= (p,a,b,N,E_0,\mathcal{O}_0)$, `pk` $= E_{\mathrm{pk}}$, `com` $= E_{\mathrm{com}}$, `sec` $= (P_{\mathrm{com}}, Q_{\mathrm{com}}, \alpha_{\mathrm{com}}, I_{\mathrm{com}})$, `chl` $= d_{\mathrm{chl}}$, `resp` $= (K_1, K_2, U_{\mathrm{com}}, V_{\mathrm{com}}, \texttt{is\_M\_halved})$.
Ensure: accept or reject.
$E_1 := E_{\mathrm{pk}}/K_1$.
$E_2 := E_1/K_2$.
if `is_M_halved` is `False` **then**
  $(a',b') := (a,b)$.
else
  $(a',b') := (a+1, b-1)$.
end if
Compute $(s_1,t_1) \in (\mathbb{Z}/2^{b'}\mathbb{Z})^2$ such that $2^{a'}(s_1U_{\mathrm{com}} + t_1V_{vom}) = 0$.
Compute $(s_2,t_2) \in (\mathbb{Z}/2^{b'}\mathbb{Z})^2$ such that $(s_1,t_2),(s_2,t_2)$ is a basis of $(\mathbb{Z}/2^{b'}\mathbb{Z})^2$.
$K_3 := 2^{a'}(s_1P_2 + t_1Q_2)$.
$E_3 := E_2/K_3$ and $\varphi_3 : E_2 \to E_3$.
$P_3 := 2^{b-b'}(s_1\varphi_3(P_2) + t_1\varphi_3(Q_2))$.
$Q_3 := 2^b(s_2\varphi_3(P_2) + t_2\varphi_3(Q_2))$.
`is_valid`, _, _, _ := `KaniCod`$(d_{\mathrm{chl}}, 2^a - d_{\mathrm{chl}}, E_3, E_{\mathrm{com}}, P_3, Q_3, 2^{b-b'}(s_1U_{\mathrm{com}} + t_1V_{\mathrm{com}}), 2^b(s_2U_{\mathrm{com}} + t_2V_{\mathrm{com}}); \emptyset, \emptyset)$.
if `is_valid` **then**
  return accept.
else
  return reject.
end if

4. Security Analysis

In this section, we give a security analysis on our protocol. To ensure that our protocol is EUF-CMA secure, we prove that the underlying Σ-protocol is knowledge-sound and honest-verifier zero-knowledge. Throughout the security analysis, we denote the Σ-protocol by Σ_{Our}.

4.1 Special-Soundness

We show that Σ_{Our} is special-sound with respect to the following relation:

$$\mathcal{R}_{\texttt{OneEnd}} = \{(E,\alpha) \mid E/\mathbb{F}_{p^2} : \text{supersingular}\ , \alpha \in \mathrm{End}(E) \backslash \mathbb{Z}\}.$$

To prove the special-soundness, we use the following lemma.

Lemma 4. *Let q be a prime power. For $x, y \in (0,q)_q$, the following two propositions are equivalent.*

(i) *$x(q-x)y(q-y)$ is the square of an integer.*

(ii) *$x = y$ or $x + y = q$ ($\Leftrightarrow x(q-x) = y(q-y)$.)*

Proof. $(ii) \Rightarrow (i)$ is trivial. We prove $(i) \Rightarrow (ii)$. Assume that $x, y \in (0,q)_q$ satisfy (i). Then the square-free part of xy is equal to that of $(q-x)(q-y)$. I.e., the following equations hold:

$$xy = m^2 r \tag{4}$$
$$(q-x)(q-y) = n^2 r, \tag{5}$$

where $m, n \in (0,q)_q$ and r is a square-free positive integer coprime to q. From now on, we will prove that m and n satisfy $m \equiv \pm n \mod q$. From (4) − (5), we have

$$(m-n)(m+n)r = q(x+y-q). \tag{6}$$

- When $q = 2^\ell$: dividing (6) by 4, we obtain the following:

$$\frac{m-n}{2} \cdot \frac{m+n}{2} \cdot r = 2^{\ell-1}\left(\frac{x+y}{2} - 2^{\ell-1}\right).$$

  Since $\frac{m-n}{2} + \frac{m+n}{2} = m$ is odd, either $\frac{m-n}{2}$ or $\frac{m+n}{2}$ is odd. Note that r is also odd. On the other hand, the right hand side is divisible by $2^{\ell-1}$. Therefore, either $\frac{m-n}{2}$ or $\frac{m+n}{2}$ is divisible by $2^{\ell-1}$ and thus $m \equiv \pm n \mod 2^\ell$ holds.

- When q is odd: since $(m-n) + (m+n) = 2m$ is coprime to q, either $(m-n)$ or $(m+n)$ is coprime to q. Note that r is also coprime to q. On the other hand, the right hand side of (6) is divisible by q. Therefore, either $(m-n)$ or $(m+n)$ is divisible by q and thus $m \equiv \pm n \mod q$ holds.

Now we will prove that $x = y$ or $x + y = q$ holds. Since $m \equiv \pm n \mod q$ and $m, n \in (0,q)_q$ hold, we have $m = n$ or $m + n = q$.

(I) When $m = n$: from (6), we have $x + y = q$.

(II) When $m + n = q$: from (6) and (4), we obtain

$$\begin{cases} x + y = (2m-q)r + q \\ xy = m^2 r. \end{cases} \tag{7}$$

Therefore, we have

$$\begin{aligned} 0 \le (x-y)^2 &= (x+y)^2 - 4xy \\ &= \{(2m-q)r + q\}^2 - 4m^2 r \\ &= (r-1)\{(2m-q)^2 r - q^2\}. \end{aligned}$$

Here, we assume that $r \neq 1$. Then $(2m-q)^2 r - q^2 \ge 0$ holds. Moreover, since $0 < x + y < 2q$, we have

$$0 < (2m-q)r + q < 2q.$$
$$\therefore (2m-q)^2 r < \frac{q^2}{r}.$$

From the above discussion, we obtain the following inequality:

$$\frac{q^2}{r} - q^2 > 0 \Leftrightarrow 0 < r < 1.$$

This contradicts to the fact that r is a positive integer. Therefore, we have $r = 1$. Finally, substituting $r = 1$ into (7), we obtain $x = y = m$.

□

Now we prove the special-soundness of Σ_{Our}.

Proof. Let $(E_{\mathrm{com}}, d_{\mathrm{chl}}, \mathrm{rsp})$ and $(E_{\mathrm{com}}, d'_{\mathrm{chl}}, \mathrm{rsp}')$ be two transcripts against the statement E_{pk} with the same commitment E_{com} but different challenges $d_{\mathrm{chl}} \neq d'_{\mathrm{chl}}$. Since rsp and rsp$'$ are efficient representations of isogenies $\varphi_{\mathrm{rsp}} : E_{\mathrm{pk}} \to E_{\mathrm{com}}$ and $\varphi'_{\mathrm{rsp}} : E_{\mathrm{pk}} \to E_{\mathrm{com}}$ of degree $2^{3b} d_{\mathrm{chl}}(2^a - d_{\mathrm{chl}})$ and $2^{3b} d'_{\mathrm{chl}}(2^a - d'_{\mathrm{chl}})$, respectively, we obtain an endomorphism $\alpha = \widehat{\varphi}'_{\mathrm{rsp}} \circ \varphi_{\mathrm{rsp}} \in \mathrm{End}(E_{\mathrm{pk}})$ of degree $2^{6b} d_{\mathrm{chl}}(2^a - d_{\mathrm{chl}}) d'_{\mathrm{chl}}(2^a - d'_{\mathrm{chl}})$. It is sufficient to show that this α is not scalar.

Assume that α is a scalar, then $\deg \alpha = 2^{6b} d_{\mathrm{chl}}(2^a - d_{\mathrm{chl}}) d'_{\mathrm{chl}}(2^a - d'_{\mathrm{chl}})$ is the square of an integer. Consequently, $d_{\mathrm{chl}}(2^a - d_{\mathrm{chl}}) d'_{\mathrm{chl}}(2^a - d'_{\mathrm{chl}})$ is the square of an integer. Note that $d_{\mathrm{chl}}, d'_{\mathrm{chl}} \in (2^{a-2}, 2^{a-1})_2 \subset (0, 2^a)_{2^a}$. From Lemma 4, we have $d_{\mathrm{chl}} = d'_{\mathrm{chl}}$ or $d_{\mathrm{chl}} + d'_{\mathrm{chl}} = 2^a$. From our assumption, $d_{\mathrm{chl}} = d'_{\mathrm{chl}}$ does not hold. Furthermore, since d_{chl} and d'_{chl} are smaller than 2^{a-1}, $d_{\mathrm{chl}} + d'_{\mathrm{chl}} = 2^a$ does not hold either. This is contradiction. □

4.2 Honest-Verifier Zero-Knowledge

We now show that Σ_{Our} is weak honest-verifier zero-knowledge (wHVZK). As in SQIsign, we use the *hint-assisted wHVZK* framework [[2], Definition 3.2], where the zero-knowledge simulator receives some additional information called *hints* sampled from a hint distribution [[2], Definition 3.1].

To use the hint-assisted wHVZK framework, we first define a hint distribution as follows.

$\underline{\mathcal{H}_{E_{\mathrm{pk}}} \to \varphi :}$

1. Take a random odd integer $d \xleftarrow{\$} (2^{a-2}, 2^{a-1})_2$.
2. Sample an isogeny $\varphi : E_{\mathrm{pk}} \to E$ uniformly among all isogenies from E_{pk} of degree $2^{3b} d(2^a - d)$.
3. Return an efficient representation of φ as with the output of Algorithm 3.

In addition, we assume that the distribution of φ sampled from $\mathcal{H}_{E_{\mathrm{pk}}}$ is statistically indistinguishable from that of φ_{rsp} output as a response of Σ_{Our}. More precisely, we assume the computational hardness of the following problem.

Problem 1. *Given a supersingular elliptic curve* $\mathtt{pk} = E_{\mathrm{pk}}$ *over* $\mathbb{F}_{p^2}$ *and* q *isogenies* $\varphi_1, \ldots, \varphi_q$ *sampled with probability* $1/2$ *from either distribution:*

- $\mathcal{D}_0 = (\mathtt{pk}, \varphi_1, \ldots, \varphi_q)$, *where* $(\mathtt{pk},\mathtt{sk}) \leftarrow \mathtt{KeyGen}(1^\lambda)$, $(\mathtt{com}_i, \mathtt{sec}_i) \leftarrow \mathtt{Commit}(\mathtt{pk},\mathtt{sk})$, $\mathtt{chl}_i \leftarrow \mathtt{Challenge}$, $\varphi_i \leftarrow \mathtt{Response}(\mathtt{pk},\mathtt{sk},\mathtt{com}_i,\mathtt{sec}_i,\mathtt{chl}_i)$ *for* $i \in \{1, \ldots, q\}$.
- $\mathcal{D}_1 = (\mathtt{pk}, \varphi_1, \ldots, \varphi_q)$, *where* $(\mathtt{pk},\mathtt{sk}) \leftarrow \mathtt{KeyGen}(1^\lambda)$, $\varphi_i \xleftarrow{\$} \mathcal{H}_{\mathtt{pk}}$ *for* $i \in \{1, \ldots, q\}$.

Determine from which distribution these isogenies are sampled.

The proof of hint-assisted wHVZK under the hardness assumption of this problem is straightforward.

5. Efficiency

In this section, we analyze and compare the signature sizes and the computational cost.

5.1 Signature size

In this subsection, we briefly analyze and compare the approximate signature sizes of the protocols for the security parameter λ. The signature of the proposed protocol consists of $(E_{\mathrm{com}}, K_1, K_2, U_{\mathrm{com}}, V_{\mathrm{com}}, \mathtt{is\_M\_haved})$. By applying the similar optimization as SQIsign [11], the approximate signature size is 12λ bits Table 1 shows the approximate signature sizes in bits of each protocols.

Table 1 Approximate signature sizes comparison.

Protocol	Signature size (bit)
SQIsign2D-West [4]	9λ
SQIsign2D-East [21]	9λ
SQIPrime2D (resp.4D) [14]	19λ (resp.12λ)
PRISM [3]	12λ
This work	$\mathbf{12}\lambda$

5.2 Computational Cost

In some signature protocols using two-dimensional isogenies, the dominant portion of the computational cost are computing the chain of $(2,2)$-isogenies. During both of the key generation and the commitment phase, we perform b computations of $(2,2)$-isogenies. In addition, during the response phase, we perform $2a$ computations of $(2,2)$-isogenies. Thus, $(2a + b)$ computations of $(2,2)$-isogenies are carried out during signature generation. On the other hand, during the verification phase, we perform a computations of $(2,2)$-isogenies. Under the approximation $a \approx b \approx \lambda$, Table 2 shows the the number of $(2,2)$-isogeny computations required at each step of the protocols. Comparing the execution times of implementations is left as future work.

Table 2 The number of the $(2,2)$-isogeny computation.

Protocol	Gen	Sign	Verf
SQIsign2D-West [4]	4λ	9λ	λ
SQIsign2D-East [21]	2λ	3.5λ	λ
SQIPrime2D [14]	2λ	4λ	2λ
PRISM [3]	4λ	4λ	2λ
This work	$\mathbf{2}\lambda$	$\mathbf{3}\lambda$	λ

6. Conclusion

In this paper, we introduce a new isogeny-based signature protocol. First, we provided a new algorithm `RandPushEnd` as a building block, and constructed a new signature scheme. Second, we show that our protocol is EUF-CMA secure using the hint-assisted wHVZK framework. Finally, we compared the signature size and the the number of the $(2,2)$-isogeny computations with those of other protocols. As a result, we confirmed that the signature size remains comparable to that of PRISM, while the computational number of the $(2,2)$-isogeny is smaller than other protocols. As a future work, we need to provide a detailed comparison based on the implementation.

Acknowledgments The second author was supported by WISE program (MEXT) at Kyushu University.

References

[1] Marius A. Aardal, Gora Adj, Diego F. Aranha, Andrea Basso, Isaac Andrés Canales Martínez, Jorge Chávez-Saab, Maria Corte-Real Santos, Pierrick Dartois, Luca De Feo, Max Duparc, Jonathan Komada Eriksen, Tako Boris Fouotsa, Décio Luiz Gazzoni Filho, Basil Hess, David Kohel, Antonin Leroux, Patrick Longa, Luciano Maino, Michael Meyer, Kohei Nakagawa, Hiroshi Onuki, Lorenz Panny, Sikhar Patranabis, Christophe Petit, Giacomo Pope, Krijn Reijnders, Damien Robert, Francisco Rodríguez Henríquez, Sina Schaeffler, and Benjamin Wesolowski. SQIsign. Technical report, National Institute of Standards and Technology, 2024. available at `https://csrc.nist.gov/Projects/pqc-dig-sig/round-2-additional-signatures`.

[2] Marius A. Aardal, Andrea Basso, Luca De Feo, Sikhar Patranabis, and Benjamin Wesolowski. A complete security proof of SQIsign. Cryptology ePrint Archive, Report 2025/379, 2025.

[3] Andrea Basso, Giacomo Borin, Wouter Castryck, Maria Corte-Real Santos, Riccardo Invernizzi, Antonin Leroux, Luciano Maino, Frederik Vercauteren, and Benjamin Wesolowski. PRISM: Simple and compact identification and signatures from large prime degree isogenies. In Tibor Jager and Jiaxin Pan, editors, *PKC 2025, Part III*, volume 15676 of *LNCS*, pages 300–332. Springer, Cham, May 2025.

[4] Andrea Basso, Pierrick Dartois, Luca De Feo, Antonin Leroux, Luciano Maino, Giacomo Pope, Damien Robert, and Benjamin Wesolowski. SQIsign2D-West - the fast, the small, and the safer. In Kai-Min Chung and Yu Sasaki, editors, *ASIACRYPT 2024, Part III*, volume 15486 of *LNCS*, pages 339–370. Springer, Singapore, December 2024.

[5] Andrea Basso and Luciano Maino. POKÉ: A compact and efficient PKE from higher-dimensional isogenies. In Serge Fehr and Pierre-Alain Fouque, editors, *EUROCRYPT 2025, Part II*, volume 15602 of *LNCS*, pages 94–123. Springer, Cham, May 2025.

[6] Andrea Basso, Luciano Maino, and Giacomo Pope. FESTA: Fast encryption from supersingular torsion attacks. In Jian Guo and Ron Steinfeld, editors, *ASIACRYPT 2023, Part VII*, volume 14444 of *LNCS*, pages 98–126. Springer, Singapore, December 2023.

[7] Wouter Castryck and Thomas Decru. An efficient key recovery attack on SIDH. In Carmit Hazay and Martijn Stam, editors, *EUROCRYPT 2023, Part V*, volume 14008 of *LNCS*, pages 423–447. Springer, Cham, April 2023.

[8] Jorge Chavez-Saab, Maria Corte-Real Santos, Luca De Feo, Jonathan Komada Eriksen, Basil Hess, David Kohel, Antonin Leroux, Patrick Longa, Michael Meyer, Lorenz Panny, Sikhar Patranabis, Christophe Petit, Francisco Rodríguez Henríquez, Sina Schaeffler, and Benjamin Wesolowski. SQIsign. Technical report, National Institute of Standards and Technology, 2023. available at `https://csrc.nist.gov/Projects/pqc-dig-sig/round-1-additional-signatures`.

[9] Pierrick Dartois, Antonin Leroux, Damien Robert, and Benjamin Wesolowski. SQIsignHD: New dimensions in cryptography. In Marc Joye and Gregor Leander, editors, *EUROCRYPT 2024, Part I*, volume 14651 of *LNCS*, pages 3–32. Springer, Cham, May 2024.

[10] Pierrick Dartois, Luciano Maino, Giacomo Pope, and Damien Robert. An algorithmic approach to (2, 2)-isogenies in the theta model and applications to isogeny-based cryptography. In Kai-Min Chung and Yu Sasaki, editors, *ASIACRYPT 2024, Part III*, volume 15486 of *LNCS*, pages 304–338. Springer, Singapore, December 2024.

[11] Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski. SQISign: Compact post-quantum signatures from quaternions and isogenies. In Shiho Moriai and Huaxiong Wang, editors, *ASIACRYPT 2020, Part I*, volume 12491 of *LNCS*, pages 64–93. Springer, Cham, December 2020.

[12] Luca De Feo, Antonin Leroux, Patrick Longa, and Benjamin Wesolowski. New algorithms for the Deuring correspondence - towards practical and secure SQISign signatures. In Carmit Hazay and Martijn Stam, editors, *EUROCRYPT 2023, Part V*, volume 14008 of *LNCS*, pages 659–690. Springer, Cham, April 2023.

[13] Max Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 14:197–272, 1941.

[14] Max Duparc and Tako Boris Fouotsa. SQIPrime: A dimension 2 variant of SQISignHD with non-smooth challenge isogenies. In Kai-Min Chung and Yu Sasaki, editors, *ASIACRYPT 2024, Part III*, volume 15486 of *LNCS*, pages 396–429. Springer, Singapore, December 2024.

[15] Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In Andrew M. Odlyzko, editor, *CRYPTO'86*, volume 263 of *LNCS*, pages 186–194. Springer, Berlin, Heidelberg, August 1987.

[16] David Jao, Reza Azarderakhsh, Matthew Campagna, Craig Costello, Luca De Feo, Basil Hess, Amir Jalali, Brian Koziel, Brian LaMacchia, Patrick Longa, Michael Naehrig, Joost Renes, Vladimir Soukharev, David Urbanik, Geovandro Pereira, Koray Karabina, and Aaron Hutchinson. SIKE. Technical report, National Institute of Standards and Technology, 2020. available at `https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions`.

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

[18] David Kohel, Kristin Lauter, Christophe Petit, and Jean-Pierre Tignol. On the quaternion ℓ-isogeny path problem. *LMS Journal of Computation and Mathematics*, 17(A):418–432, 2014.

[19] Luciano Maino, Chloe Martindale, Lorenz Panny, Giacomo Pope, and Benjamin Wesolowski. A direct key recovery attack on SIDH. In Carmit Hazay and Martijn Stam, editors, *EUROCRYPT 2023, Part V*, volume 14008 of *LNCS*, pages 448–471. Springer, Cham, April 2023.

[20] Kohei Nakagawa and Hiroshi Onuki. QFESTA: Efficient algorithms and parameters for FESTA using quaternion algebras. In Leonid Reyzin and Douglas Stebila, editors, *CRYPTO 2024, Part V*, volume 14924 of *LNCS*, pages 75–106. Springer, Cham, August 2024.

[21] Kohei Nakagawa, Hiroshi Onuki, Wouter Castryck, Mingjie Chen, Riccardo Invernizzi, Gioella Lorenzon, and Frederik Vercauteren. SQIsign2D-East: A new signature scheme using 2-dimensional isogenies. In Kai-Min Chung and Yu Sasaki, editors, *ASIACRYPT 2024, Part III*, volume 15486 of *LNCS*, pages 272–303. Springer, Singapore, December 2024.

[22] Hiroshi Onuki and Kohei Nakagawa. Ideal-to-isogeny algorithm using 2-dimensional isogenies and its application to SQIsign. In Kai-Min Chung and Yu Sasaki, editors, *ASIACRYPT 2024, Part III*, volume 15486 of *LNCS*, pages 243–271. Springer, Singapore, December 2024.

[23] Christophe Petit and Spike Smith. An improvement to the quaternion analogue of the ℓ-isogeny path problem, 2018. Conference talk at MathCrypt.

[24] Damien Robert. Breaking SIDH in polynomial time. In Carmit Hazay and Martijn Stam, editors, *EUROCRYPT 2023, Part V*, volume 14008 of *LNCS*, pages 472–503. Springer, Cham, April 2023.