Δ-SQIsign: A New Isogeny-Based Signature Scheme Using Degree Challenges

Kohei Nakagawa, Ryo Yoshizumi

NTT Social Informatics Laboratories, Japan

Abstract. Isogeny-based cryptography is a kind of cryptography whose security relies on the computational hardness of the isogeny problem. This field is gaining attention as a promising candidate for post-quantum cryptography. Among the notable schemes within this category is SQIsign, a signature schemes that has been submitted to the NIST Post-Quantum Cryptography Standardization competition. In this paper, we introduce a new isogeny-based signature scheme, Δ-SQIsign, which represents a significant departure from existing isogeny-based signatures including SQIsign. The key distinction in our 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. To construct such a scheme, we introduce a new algorithm, called Δ-KLPT, which is a variant of GeneralizedKLPT. Similar to GeneralizedKLPT, our algorithm outputs an ideal equivalent to a given ideal with a fixed norm; however, under certain conditions, it produces an ideal of smaller norm than GeneralizedKLPT.

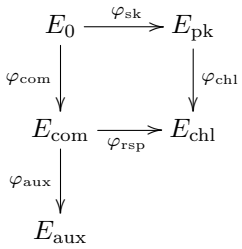
1 Introduction

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 [14], which was submitted to the NIST PQC standardization competition for additional signature [9]. Although SIKE [19] was also representative isogeny-based cryptography, several attacks on SIKE [8, 22, 26] 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.

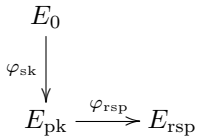
* The name Δ-SQIsign is derived from two concepts. Firstly, the Greek letter Δ corresponds to the 'D' in 'Degree,' reflecting the scheme's characteristic of using degree as a challenge. Secondly, the symbol Δ, resembling a triangle, represents the triangular shape of the isogeny diagram upon which this scheme is based.

Recently, a lot of cryptography using high-dimensional isogenies have been studied: encryption schemes such as FESTA [5], QFESTA [23], and POKÉ [4], and variants of SQIsign such as SQIsignHD [12], SQIsign2D-West [3], SQIsign2D-East [24], SQIPrime [17], and SQIsign2D^2 [29]. In particular, SQIsign2D-West has been adopted as the SQIsign specification in Round 2 of the NIST competition [1]. In this paper, we refer to SQIsign from Round 1 as 'SQIsign-v1.0' and from Round 2 as 'SQIsign-v2.0'. Additionally, we collectively refer to SQIsign-v2.0, SQIsign2D-East, SQIPrime, and SQIsign2D^2, which utilize two-dimensional isogenies, as the 'SQIsign2D variants'. The SQIsign2D variants rely on the hardness of the *endomorphism ring problem*, which is the problem to compute the endomorphism ring of a given supersingular elliptic curve. Roughly speaking, the SQIsign2D variants are obtained by applying the Fiat-Shamir transform on a Σ-protocol based on the following diagram.



In this protocol, a prover having a secret isogeny $\varphi_{\mathrm{sk}} : E_0 \to E_{\mathrm{pk}}$ first generates a random isogeny $\varphi_{\mathrm{com}} : E_0 \to E_{\mathrm{com}}$ and sends E_{com} to a verifier. The verifier then generates a random isogeny $\varphi_{\mathrm{chl}} : E_{\mathrm{pk}} \to E_{\mathrm{chl}}$ and returns it to the prover. The prover then computes an isogeny $\varphi_{\mathrm{rsp}} : E_{\mathrm{com}} \to E_{\mathrm{chl}}$ using the secret φ_{sk} and sends φ_{rsp} to the verifier. At this time, the prover can also send an auxiliary isogeny φ_{rsp} to help the verifier computations (except for SQIsignHD). Finally, the verifier checks if φ_{rsp} is an isogeny from E_{com} to E_{chl}.

Furthermore, a recent signature scheme called PRISM has been proposed, which takes a different approach from the SQIsign2D variants. The main difference is that PRISM rely on the hardness of a novel problem to compute a large prime-degree isogeny from a supersingular elliptic curve with an unknown endomorphism ring. PRISM is obtained by applying the hash-and-sign paradigm on a identification protocol based on the following diagram.



In this protocol, a verifier first generates a random prime q and sends it to a prover as a challenge. Then the prover having a secret isogeny $\varphi_{\mathrm{sk}} : E_0 \to E_{\mathrm{pk}}$ computes an isogeny φ_{rsp} from E_{pk} of degree $q(2^e - q)$ for an integer e and sends φ_{rsp} to the verifier. Finally, the verifier checks if $\deg(\varphi_{\mathrm{rsp}}) = q(2^e - q)$ holds.

PRISM has a lower computational cost for signing compared to the SQIsign2D variants. However, its verification requires nearly twice as many 2-dimensional isogeny computations as SQIsign-v2.0, SQIsign2D-East, and SQIsign2D^2. The signature size is comparable to that of the SQIsign2D variants.

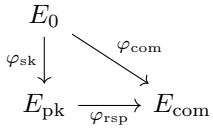
1.1 Contributions

In this paper, we make the following contributions.

- To construct such a scheme, we introduce a new algorithm, called Δ-KLPT, which is a variant of GeneralizedKLPT [14]. Similar to GeneralizedKLPT, our algorithm outputs an ideal equivalent to a given ideal with a fixed norm; however, under certain conditions, it produces an ideal of much smaller norm compared to GeneralizedKLPT.
- We present a novel signature scheme, Δ-SQIsign, based on an approach that differs from both the SQIsign2D variants and PRISM. The key distinction between our scheme and the SQIsign2D variants is its use of the degree of isogeny as a challenge within the underlying Σ-protocol, similar to PRISM. On the other hand, Δ-SQIsign differs from PRISM in that its security relies on the hardness of the endomorphism ring problem.
- We give the security analysis of our scheme using the *hint-assisted wHVZK* framework [1], which is also used in SQIsign-v2.0.
- We achieve the faster signing compared to the SQIsign-v2.0 variants though the result was less efficient than PRISM. In addition, we achieve the comparable verification cost compared to the SQIsign2D variants.
- We provide a proof-of-concept implementation of Δ-SQIsign in SageMath [27].

1.2 Technical Overview

In the following, we give an overview of our construction of Δ-SQIsign. Our Δ-SQIsign is obtained by applying the Fiat-Shamir transform on the Σ-protocol based on the following diagram.



In our Σ-protocol, a prover having a secret N-isogeny $\varphi_{\mathrm{sk}} : E_0 \to E_{\mathrm{pk}}$ first generates another N-isogeny $\varphi_{\mathrm{com}} : E_0 \to E_{\mathrm{com}}$ and sends E_{com} as a commitment to a verifier. The verifier then samples a random odd integer d and sends it to the prover as a challenge. The prover then computes an isogeny $\varphi_{\mathrm{rsp}} : E_{\mathrm{pk}} \to E_{\mathrm{com}}$ of degree $2^{e_1}d(2^{e_2} - d)$ for integers e_1, e_2 and sends φ_{rsp} to the verifier. Finally, the verifier checks if $\deg(\varphi_{\mathrm{rsp}}) = 2^{e_1}d(2^{e_2} - d)$ holds.

To generate such an isogeny φ_{rsp}, we construct a new algorithm named Δ-KLPT. This algorithm takes as input two left $\mathcal{O}_0$-ideals I_1, I_2 of the same norm N

and an integer M. Then it outputs an ideal J equivalent to $\bar{I}_1 I_2$ of norm dividing M. Note that we require that $n(I_1) = n(I_2)$ unlike GeneralizedKLPT. Under this conditions, the norm of the ideal output by our algorithm is $O(pN^3)$, which is substantially smaller than $O(p^3N^3)$ obtained by GeneralizedKLPT under the same conditions.

1.3 Organization

In Section 2, we give some notation and background knowledge used in this paper. In Section 3, we propose our new algorithm Δ-KLPT and construct our signature scheme Δ-SQIsign. In Section 4, we analyze the security of Δ-SQIsign. In Section 5, we give some concrete parameters for Δ-SQIsign and analyze the signature sizes and the computational costs of Δ-SQIsign. Finally, in Section 6, we give the conclusion of this paper.

2 Preliminaries

In this section, we summarize some background knowledge used in this paper.

2.1 Notation

Throughout this paper, we use the following notation. We let p be a prime number of cryptographic size, i.e., p is at least about 2^{256} and let λ be a security parameter. Let $f(x)$ and $g(x)$ be real functions. We write $f(x) = O(g(x))$ if there exists a constant $c \in \mathbb{R}$ such that $f(x)$ is bounded by $c \cdot g(x)$ for sufficiently large x. For a finite set S, we write $x \xleftarrow{\$} S$ if x is sampled uniformly at random from S. Let $\perp$ be the symbol indicating failure of an algorithm. For integers ℓ, m, n, we denote by $(m, n)_\ell$ a set of integers x such that $m < x < n$ and $\gcd(x, \ell) = 1$. For an odd prime N and an integer M, $\left(\frac{M}{N}\right)$ denotes the Legendre symbol.

2.2 Abelian varieties and Isogenies

In this paper, we mainly use principally polarized superspecial abelian varieties defined over a finite field of characteristic p of dimension one or two. Such a variety is isomorphic to a supersingular elliptic curve, the product of two supersingular elliptic curves, or a Jacobian of a superspecial hyperelliptic curve of genus two, and always has a model defined over $\mathbb{F}_{p^2}$. Therefore, we only consider varieties defined over $\mathbb{F}_{p^2}$.

Basic Facts. An *isogeny* is a rational map between abelian varieties which is a surjective group homomorphism with finite kernel. The *degree* of an isogeny φ is its degree as a rational map and is denoted by $\deg \varphi$. An isogeny φ is *separable* if $\#\ker \varphi = \deg \varphi$. A separable isogeny is uniquely determined by its kernel up to post-composition of isomorphism. For an isogeny $\varphi : A \to B$ between principally

polarized abelian varieties, there exists an isogeny $B \to A$ called the *dual isogeny* (with respect to the polarization). We denote the dual isogeny of φ by $\hat{\varphi}$.

Let $\varphi : A \to B$ and $\psi : A \to C$ be separable isogenies of coprime degrees. If a separable isogeny $\psi' : B \to D$ satisfies $\ker \psi' = \varphi(\ker \psi)$, we say that ψ' is the *push-forward* of ψ by φ and denote it by $\psi' = [\varphi]_*\psi$.

Let A and B be principally polarized abelian varieties. If there exists an isogeny between A and B, then the dimensions of A and B are the same. If A is superspecial, then there exists an isogeny between A and B if and only if B is a superspecial abelian variety of the same dimension as A.

Let A be a principally polarized abelian variety and ℓ a positive integer. An *ℓ-isotropic subgroup* of A is a subgroup of the ℓ-torsion subgroup $A[\ell]$ of A on which the ℓ-Weil pairing is trivial. An ℓ-isotropic subgroup G is *maximal* if there is no other ℓ-isotropic subgroup containing G. A separable isogeny whose kernel is a maximal ℓ-isotropic subgroup is called an *ℓ-isogeny* if the dimension of the domain is one or an *(ℓ, ℓ)-isogeny* if the dimension of the domain is two.

Let E be an elliptic curve defined over $\mathbb{F}_{p^2}$ and let n be an integer such that the n-torsion subgroup $E[n]$ is contained in $E(\mathbb{F}_{p^2})$. Then we can compute a deterministic basis of $E[n]$ by using deterministic algorithms such as [9, Algorithm 3] and [1, Algorithm 2.2].

Computing Isogenies. Let A be a principally polarized abelian variety, ℓ a positive integer, and G a maximal ℓ-isotropic subgroup of A.

If the dimension of A is one, then we can compute an ℓ-isogeny φ with kernel G by Vélu's formulas [28]. More precisely, given A, ℓ, G, Vélu's formulas give a method to compute the codomain of φ in $O(\ell)$ operations on a field containing the points in G. In addition, for additional input $P \in A$, we can compute $\varphi(P)$ in $O(\ell)$ operations on a field containing the points in G and P.

If the dimension of A is two and $\ell = 2$, then we can compute $(2, 2)$-isogeny with kernel G by the recent formulas proposed by Dartois, Maino, Pope, and Robert [13].

For an isogeny $\varphi : A \to B$, we say that information $\mathcal{I}_\varphi$ is an *efficient representation* of φ when we can compute $\varphi(P)$ in polynomial time from a given point $P \in A$ and the information $\mathcal{I}_\varphi$. For example, the tuple (A, ℓ, G) described above is an efficient representation of ℓ-isogeny $\varphi : A \to B$ when ℓ is smooth. In this paper, we assume that an isogeny is given by an efficient representation.

2.3 Quaternion Algebras and the Deuring Correspondence

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 $a, b \in \mathbb{Q}^*$. 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 $n(\alpha)$.

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

For an ideal I of $H(a,b)$, we define $\mathcal{O}_L(I) := \{\alpha \in H(a,b) | \alpha \cdot I \subset I\}$, which is known to be a maximal order of $H(a,b)$ and we call it a *left order* of I. A *right order* $\mathcal{O}_R(I)$ of I is similarly defined. For a maximal order $\mathcal{O}$, an *(integral) left $\mathcal{O}$-ideal* I is an ideal such that $\mathcal{O}_L(I) = \mathcal{O}$ and $I \subset \mathcal{O}$. 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 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 $\beta \in H(a,b)^*$ such that $I = J\beta$.

Deuring Correspondence. Deuring [16] 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 scheme. 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 $\mathcal{O}_0 := \mathbb{Z}\langle 1, \mathbf{i}, \frac{\mathbf{i}+\mathbf{j}}{2}, \frac{1+\mathbf{k}}{2}\rangle$. 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.

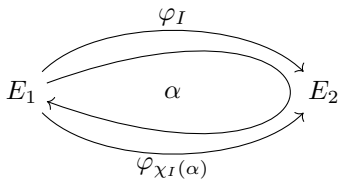
Some isogeny-based protocols, e.g., SQISign-v1.0 [14], need to compute the image under an element in $\mathcal{O}_0$ represented by the coefficients with respect to the basis $(1, \mathbf{i}, \frac{\mathbf{i}+\mathbf{j}}{2}, \frac{1+\mathbf{k}}{2})$. Let $P \in E_0(\mathbb{F}_{p^2})$ and $\alpha = x + y\mathbf{i} + z\frac{\mathbf{i}+\mathbf{j}}{2} + t\frac{1+\mathbf{k}}{2}$ 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 scheme. In this case, by pre-computing 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 $\varphi : E_1 \to E_2$ be an N-isogeny, then the isogeny φ can be associated to a left $\mathcal{O}_1$-ideal I_φ as follows:

$$I_\varphi = \{\alpha \in \mathcal{O}_1 \mid \alpha(P) = O,\ \forall P \in \ker\varphi\}.$$

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 $n(I_\varphi)$ is equal to the degree N of φ. Moreover, two isogenies $\varphi, \psi : E_1 \to E_2$ that have the same domain and codomain correspond to equivalent ideals $I_\varphi \sim I_\psi$.

Let I be a connecting ideal from $\mathcal{O}_1 \cong \mathrm{End}(E_1)$ to $\mathcal{O}_2 \cong \mathrm{End}(E_2)$, and let $\varphi_I : E_1 \to E_2$ be the corresponding isogeny. For $\alpha \in I \setminus \{0\}$, we define $\chi_I(\alpha) := I\frac{\bar{\alpha}}{n(I)}$, which is an ideal equivalent to I. We denote the norm of $\chi_I(\alpha)$ by $q_I(\alpha) := \frac{n(\alpha)}{n(I)} \in \mathbb{Z}$. The corresponding isogeny $\varphi_{\chi_I(\alpha)} : E_1 \to E_2$ satisfies $\widehat{\varphi_{\chi_I(\alpha)}} \circ \varphi_I = \alpha$.



Algorithms Using Quaternion Algebras. As in the above, we let $\mathcal{O}_0$ be the maximal order of $\mathcal{B}_{p,\infty}$ with basis $(1, \mathbf{i}, \frac{\mathbf{i}+\mathbf{j}}{2}, \frac{1+\mathbf{k}}{2})$. We introduce three existing algorithms using quaternion algebras necessary for the construction of our Δ-KLPT.

- $\texttt{FullRepresentInteger}_{\mathcal{O}_0}(M)$ [15]

Input: An integer $M > p$.
Output: $\alpha \in \mathcal{O}_0$ such that $n(\alpha) = M$.

- $\texttt{StrongApproximation}_M(N, C_0, D_0)$ [21, 25]

Input: A prime number N, integers M, C_0, D_0 such that $\left(\frac{M}{N}\right) = \left(\frac{p(C_0^2+D_0^2)}{N}\right)$ 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 $\mu_1 \in \mathcal{O}_0$.

In addition, we introduce an algorithm called GeneralizedKLPT, which is relevant to our new algorithm Δ-KLPT. GeneralizedKLPT is first proposed as a building block of SQIsign-v1.0 [14].

- $\texttt{GeneralizedKLPT}_M(I_0, I)$

Input: An integer M, a left $\mathcal{O}_0$-ideal I_0 of norm N, and a left $\mathcal{O}_R(I_0)$-ideal I.
Output: Equivalent ideal $J \sim I$ of norm M.

For this algorithm to succeed, it requires that $M = O(p^3N^3)$.

2.4 Kani's lemma

In this subsection, we introduce an algorithm `Kani`. This algorithm realizes to calculate isogenies of dimension one by computing isogenies of dimension two instead. This algorithm comes from attacks to SIDH by [8, 22, 26]. We use the following theorem, which is based on Kani's lemma [20].

Theorem 1 ([22, Theorem 1]). *Let d_1, d_2 be comprime integers, and $D = d_1 + d_2$. Let E, E_1, E_2, and F be elliptic curves of the following commutative diagram:*

$$\begin{array}{ccc} E & \xrightarrow{\psi_1} & E_1 \\ {\scriptstyle \psi_2}\downarrow & \searrow^{f} & \downarrow{\scriptstyle \psi_2'} \\ E_2 & \xrightarrow[\psi_1']{} & F \end{array}$$

where $f = \psi_2' \circ \psi_1 = \psi_1' \circ \psi_2$, $\deg(\psi_1) = \deg(\psi_1') = d_1$, and $\deg(\psi_2) = \deg(\psi_2') = d_2$. Then, the isogeny

$$\Phi = \begin{pmatrix} \psi_1 & \hat{\psi'}_2 \\ -\psi_2 & \hat{\psi}_1' \end{pmatrix} : E \times F \to E_1 \times E_2 \tag{1}$$

is a (D, D)-isogeny with respect to the natural product polarizations on $E \times F$ and $E_1 \times E_2$. In addition, the kernel of Φ is

$$\mathrm{Ker}(\Phi) = \{(d_1 P, f(P)) \in E \times F \mid P \in E[D]\}.$$

When we have $f(P)$ and $f(Q)$ for a basis (P, Q) of $E[D]$, we can construct $\mathrm{Ker}(\Phi)$. Thus, we can compute Φ up to an automorphism of the codomain $E_1 \times E_2$. If we assume $E_1 \not\cong E_2$, automorphisms of $E_1 \times E_2$ are the form of $\begin{pmatrix} \iota_1 & 0 \\ 0 & \iota_2 \end{pmatrix}$ for $\iota_1 \in \mathrm{Aut}(E_1)$ and $\iota_2 \in \mathrm{Aut}(E_2)$. Thus, from the data of $\mathrm{Ker}(\Phi)$, we can compute ψ_1, ψ_2, ψ_1', and ψ_2' up to the codomains.

Using Theorem 1, we have an algorithm `Kani` which plays a central role in our scheme. Let d_1, d_2, D be integers as in Theorem 1, and let $f : E \to F$ be an isogeny of degree $d_1 d_2$ between supersingular elliptic curves. Then, f is uniquely decomposed to the composition $\psi_1 : E \to E_1$ of degree d_1 and $\psi_2' : E_1 \to F$ of degree d_2 up to isomorphism.

$$E \overset{\psi_1}{\to} E_1 \overset{\psi_2'}{\to} F$$

In this setting, the algorithm `Kani` returns the following output from the input.

Input: Integers d_1, d_2, a basis $P, Q \in E[D]$, the images $f(P), f(Q) \in F[D]$; a finite subset $S \subset E$; a finite subset $T \subset F$.

Output: A supersingular elliptic curve E_1, the images of S under ψ_1, and the images of T under $\hat{\psi}'_2$ for some $\iota_1 \in \mathrm{Aut}(E_1)$.

The procedure for `Kani` is as follows.

1. Compute a (D, D)-isogeny Φ with kernel $\langle (d_1 P, f(P)), (d_1 Q, f(Q)) \rangle$.
2. If the codomain of Φ is not the product of elliptic curves, then return $\perp$.
3. Otherwise let $E'_1 \times E'_2$ be the codomain of Φ.
4. Let $P'_1 \in E'_1$ and $Q'_1 \in E'_1$ be first components of $\Phi((P, O_F))$ and $\Phi((Q, O_F))$.
5. Compute the D-Weil pairings $e_D(P, Q)$ and $e_D(P'_1, Q'_1)$.
6. If $e_D(P, Q)^d = e_D(P'_1, Q'_1)$ then return E'_1 and the first components of $\Phi((R_1, O_{E_2}))$ and $\Phi((O_{E_1}, R_2))$ for $R_1 \in S$ and $R_2 \in T$.
7. If $e_D(P, Q)^{D-d} = e_D(P'_1, Q'_1)$ then return E'_2 and the second components of $\Phi((R_1, O_{E_2}))$ and $\Phi((O_{E_1}, R_2))$ for $R_1 \in S$ and $R_2 \in T$.
8. Otherwise, return $\perp$.

In many cases, including this paper, we apply this algorithm for the case of $D = 2^e$ for an integer e, $D|(p+1)$, and E, F are over $\mathbb{F}_{p^2}$. Then, the computational cost is $O(e(\#S + \#T))$ operations on $\mathbb{F}_{p^2}$. We write this algorithm by

$$E_1; \psi_1(S); \hat{\psi}'_2(T) = \mathtt{Kani}_{d_1, d_2}(P, Q, f(P), f(Q); S; T).$$

2.5 Ideal-to-Isogeny Algorithm

Here, we introduce an algorithm for computing an isogeny $\varphi_I : E_0 \to E_I$ corresponding to a given left $\mathcal{O}_0$-ideal I. The most efficient algorithm currently known is Qlapoti [6]. Qlapoti was proposed to improve SQIsign-v2.0 and PRISM, and recently, qt-Pegasis [11], an improved version of PEGASIS [10] based on the same technique as Qlapoti, has also been proposed. In the construction of Δ-SQIsign, we make use of Qlapoti. Therefore, in this subsection, we give an overview of Qlapoti.

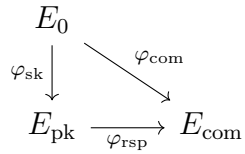
Let $p = 2^e f - 1$ be a prime for a sufficiently small integer f and let $\mathcal{O}_0$ be the maximal order of $\mathcal{B}_{p,\infty}$ with basis $(1, \mathbf{i}, \frac{\mathbf{i}+\mathbf{j}}{2}, \frac{1+\mathbf{k}}{2})$. Then, for a given left $\mathcal{O}_0$-ideal I, Qlapoti performs the following computations:

1. Find $\beta_1, \beta_2 \in I$ such that $q_I(\beta_1)$ and $q_I(\beta_2)$ are odd and satisfy
$$q_I(\beta_1) + q_I(\beta_2) = 2^e.$$
2. Let $I_1 = \chi_J(\beta_1)$ and $I_2 = \chi_J(\beta_2)$. Note that we have $n(I_1) + n(I_2) = 2^e$.
3. Compute φ_{I_1} (and φ_{I_2}) by applying `Kani` on the following diagram:
$$\begin{array}{ccc} E_0 & \longrightarrow & E \\ {\scriptstyle \varphi_{I_1}}\downarrow & \searrow^{\theta} & \downarrow \\ E_I & \xrightarrow[\hat{\varphi}_{I_2}]{} & E_0, \end{array}$$
where $\theta = \beta_2 \circ \hat{\beta}_1 \in \mathrm{End}(E_0)$.
4. Compute $\varphi_I = (q_I(\beta_1))^{-1} \varphi_{I_1} \circ \beta_1$ over $E_0[2^e]$ and return $\varphi_I|_{E_0[2^e]}$.

Note that the dominant computational cost of Qlapoti lies in the $(2^e, 2^e)$-isogeny computation performed in Step 3.

3 New Signature Scheme: Δ-SQIsign

In this section, we introduce our signature scheme, Δ-SQIsign. Our signature is constructed by applying the Fiat-Shamir transform [18] 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 $M_{\mathrm{chl}} \in \mathbb{Z}$, the prover computes an isogeny $\varphi_{\mathrm{rsp}} : E_{\mathrm{pk}} \to E_{\mathrm{com}}$ of degree M_{chl}.

First, in Section 3.1, we give a new algorithm named Δ-*KLPT*, which is used to compute the response isogeny φ_{rsp}. Second, in Section 3.2, we describe our Σ-protocol.

3.1 Δ-KLPT

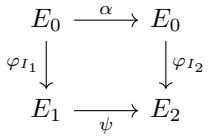
In this subsection, we introduce a new algorithm named Δ-*KLPT* (Algorithm 1), used in Δ-SQIsign. The input and output of this algorithm are roughly as follows.

Input: An integer M and two left $\mathcal{O}_0$-ideals I_1, I_2 of prime norm N such that $\gcd(M, N) = 1$ and $N \equiv 3 \pmod 4$.
Output: Connecting ideal J from $\mathcal{O}_R(I_1)$ to $\mathcal{O}_R(I_2)$ of norm M.

To build our algorithm, we first show the following lemma (Lemma 1).

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

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



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

Proof. (i) is equivalent to $\mathrm{Ker}(\varphi_{I_2} \circ \alpha) \supset \mathrm{Ker}(\varphi_{I_1})$. 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 $N = n(I_1) = \gcd(n(\alpha_1), N^2)$, 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). □

Our objective in this subsection is to find $\alpha \in \mathcal{O}_0$ of norm M satisfying condition (i), given M, I_1, and I_2. Then, the ideal $J = I_1^{-1}I_2\alpha$ corresponding to ψ is the correct output of Δ-KLPT. To do so, we first compute $(C_0 : D_0) \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ such that $\mu_0 = C_0\mathbf{j} + D_0\mathbf{k}$ satisfies condition (ii), that is equivalent to the following:

$$\alpha_2\mu_0\overline{\alpha_1} = C_0(\alpha_2\ \mathbf{j}\ \overline{\alpha_1}) + D_0(\alpha_2\ \mathbf{k}\ \overline{\alpha_1}) \equiv 0 \pmod{N\mathcal{O}_0}. \tag{2}$$

When $N \equiv 3 \pmod 4$, we can always find such $(C_0 : D_0)$, since it always holds that $N \nmid n(\mu_0)$. Then we use $\texttt{StrongApproximation}_M(N, C_0, D_0)$ to obtain $\alpha = m\mu_0 + N\mu_1$ of reduced norm M, where $m \in \mathbb{Z}$ and $\mu_1 \in \mathcal{O}_0$. To apply `StrongApproximation`, two conditions $M > pN^3$ and $\left(\frac{M}{N}\right) = \left(\frac{p(C_0^2+D_0^2)}{N}\right)$ have to be satisfied. If the later condition does not hold, by dividing M by 2 (here we assume $2|M$, $\left(\frac{2}{N}\right) = -1$, and $M/2 > pN^3$ in advance), the required condition holds. In this case, the reduced norm of α is also halved. We show the detail of Δ-`KLPT` in Algorithm 1. Note that our algorithm outputs $\alpha \in \mathcal{O}_0$ instead of the ideal $J = I_1^{-1}I_2\alpha$ since we use this α in the signing procedure. We also output a flag `is_M_halved` indicating whether M is halved.

In the GeneralizedKLPT, the size of the target norm M should be at least $O(p^3N^3)$. In contrast, in our Δ-KLPT, the size of M is reduced to $O(pN^3)$. Consequently, our algorithm can generate smaller signatures than those produced by GeneralizedKLPT.

Remark 1. If I_1 or I_2 is chosen uniformly at random among all left $\mathcal{O}_0$-ideals of norm N, then $(C_0 : D_0)$ satisfying condition (ii) is distributed uniformly over $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$. Therefore, the probability that M is halved is $1/2$.

3.2 Underlying Σ-Protocol

In this subsection, we introduce our new Σ-protocol.

Parameter setting. For the security parameter λ, the public parameter for Δ-SQIsign is as follows:

- A large prime $p = 2^{a+b}f - 1$ with $a \approx b \approx \lambda$ and $f \in \mathbb{N}$ as small as possible.
- An odd prime N such that $N \approx 2^\lambda$ and $N \equiv 3 \mod 8$.

Algorithm 1 Δ-$\texttt{KLPT}_M(I_1, I_2)$

Input: An integer M and two left $\mathcal{O}_0$-ideals I_1, I_2 of prime norm N such that M is even, $N \equiv 3 \mod 8$, $\gcd(M, N) = 1$, $M/2 > pN^3$.

Output: $\alpha \in \mathcal{O}_0$ such that $J = I_1^{-1} I_2 \alpha$ is a connecting ideal from $\mathcal{O}_R(I_1)$ to $\mathcal{O}_R(I_2)$ of norm M or $M/2$ and a flag `is_M_halved` indicating whether M is halved.

1: Let $\alpha_1, \alpha_2 \in \mathcal{O}_0$ such that $I_1 = \mathcal{O}_0\langle \alpha_1, N\rangle$ and $I_2 = \mathcal{O}_0\langle \alpha_2, N\rangle$.
2: Compute $(C_0 : D_0) \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ such that

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

3: **if** $\left(\frac{M}{N}\right) = \left(\frac{p(C_0^2+D_0^2)}{N}\right)$ **then**
4: $\quad M, \texttt{is_M_halved} \leftarrow M, \texttt{False}$.
5: **else**
6: $\quad M, \texttt{is_M_halved} \leftarrow \frac{M}{2}, \texttt{True}$.
7: **end if**
8: $\alpha \leftarrow \texttt{StrongApproximation}_M(N, C_0, D_0)$.
9: **return** $\alpha, \texttt{is_M_halved}$.

- An elliptic curve $E_0 : y^2 = x^3 + x$ over $\mathbb{F}_{p^2}$.
- A maximal order $\mathcal{O}_0 = \mathbb{Z}\langle 1, \mathbf{i}, \frac{\mathbf{i}+\mathbf{j}}{2}, \frac{1+\mathbf{k}}{2}\rangle$ of $B_{p,\infty}$. This order is isomorphic to $\mathrm{End}(E_0)$ and we identify $\mathrm{End}(E_0)$ with $\mathcal{O}_0$ via the isomorphism described in Section 2.3.
- A deterministic basis (P_0, Q_0) of $E_0[2^{a+b}]$ that is $\mathbb{F}_{p^2}$-rational.

Key generation. In the key generation step, we construct a random N-isogeny from E_0; $\varphi_{\mathrm{sk}} : E_0 \to E_{\mathrm{pk}}$. The procedure is based on the idea from QFESTA's algorithm [23, Algorithm 2].

1. Let e be the smallest integer satisfying $N < 2^e$ and let $e' = a + b - e$.
2. Compute $\alpha_{\mathrm{sk}} \in \mathcal{O}_0$ of reduced norm $N(2^e - N)2^{e'}$ by `FullRepresentInteger`.
3. Decompose α_{sk} to three isogenies:

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

   such that $\deg(\varphi_{\mathrm{sk}}) = N, \deg(\rho) = 2^e - N$, and $\deg(\psi) = 2^{e'}$.
4. Since $\mathrm{Ker}(\hat{\psi}) = \mathrm{Ker}(\widehat{\alpha_{\mathrm{sk}}})[2^{e'}]$, we can compute $\hat{\psi}$ and F. Thus, we compute $\hat{\psi} \circ \alpha_{\mathrm{sk}}(P_0) = \rho \circ \varphi_{\mathrm{sk}}(2^{e'} P_0)$, $\hat{\psi} \circ \alpha_{\mathrm{sk}}(Q_0) = \rho \circ \varphi_{\mathrm{sk}}(2^{e'} Q_0) \in F[2^e]$.
5. Compute $P_{\mathrm{pk}} := \varphi_{\mathrm{sk}}(P_0), Q_{\mathrm{pk}} := \varphi_{\mathrm{sk}}(Q_0) \in E_{\mathrm{pk}}[2^{a+b}]$ by `Kani`.
6. 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 $(P_{\mathrm{pk}}, Q_{\mathrm{pk}}, I_{\mathrm{sk}})$ as the secret key. An Algorithm 2 describes the key generation.

Commitment. The commitment procedure 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 $\texttt{com} = E_{\mathrm{com}}$ and $\texttt{sec} = (P_{\mathrm{com}}, Q_{\mathrm{com}}, I_{\mathrm{com}})$.

Algorithm 2 `KeyGen`

Input: $\texttt{param} = (p, a, b, N, E_0, \mathcal{O}_0)$.
Output: $\texttt{pk} = E_{\text{pk}}$, $\texttt{sk} = (P_{\text{pk}}, Q_{\text{pk}}, I_{\text{sk}})$.

1: Let e be the smallest integer satisfying $N < 2^e$ and let $e' = a + b - e$.
2: $\alpha_{\text{sk}} \coloneqq \texttt{FullRepresentInteger}_{\mathcal{O}_0}(N(2^e - N)2^{e'})$.
3: Compute a basis $K_{\hat{\psi}}$ of $\text{Ker}(\hat{\alpha_{\text{sk}}}) \cap E_0[2^{e'}]$.
4: Compute $P, Q = \hat{\psi} \circ \alpha_{\text{sk}}(P_0), \hat{\psi} \circ \alpha_{\text{sk}}(Q_0) \in F[2^e]$ under $\hat{\psi} : E_0 \to F = E_0/K_{\hat{\psi}}$.
   // $P = \rho \circ \varphi_{\text{sk}}(2^{e'}P_0),\ Q = \rho \circ \varphi_{\text{sk}}(2^{e'}Q_0)$.
5: $E_{\text{pk}}; P_{\text{pk}}, Q_{\text{pk}}; \emptyset \leftarrow \texttt{Kani}_{N, 2^e - N}(2^{e'}P_0, 2^{e'}Q_0, P, Q; P_0, Q_0; \emptyset)$.
   // $P_{\text{pk}} = \varphi_{\text{sk}}(P_0),\ Q_{\text{pk}} = \varphi_{\text{sk}}(Q_0)$.
6: Let $I_{\text{sk}} \coloneqq \mathcal{O}_0\langle \alpha_{\text{sk}}, N \rangle$.
7: **return** $\texttt{pk} = E_{\text{pk}}, \texttt{sk} = (P_{\text{pk}}, Q_{\text{pk}}, I_{\text{sk}})$.

Challenge. We let the challenge space $\mathcal{C} = (2^{a-2}, 2^{a-1})_2$, which is a set of odd integers within $(2^{a-2}, 2^{a-1})$. During the challenge phase, the verifier samples an integer $d_{\text{chl}} \xleftarrow{\$} \mathcal{C}$, and sets $\texttt{chl} = d_{\text{chl}}$. Against the challenge, we define the target degree M_{chl} as $M_{\text{chl}} \coloneqq 2^{a+2b} d_{\text{chl}}(2^a - d_{\text{chl}})$.

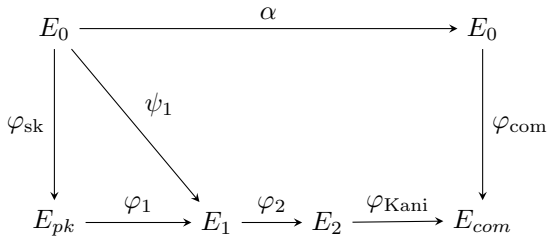
Response. The goal of the prover is to compute the isogeny $\varphi_{\text{rsp}} : E_{\text{pk}} \to E_{\text{com}}$ of degree M_{chl} or $M_{\text{chl}}/2$. To do so, we first compute

$$J, \texttt{is_M_halved} = \Delta\text{-}\texttt{KLPT}_{M_{\text{chl}}}(I_{\text{sk}}, I_{\text{com}}).$$

If `is_M_halved` is `False`, we have $n(J) = M_{\text{chl}}$, otherwise, we have $n(J) = M_{\text{chl}}/2$. Then, we compute the isogeny φ_{rsp} corresponding to J using Qlapoti.

Remark 2. In the above step, to use Δ-`KLPT`, it needs to be satisfied that $M_{\text{chl}}/2 = 2^{2a+b-1} d_{\text{chl}}(2^a - d_{\text{chl}}) > pN^3$. Since $p = 2^{a+b}f - 1$ and $2^{a-2} < d_{\text{chl}} < 2^{a-1}$, this condition holds provided that $3 \cdot 2^{2a+b-5} > fN^3$. Considering $a \approx b \approx \lambda$, this condition can be satisfied by choosing N to be slightly smaller than 2^λ.

Now we go into more detail. During the response phase, we utilize the following diagram:



In the above diagram, the horizontal composition below $\varphi_{\text{rsp}} \coloneqq \varphi_{\text{Kani}} \circ \varphi_2 \circ \varphi_1$ is the push-forward of α through φ_{sk} such that $\deg(\varphi_1) = 2^{a+b}$, $\deg(\varphi_2) = 2^b$ or 2^{b-1}, and $\deg(\varphi_{\text{Kani}}) = d_{\text{chl}}(2^a - d_{\text{chl}})$. The response is computed as follows.

1. Let $\alpha, \texttt{is_M_halved} \leftarrow \Delta\text{-}\texttt{KLPT}_{M_{\mathrm{chl}}}(I_{\mathrm{sk}}, I_{\mathrm{com}})$.
2. Let $b' = b$ if $\texttt{is_M_halved}$ is $\texttt{False}$, otherwise, let $b' = b - 1$.
3. Let $L = I_{\mathrm{com}} \cdot \alpha$, which corresponds to $\varphi_{\mathrm{rsp}} \circ \varphi_{\mathrm{sk}}$.
4. Let $L_1 = L + N2^{a+b}\mathcal{O}_0$, which corresponds to $\varphi_1 \circ \varphi_{\mathrm{sk}}$.
5. From φ_{sk} and L_1, compute a basis K_1 of $\ker \varphi_1$.
6. Find an equivalent ideal $L_1' = \chi_{L_1}(\beta)$ of L_1 of odd norm N_1' coprime to M_{chl}.
7. Compute the corresponding isogeny $\psi_1 : E_0 \to E_1$ of L_1' via Qlapoti.
8. Let $L' = L\dfrac{\bar{\beta}}{N2^{a+b}}$, which corresponds to $\varphi_{\mathrm{Kani}} \circ \varphi_2 \circ \psi_1$.
9. Let $L_2' = L' + N_1'2^{b'}\mathcal{O}_0$, which corresponds to $\varphi_2 \circ \psi_1$.
10. From ψ_1 and L_2', compute a basis K_2 of $\ker \varphi_2$.
11. Let s be an integer such that $K_2 = 2^a(P_1 + sQ_1)$ for a deterministic basis (P_1, Q_1) of $E_1[2^{a+b'}]$. (Swap P_1 and Q_1 if necessary.)
12. Let $\gamma = \dfrac{\alpha\bar{\beta}}{2^{a+b}} \in \mathcal{O}_0$, which corresponds to $\hat{\varphi}_{\mathrm{com}} \circ \varphi_{\mathrm{Kani}} \circ \varphi_2 \circ \psi_1$.
13. Compute $\varphi_{\mathrm{Kani}}|_{E_2[2^a]}$ using the following equation:

$$NN_1'\varphi_{\mathrm{Kani}} \circ \varphi_2 = \varphi_{\mathrm{com}} \circ \gamma \circ \hat{\psi}_1.$$

    More precisely, compute

$$U_{\mathrm{com}} = (NN_1')^{-1}\varphi_{\mathrm{com}}\circ\gamma\circ\hat{\psi}_1(P_1+sQ_1),\ V_{\mathrm{com}} = (NN_1')^{-1}\varphi_{\mathrm{com}}\circ\gamma\circ\hat{\psi}_1(2^{b'}Q_1).$$

    Then we have $U_{\mathrm{com}} = \varphi_{\mathrm{Kani}}(\varphi_2(P_1 + sQ_1)), V_{\mathrm{com}} = \varphi_{\mathrm{Kani}}(\varphi_2(2^{b'}Q_2))$, where $(\varphi_2(P_1 + sQ_1), \varphi_2(2^{b'}Q_1))$ is a basis of $E_2[2^a]$.
14. Finally, return $K_1 \in E_{\mathrm{pk}}[2^{a+b}], K_2 \in E_1[2^{b'}]$ and $U_{\mathrm{com}}, V_{\mathrm{com}} \in E_{\mathrm{com}}[2^a]$ as the response.

In Algorithm 3, we show the procedure of the response.

Verification. In the verification, we first compute a 2^{a+b}-isogeny $\varphi_1 : E_{\mathrm{pk}} \to E_1$ with kernel $\langle K_1 \rangle$ and let (P_1, Q_1) be a deterministic basis of $E_1[2^{a+b'}]$. Then we find an integer s such that $K_2 = 2^a(P_1 + sQ_2)$. (Swap P_1 and Q_1 if necessary.)

Next, we compute a $2^{b'}$-isogeny $\varphi_2 : E_1 \to E_2$ with kernel $\langle K_2 \rangle$ and let $P_2 = \varphi_2(P_1 + sQ_1)$ and $Q_2 = \varphi_2(2^{b'}Q_1)$. Now we have a basis (P_2, Q_2) of $E_2[2^a]$ and their images $(U_{\mathrm{com}}, V_{\mathrm{com}})$ under $\varphi_{\mathrm{Kani}} : E_2 \to E_{\mathrm{com}}$.

Next, we decompose $d_{\mathrm{chl}}(2^a - d_{\mathrm{chl}})$-isogeny $\varphi_{\mathrm{Kani}} : E_2 \to E_{\mathrm{com}}$ to

$$E_2 \xrightarrow{f} F \xrightarrow{f'} E_{\mathrm{com}}$$

of $\deg(f) \in \{d_{\mathrm{chl}}, 2^a - d_{\mathrm{chl}}\}$. Then we apply $\texttt{Kani}$ to this decomposition, and we have a $(2^a, 2^a)$-isogeny $\Phi : E_2 \times E_{\mathrm{com}} \to F \times F'$. We compute $(R, -) := \Phi((P_2, 0))$ and $(S, -) := \Phi((Q_2, 0))$, which holds that $R = f(P_2)$ and $S = f(Q_2)$. Hence, it holds

$$e_{2^a}^F(R, S) = e_{2^a}^F(f(P_2), f(Q_2)) = e_{2^a}^{E_2}(P_2, Q_2)^{\deg(f)}. \tag{3}$$

We finally confirm that one of the following equations holds:

$$e_{2^a}^F(R, S) = e_{2^a}^{E_2}(P_2, Q_2)^{d_{\mathrm{chl}}} \quad \text{or} \quad e_{2^a}^F(R, S) = e_{2^a}^{E_2}(P_2, Q_2)^{2^a - d_{\mathrm{chl}}}$$

which follows from equation (3). An Algorithm 4 describes the verification.

Algorithm 3 `Response`

Input: `param` $= (p, a, b, N, E_0, \mathcal{O}_0)$, `pk` $= E_{\mathrm{pk}}$, `sk` $= (P_{\mathrm{pk}}, Q_{\mathrm{pk}}, I_{\mathrm{sk}})$, `com` $= E_{\mathrm{com}}$, `sec` $= (P_{\mathrm{com}}, Q_{\mathrm{com}}, I_{\mathrm{com}})$, `chl` $= d_{\mathrm{chl}}$.
Output: `resp`$=(K_1, K_2, U_{\mathrm{com}}, V_{\mathrm{com}},$ `is_M_halved`$)$.

$M_{\mathrm{chl}} \leftarrow 2^{a+2b} d_{\mathrm{chl}}(2^a - d_{\mathrm{chl}})$.
$\alpha,$ `is_M_halved` $\leftarrow \Delta$-`KLPT`$_{M_{\mathrm{chl}}}(I_{\mathrm{sk}}, I_{\mathrm{com}})$.
if `is_M_halved` is `False` **then**
  $b' \leftarrow b$.
else
  $b' \leftarrow b - 1$.
end if
$L \leftarrow I_{\mathrm{com}} \cdot \alpha$.
$L_1 \leftarrow L + N2^{a+b}\mathcal{O}_0$.
Let $\alpha_1 \in \mathcal{O}_0$ such that $L_1 = \mathcal{O}_0\langle \alpha_1, N2^{a+b} \rangle$.
Let K_1 be a generator of $\langle \varphi_{\mathrm{sk}} \circ \hat{\alpha}_1(P_0), \varphi_{\mathrm{sk}} \circ \hat{\alpha}_1(Q_0) \rangle$.
Find an equivalent ideal $L_1' = \chi_{L_1}(\beta)$ of L_1 of odd norm N_1' coprime to M_{chl}.
Compute the corresponding isogeny $\psi_1 : E_0 \to E_1$ of L_1' via Qlapoti.
$L' \leftarrow L\dfrac{\bar{\beta}}{N2^{a+b}}$.
$L_2' \leftarrow L' + N_1' 2^{b'}$.
Let $\alpha_2 \in \mathcal{O}_0$ such that $L_2' = \mathcal{O}_0\langle \alpha_2, N_1' 2^{b'} \rangle$.
Let K_2 be a generator of $\langle \psi_1 \circ \hat{\alpha}_2(P_0), \psi_1 \circ \hat{\alpha}_2(Q_0) \rangle$.
Let s be an integer such that $K_2 = 2^a(P_1 + sQ_1)$ for a deterministic basis (P_1, Q_1) of $E_1[2^{a+b'}]$. (Swap P_1 and Q_1 if necessary.)
$\gamma \leftarrow \dfrac{\alpha\bar{\beta}}{2^{a+b}} \in \mathcal{O}_0$.
$U_{\mathrm{com}}, V_{\mathrm{com}} \leftarrow (NN_1')^{-1}\varphi_{\mathrm{com}} \circ \gamma \circ \hat{\psi}_1(P_1 + sQ_1), (NN_1')^{-1}\varphi_{\mathrm{com}} \circ \gamma \circ \hat{\psi}_1(2^{b'}Q_1)$.
return `resp` $= (K_1, K_2, U_{\mathrm{com}}, V_{\mathrm{com}},$ `is_M_halved`$)$.

4 Security Analysis

In this section, we give a security analysis on our signature scheme Δ-SQIsign. To ensure that our scheme 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 our Σ-protocol by Σ_Δ.

4.1 Special-Soundness

We show that Σ_Δ 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 2. *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.

Algorithm 4 `Verify`

Input: `param` $= (p, a, b, N, E_0, \mathcal{O}_0)$, `pk` $= E_{\mathrm{pk}}$, `com` $= E_{\mathrm{com}}$, `chl` $= d_{\mathrm{chl}}$. `resp` $= (K_1, K_2, U_{\mathrm{com}}, V_{\mathrm{com}}, \texttt{is_M_halved})$.
Output: accept or reject.

if `is_M_halved` is `False` **then**
  $b' \leftarrow b$.
else
  $b' \leftarrow b - 1$.
end if
Compute a 2^{a+b}-isogeny $\varphi_1 : E_{\mathrm{pk}} \to E_1$ with kernel $\langle K_1 \rangle$.
Let s be an integer such that $K_2 = 2^a(P_1 + sQ_1)$ for a deterministic basis (P_1, Q_1) of $E_1[2^{a+b'}]$. (Swap P_1 and Q_1 if necessary.)
Compute a $2^{b'}$-isogeny $\varphi_2 : E_1 \to E_2$ with kernel $\langle K_2 \rangle$ and let $P_2 \leftarrow \varphi_2(P_1 + sQ_1)$ and $Q_2 \leftarrow \varphi_2(2^{b'}Q_1)$.
$F; R, S; \emptyset \leftarrow \mathtt{Kani}_{d_{\mathrm{chl}}, 2^a - d_{\mathrm{chl}}}(P_2, Q_2, U_{\mathrm{com}}, V_{\mathrm{com}}; P_2, Q_2; \emptyset)$. If it fails, **return** reject.
$g := e_{2^a}(P_2, Q_2)$, $h := e_{2^a}(R, S)$.
if $h = g^{d_{\mathrm{chl}}}$ **or** $h = g^{-d_{\mathrm{chl}}}$ **then**
  return accept.
else
  return reject.
end if

(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:

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

Note that $\frac{m \pm n}{2}, \frac{x+y}{2} \in \mathbb{Z}$ since m, n, x, and y are odd. 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 $m, n \in (0, q)_q$ holds, 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

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

Here, we assume that $r \neq 1$. Then we have $(2m-q)^2 r - q^2 \geq 0$ from the above inequality. In addition, 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 an 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_Δ.

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 $d_{\mathrm{chl}} \neq d'_{\mathrm{chl}}$. Then rsp and rsp′ give efficient representations of two isogenies $\varphi_{\mathrm{rsp}} : E_{\mathrm{pk}} \to E_{\mathrm{com}}$ and $\varphi'_{\mathrm{rsp}} : E_{\mathrm{pk}} \to E_{\mathrm{com}}$ of degree $2^c d_{\mathrm{chl}}(2^a - d_{\mathrm{chl}})$ and $2^{c'} d'_{\mathrm{chl}}(2^a - d'_{\mathrm{chl}})$, where $c, c' \in \{a + 2b, a + 2b - 1\}$. Thus, we obtain an endomorphism $\alpha = \widehat{\varphi}'_{\mathrm{rsp}} \circ \varphi_{\mathrm{rsp}} \in \mathrm{End}(E_{\mathrm{pk}})$ of degree $2^{c+c'} d_{\mathrm{chl}}(2^a - d_{\mathrm{chl}}) d'_{\mathrm{chl}}(2^a - d'_{\mathrm{chl}})$. It is sufficient to show that this α is non-scalar.

Assume that α is a scalar, then $\deg \alpha = 2^{c+c'} d_{\mathrm{chl}}(2^a - d_{\mathrm{chl}}) d'_{\mathrm{chl}}(2^a - d'_{\mathrm{chl}})$ is the square of an integer. Since d_{chl} and d'_{chl} are odd, $c + c'$ should be even and $d_{\mathrm{chl}}(2^a - d_{\mathrm{chl}}) d'_{\mathrm{chl}}(2^a - d'_{\mathrm{chl}})$ is the square of an integer. Since $d_{\mathrm{chl}}, d'_{\mathrm{chl}} \in (2^{a-2}, 2^{a-1})_2 \subset (0, 2^a)_{2^a}$, from Lemma 2, 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_Δ 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. Let $c \xleftarrow{\$} \{a+2b, a+2b-1\}$ and let $M = 2^c d(2^a - d)$.
3. Sample a random M-isogeny $\varphi : E_{\mathrm{pk}} \to E$ uniformly among all M-isogenies from E_{pk}.
4. 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_Δ. 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 $(\mathtt{pk}, \mathtt{sk}) \leftarrow \mathtt{KeyGen}(1^\lambda)$, $(\mathtt{com}_i, \mathtt{sec}_i) \leftarrow \mathtt{Commit}(\mathtt{pk}, \mathtt{sk})$, $\mathtt{chl}_i \xleftarrow{\$} \mathcal{C}$, $\varphi_i \leftarrow \mathtt{Response}(\mathtt{pk}, \mathtt{sk}, \mathtt{com}_i, \mathtt{sec}_i, \mathtt{chl}_i)$ 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.

4.3 Hardness Analysis

We denote the codomain of φ_i given in Problem 1 by E_i for $i \in \{1, \ldots, q\}$. First, we focus on the distribution of E_i to distinguish $\mathcal{D}_0$ and $\mathcal{D}_1$. In $\mathcal{D}_0$, E_i is computed via Algorithm 2, which is a variant of QFESTA's Algorithm [23, Algorithm 2]. The distribution of such E_i does not seem to be uniform; however, there is no known efficient method to distinguish this distribution from a uniform distribution. In [23], they propose a heuristic which suggests that the output distribution of [23, Algorithm 2] is computationally indistinguishable from uniform. In contrast, E_i in $\mathcal{D}_1$ is the codomain of an isogeny uniformly chosen among isogenies of degree $2^c d(2^a - d)$ from E_{pk}. It is known that when

the degree of the isogeny is sufficiently large, the distribution of its codomain becomes statistically uniform. Therefore, it can be assumed that the distribution of E_i is statistically uniform in both $\mathcal{D}_0$ and $\mathcal{D}_1$.

Next, we consider the distribution of φ_i. In $\mathcal{D}_0$, φ_i is the push-forward, via φ_{sk}, of an endomorphism α of E_0 of degree $2^c d(2^a - d)$, which is computed by Δ-KLPT, whereas in $\mathcal{D}_1$, φ_i is uniform among isogenies of degree $2^c d(2^a - d)$ from E_{pk}. Here, φ_i in $\mathcal{D}_1$ can be considered as the push-forward via φ_{sk} of an isogeny $\alpha : E_0 \to *$ uniformly chosen among isogenies of degree $2^c d(2^a - d)$ from E_0. Thus, we can regard our problem as a problem of distinguishing the distribution of $[\varphi_{\mathrm{sk}}]_*\alpha$, where α is chosen from a limited set of isogenies or from all isogenies of fixed degree from E_0. This problem is similar to [14, Problem 2], whose hardness is assumed to prove the zero-knowledge property of SQIsign-v1.0. Therefore, similar to the discussion in [14], it seems that there is no strategy that is superior to a direct key recovery, computing φ_{sk} from the knowledge of E_{pk} (or computing φ_{com} from the knowledge of E_{com}).

Finally, we consider the hardness of a direct key recovery attack to find φ_{sk} between E_0 and E_{pk}. Since the degree N of φ_{sk} is a prime number, a meet-in-the-middle attack is not more effective than an exhaustive search attack on N-isogenies from E_0. Since the number of N-isogenies from E_0 is $O(N)$, the exhaustive search requires a computational cost of $O(N)$. In our setting, we have $N = O(2^\lambda)$. Therefore, the cost of the exhaustive search is $O(2^\lambda)$.

5 Efficiency

In this section, we analyze the efficiency of Δ-SQIsign. First, we provide concrete parameters for NIST security levels I, III, and V. Second, we evaluate the signature sizes and compare them with other protocols. Finally, we evaluate and compare the computational costs.

5.1 Parameters

In this subsection, we specify the concrete parameters for the NIST security levels I, III, and V. It is required that $p \approx 2^{2\lambda}$, $3 \cdot 2^{2a+b-5} > fN^3$, and $N \equiv 3 \bmod 8$. Table 1 lists the concrete parameters a, b, p, and N. Note that the choices of p follow SQIsign-v2.0 [1, Section 5.2].

5.2 Public key and signature sizes

In this subsection, we analyze the public key and signature sizes of Δ-SQIsign and compare them with other protocols. The main results are presented in Table 2.

Public key sizes. The public key of Δ-SQIsign is an elliptic curve E_{pk}. Since we represent elliptic curves in Montgomery model, the curve is described by a single element of $\mathbb{F}_{p^2}$. In addition, to optimize the generation of a deterministic

Table 1. Parameters and public key and signature sizes (in bytes) for each NIST security level.

Δ-SQIsign	a	b	$p = 2^{a+b} \cdot f - 1$	N	Public key (bytes)	Signature (bytes)
NIST I	128	120	$2^{248} \cdot 5 - 1$	$2^{118} - 5$	66	177
NIST III	192	184	$2^{376} \cdot 65 - 1$	$2^{182} - 413$	98	265
NIST V	256	244	$2^{500} \cdot 27 - 1$	$2^{242} - 1077$	130	352

Table 2. Public key and signature sizes (in bytes) comparison for the NIST security level I

Protocol (NIST I)	Public key	Signature
SQIsign-v2.0	65	148
PRISM	66	189
SQIsign2D-East	66	164
Δ-SQIsign	**66**	**177**

basis of $E_{\mathrm{pk}}[2^{a+b}]$, we include a hint requiring 2 bytes. For details on this hint, we refer to the SQIsign-v2.0 specification [1, Section 2.2.3]. In summary, the public key size is $(\lceil \log_2(p^2) \rceil + 16)$ bits. Since $p \approx 2^{2\lambda}$, this is approximately 4λ bits. Table 1 reports the concrete public key sizes in bytes. We compare the public key sizes in bytes with those of other protocols in Table 2, and observe that the public key size of our protocol is comparable to the other protocols.

Signature sizes. The signature of Δ-SQIsign consists of E_{com}, $K_1 \in E_{\mathrm{pk}}[2^{a+b}]$, $K_2 \in E_1[2^{b'}]$, $U_{\mathrm{com}}, V_{\mathrm{com}} \in E_{\mathrm{com}}[2^a]$, and a boolean `is_M_haved`. We can represent E_{com} by its Montgomery coefficient, which is an element of $\mathbb{F}_{p^2}$. We can represent four points $K_1, K_2, U_{\mathrm{com}}, V_{\mathrm{com}}$ by the coefficients for each deterministic torsion basis. More precisely, we represent K_1 by $s_1 \in \mathbb{Z}/2^{a+b}\mathbb{Z}$ such that $K_1 = P_{\mathrm{pk}} + s_1 Q_{\mathrm{pk}}$ (or $K_1 = Q_{\mathrm{pk}} + s_1 P_{\mathrm{pk}}$) for a deterministic basis $(P_{\mathrm{pk}}, Q_{\mathrm{pk}})$ of $E_{\mathrm{pk}}[2^{a+b}]$ and K_2 by $s_2 \in \mathbb{Z}/2^{b'}\mathbb{Z}$ such that $K_2 = 2^a(P_1 + s_2 Q_1)$ (or $K_2 = 2^a(Q_1 + s_2 P_1)$) for a deterministic basis (P_1, Q_1) of $E_1[2^{a+b'}]$. Furthermore, we additionally require one bit indicating whether P_{pk} and Q_{pk} are swapped, and one bit indicating whether P_1 and Q_1 are swapped when representing K_1 and K_2. As for $U_{\mathrm{com}}, V_{\mathrm{com}} \in E_{\mathrm{com}}[2^a]$, we represent them by four elements of $\mathbb{Z}/2^a\mathbb{Z}$, which are coefficients for a deterministic basis of $E_{\mathrm{com}}[2^a]$.

In summary, the signature requires $2\lceil \log_2 p \rceil$ bits for E_{com}, $a + b + 1$ bits for K_1, $b' + 1$ bits for K_2, $4a$ bits for $U_{\mathrm{com}}, V_{\mathrm{com}}$, and 1 bit for `is_M_haved`. Approximately, the signature size is 11λ bits since $p \approx 2^{2\lambda}$ and $a \approx b \approx \lambda$. Table 1 shows the signature size in bytes for each security level. As shown in Table 2, for instance, the signature size in bytes is approximately 1.2 times larger than that of SQIsign-v2.0.

Table 3. Number of isogeny computation of each degree for NIST security level I. Parenthesized values denote cases where the numbers may differ slightly.

Protocol (NIST I)		2	3	(2,2)
SQIsign-v2.0 (& Qlapoti)	**keygen**	-	-	246
	sign	(248)	-	622
	verify	(248)	-	(126)
PRISM (& Qlapoti)	**keygen**	-	-	248
	sign	-	-	248
	verify	-	-	248
SQIsign2D-East	**keygen**	-	-	253
	sign	126	(2)	760
	verify	126	(2)	127
Δ-SQIsign	**keygen**	**130**	-	**118**
	sign	**130**	-	**366**
	verify	(**368**)	-	**128**

5.3 Computational Cost

In this subsection, we count and compare the number of isogeny computations of dimension 1 and 2. In the protocol of Δ-SQIsign, we only compute 2-isogenies and (2,2)-isogenies. Let e be the smallest integer satisfying $N < 2^e$ and let $e' = a + b - e$. First, during the key generation phase, we perform e' computations of 2-isogenies and e computations of $(2, 2)$-isogenies. Second, during the signing, we perform e' computations of 2-isogenies and $(e + a + b)$ computations of $(2, 2)$-isogenies. Last, during the verification, we perform $a + 2b$ (or $a + 2b - 1$) computations of 2-isogenies and a computations of $(2, 2)$-isogenies.

Table 3 shows the numbers of 2-isogeny and $(2, 2)$-isogeny computations required at each step of the protocols for NIST security level I. For SQIsign-v2.0 and PRISM, as remarked in Section 2.5, the computational cost can be reduced, compared to the original ones, by using the Qlapoti algorithm [7]. Table 3 shows the cost when using Qlapoti.

Based on Table 3, we compare the computational costs with those of other protocols. For the signing, the number of $(2, 2)$-isogeny computations in Δ-SQIsign is, for instance, about 60% of that in SQIsign-v2.0. The number of 2-isogeny computations, which are less costly than $(2, 2)$-isogeny computations, is also smaller than SQIsign-v2.0. Therefore, the signing cost of Δ-SQIsign is expected to be smaller than that of SQIsign-v2.0. For the verification, the number of $(2, 2)$-isogeny computations in Δ-SQIsign is only slightly larger than SQIsign-v2.0 and SQIsign2D-East, but smaller than PRISM. However, the number of 2-isogeny computations is the largest, being about 1.5 times compared to SQIsign-v2.0.

In addition, we provide a proof-of-concept implementation of Δ-SQIsign in SageMath [27]. Our implementation is available at https://github.com/

Table 4. The average execution time (in seconds) over 100 runs for each implementation in SageMath.

Δ-SQIsign	**keygen**	**sign**	**verify**
NIST I	1.51	6.16	0.87
NIST III	4.81	18.78	2.58
NIST V	9.66	27.67	5.01

Yoshizumi-Ryo/Delta-SQIsign-sage. Table 4 shows the average execution time in seconds for each step over 100 runs. All experiments were conducted on a MacBook Air (M4), with 8 GB unified memory, running macOS 26.0.1, using Python 3.13.2 and SageMath 10.7. An optimized implementation in C is left for future work.

6 Conclusion

In this paper, we introduce a new isogeny-based signature scheme named Δ-SQIsign by using our new algorithm Δ-KLPT. We prove that Δ-SQIsign is EUF-CMA secure under the hardness of the one-endomorphism problem, using the hint-assisted wHVZK framework. Regarding efficiency, signing cost is expected to be smaller than that of the SQIsign-v2.0 combined with the Qlapoti algorithm, although it remains less efficient than PRISM. For verification, while it is slightly less efficient than SQIsign-v2.0, it outperforms PRISM. Finally, we provide a proof-of-concept implementation in SageMath, and leave an optimized C implementation for future work.

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, 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.

4. 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.
5. 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.
6. Giacomo Borin, Maria Corte-Real Santos, Jonathan Komada Eriksen, Riccardo Invernizzi, Marzio Mula, Sina Schaeffler, and Frederik Vercauteren. Qlapoti: Simple and efficient translation of quaternion ideals to isogenies. In Goichiro Hanaoka and Bo-Yin Yang, editors, *ASIACRYPT 2025, Part IV*, volume 16248 of *LNCS*, pages 174–205. Springer, Singapore, December 2025.
7. Giacomo Borin, Maria Corte-Real Santos, Jonathan Komada Eriksen, Riccardo Invernizzi, Marzio Mula, Sina Schaeffler, and Frederik Vercauteren. Qlapoti: Simple and Efficient Translation of Quaternion Ideals to Isogenies. *Cryptology ePrint Archive, Report 2025/1604*, 2025.
8. 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.
9. 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.
10. Pierrick Dartois, Jonathan Komada Eriksen, Tako Boris Fouotsa, Arthur Herlédan Le Merdy, Riccardo Invernizzi, Damien Robert, Ryan Rueger, Frederik Vercauteren, and Benjamin Wesolowski. PEGASIS: Practical effective class group action using 4-dimensional isogenies. In Yael Tauman Kalai and Seny F. Kamara, editors, *CRYPTO 2025, Part I*, volume 16000 of *LNCS*, pages 67–99. Springer, Cham, August 2025.
11. Pierrick Dartois, Jonathan Komada Eriksen, Riccardo Invernizzi, and Frederik Vercauteren. qt-pegasis: Simpler and faster effective class group actions. Cryptology ePrint Archive, Report 2025/1859, 2025.
12. 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.
13. 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.
14. 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.
15. 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.
16. Max Deuring. Die typen der multiplikatorenringe elliptischer funktionenkörper. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 14:197–272, 1941.
17. 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.
18. 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.
19. 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.
20. Ernst Kani. The number of curves of genus two with elliptic differentials. *Journal für die reine und angewandte Mathematik*, 1997(485):93–122, 1997.
21. David Kohel, Kristin Lauter, Christophe Petit, and Jean-Pierre Tignol. On the quaternion-isogeny path problem. *LMS Journal of Computation and Mathematics*, 17(A):418–432, 2014.
22. 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.
23. 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.
24. 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.
25. Christophe Petit and Spike Smith. An improvement to the quaternion analogue of the ℓ-isogeny path problem, 2018. Conference talk at MathCrypt.
26. 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.
27. W. A. Stein et al. *Sage Mathematics Software (Version 10.5)*. The Sage Development Team, 2024. `http://www.sagemath.org`.
28. Jacques Vélu. Isogénies entre courbes elliptiques. *Comptes-Rendus de l'Académie des Sciences*, 273:238–241, 1971.
29. Zheng Xu, Kaizhan Lin, Chang-An Zhao, and Yi Ouyang. SQIsign2D^2: New SQIsign2D variant by leveraging power smooth isogenies in dimension one. In Goichiro Hanaoka and Bo-Yin Yang, editors, *ASIACRYPT 2025, Part IV*, volume 16248 of *LNCS*, pages 341–371. Springer, Singapore, December 2025.