New Ring Signatures From Quaternions and Isogenies

Kohei Nakagawa, Noboru Kunihiro

University of Tsukuba, Japan

Abstract. Ring signatures allow a user to sign a message on behalf of a set of public keys while hiding which member produced the signature. Constructing efficient ring signatures from post-quantum assumptions is an important problem. Among isogeny-based signatures, SQIsign has attracted significant attention due to its extremely compact signature size. Recently, a ring signature scheme called Erebor, based on the Round 1 version of SQIsign (referred to as SQIsign1.0, in contrast to SQIsign2.0 from Round 2), was proposed by Borin, Lai, and Leroux. Their construction modifies the underlying Σ-protocol of SQIsign1.0 to achieve special HVZK, and then applies the AOS framework, which transforms special HVZK Σ-protocols into ring signatures. In this paper, we first construct a new Σ-protocol that satisfies special HVZK, and then apply the AOS framework to obtain a new ring signature scheme. Compared to Erebor, our ring signature achieves lower computational costs for both signing and verification.

Keywords: Ring signature, Isogeny, Quaternion, SQIsign

1 Introduction

Ring Signatures. Ring signatures, introduced by Rivest, Shamir, and Tauman [29], allow a user to sign a message on behalf of a set of public keys while hiding which member of the set produced the signature. Unlike group signatures, ring signatures do not require any trusted setup or group manager. Today, ring signatures are widely used in a variety of applications such as electronic voting systems [22] and blockchain technologies [17,26]. In electronic voting systems, they help ensure voter privacy while preserving the integrity of the election process. In blockchain technologies, they play a key role in enabling confidential transactions by hiding the identity of the transaction initiator.

Numerous ring signature schemes based on classical assumptions have been proposed [3,7,19,29,32]. However, with the emergence of quantum computers, constructing ring signatures based on post-quantum assumptions has become an important research direction. As a result, various post-quantum ring signature schemes have been proposed [5,6,10,18,20,23,32].

Isogeny-Based Signatures. Isogeny-based cryptography is a promising candidate for post-quantum cryptography due to its compact public keys and signatures. 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 [11].

Recent works have introduced more efficient constructions by exploiting higher-dimensional isogeny techniques such as SQIsignHD [12], SQIsign2D-West [4], SQIsign2D-East [24], SQIPrime [16], SQIsign2D^2 [31], and SQIsign [1] in the NIST competition Round 2. (For clarity, we refer to the Round 1 version of SQIsign as SQIsign1.0 and the Round 2 version as SQIsign2.0 hereafter.) These schemes achieve significant performance improvements by utilizing isogenies of non-smooth degrees. However, this design choice complicates the analysis of the underlying Σ-protocols. In particular, constructing a simulator that generates transcripts without using secret key becomes difficult, and honest-verifier zero-knowledge is typically proven only in the presence of special oracles or hint distributions.

Ring Signatures from Isogenies. A natural approach to constructing ring signatures is to apply a general transformation such as AOS framework [3] on Σ-protocols. However, to apply AOS framework, the Σ-protocol must satisfy special HVZK, which means the existance of a PPT simulator that generates transcripts from a public key and a challenge. Therefore, recent Σ-protocols relying on non-smooth degree isogenies cannot apply this transformation.

On the other hand, the Σ-protocol underlying SQIsign1.0 [11] satisfies this property because it relies on smooth-degree isogenies and admits an explicit simulator. Based on this fact, Borin et. al. proposed a ring signature scheme named 'Erebor' [10] constructed from isogenies and quaternion algebras by applying AOS framework on the SQIsign1.0 Σ-protocol. Their construction achieves full anonymity, but its efficiency is tied to the underlying SQIsign1.0 protocol, leaving room for improvements in the computational cost.

In this work, we design a new isogeny-based Σ-protocol that improves the computational cost of SQIsign1.0 while preserving special HVZK. Using this protocol, we construct a new ring signature scheme with improved computational cost.

1.1 Contributions

Our main contributions are summarized as follows.

- **A new isogeny-based Σ-protocol.** We propose a new isogeny-based Σ-protocol. Compared with the Σ-protocol underlying SQIsign1.0, our protocol achieves faster simulator and verification. It leads the improved computational efficiency.
- **Efficient response computation using Δ-KLPT.** The response of our protocol involves computing a smooth-degree isogeny satisfying a torsion image condition. To keep the degree of this isogeny small, we use a recently

proposed algorithm called Δ-KLPT [25, Algorithm 1]. Our construction is similar to recent techniques based on level structures. However, our approach differs from these approaches in that it controls the image of a single point, whereas they control the images of two torsion points.

– **A new isogeny-based ring signature scheme.** By applying the AOS framework [3] on our new Σ-protocols, we obtain a new ring signature scheme.
– **Improved efficiency over existing constructions.** Compared with the Erebor [10] derived from SQIsign1.0, our scheme achieves improved computational efficiency for signing and verification while our signature size is a bit larger than that of Erebor.

1.2 Technical Overview

We briefly describe the main ideas behind our construction.

Let E_0 be a fixed supersingular elliptic curve. In the key generation algorithm, the secret key is an isogeny

$$\varphi_{\mathrm{sk}} : E_0 \to E_{\mathrm{pk}}$$

of prime degree N_{sk}. Similarly, in the commitment phase the prover samples another isogeny of the same degree N_{sk}:

$$\varphi_{\mathrm{com}} : E_0 \to E_{\mathrm{com}}.$$

The verifier generates a challenge representing an N_{chl}-torsion point

$$R_{\mathsf{com}} \in E_{\mathsf{com}}[N_{\mathsf{chl}}].$$

To compute the response, the prover deterministically derives a torsion point

$$P_{\mathsf{pk}} \in E_{\mathsf{pk}}[N_{\mathsf{chl}}]$$

and computes a smooth-degree isogeny $\varphi_{\mathrm{rsp}} : E_{\mathsf{pk}} \to E_{\mathsf{com}}$ such that

$$\varphi_{\mathsf{rsp}}(P_{\mathsf{pk}}) \in \langle R_{\mathsf{com}} \rangle.$$

The verifier checks that the response isogeny satisfies the above condition. In order to keep the degree of φ_{rsp} small and smooth, we employ a technique similar to a recent algorithm named Δ-KLPT [25, Algorithm 1], which allows us to construct the required degree isogeny between E_{pk} and E_{com} when $\deg \varphi_{\mathsf{sk}} = \deg \varphi_{\mathsf{com}}$.

Our Σ-protocol admits a simulator that generates valid transcripts from a public key and a challenge. This property enables the use of a standard transformation from Σ-protocols to ring signatures. Applying this transformation yields an isogeny-based ring signature scheme with improved efficiency compared to previous constructions based on SQIsign1.0.

1.3 Related Work

Our approach to specifying the image of a point under an isogeny as the challenge in the Σ-protocol is similar to the level structure technique used in the recently proposed SQInstructor [9]. However, while the level structure approach handles a torsion basis (i.e., two points), our method relies on a single point. Whether the level structure technique can be incorporated into our Σ-protocol construction remains an interesting direction for future work.

1.4 Organization

The remainder of this paper is organized as follows. Section 2 reviews the necessary background on supersingular isogenies and quaternion ideals. Section 3 presents our new isogeny-based Σ-protocol and the resulting ring signature scheme obtained via a standard transformation. Section 4 analyzes the security of the proposed scheme. Section 5 discusses efficiency aspects and compares our scheme with existing constructions. Finally, Section 6 concludes the 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. For a positive integer N, we define $[N] := \{1, \ldots, N\}$.

2.2 Σ-Protocol and Ring Signature

Σ-Protocols A Σ-protocol is a three-round interactive proof system between a prover $\mathcal{P}$ and a verifier $\mathcal{V}$ for a relation $\mathcal{R}$.

Let $\mathcal{R} \subseteq \mathcal{X} \times \mathcal{W}$ be an NP relation. For $(x, w) \in \mathcal{R}$, x is called the *statement* and w is the corresponding *witness*. A Σ-protocol for $\mathcal{R}$ consists of four algorithms $(\mathsf{Gen}, \mathsf{P}_1, \mathsf{P}_2, \mathsf{V})$ and a challenge space $\mathcal{C}$ executed as follows.

- **Key generation.** The prover $\mathcal{P}$ generates a valid relation $(x, w) \leftarrow \mathsf{Gen}(1^\lambda)$ and publishes x.
- **Commitment.** The prover $\mathcal{P}$ on input (x, w) runs $\mathsf{P}_1(x, w)$ to generate a commitment com and internal state st, and sends com to the verifier.
- **Challenge.** The verifier samples a random challenge $\mathsf{chl} \xleftarrow{\$} \mathcal{C}$ from a challenge space $\mathcal{C}$ and sends chl to the prover.

- **Response.** The prover computes $\mathsf{rsp} \leftarrow \mathsf{P}_2(x, w, \mathsf{st}, \mathsf{chl})$ and sends rsp to the verifier.
- **Verify.** The verifier accepts if $\mathsf{V}(x, \mathsf{com}, \mathsf{chl}, \mathsf{rsp}) = 1$.

In addition, a Σ-protocol must satisfy the following properties.

Correctness. A Σ-protocol is said to be *correct* if for all $(x, w) \in \mathcal{R}$, an honest execution between $\mathcal{P}(x, w)$ and $\mathcal{V}(x)$ is accepted with probability 1.

Special Soundness. A Σ-protocol is said to be *special sound* if there exists a polynomial-time extractor $\mathcal{E}$ such that given two accepting transcripts

$$(\mathsf{com}, \mathsf{chl}, \mathsf{rsp}), \quad (\mathsf{com}, \mathsf{chl}', \mathsf{rsp}')$$

with $\mathsf{chl} \neq \mathsf{chl}'$, the extractor outputs a witness

$$w \leftarrow \mathcal{E}(x, \mathsf{com}, \mathsf{chl}, \mathsf{rsp}, \mathsf{chl}', \mathsf{rsp}')$$

such that $(x, w) \in \mathcal{R}$.

Honest-Verifier Zero-Knowledge (HVZK). A Σ-protocol is said to be *honest-verifier zero-knowledge (HVZK)* if there exists a probabilistic polynomial-time simulator $\mathcal{S}$ that on input x outputs transcripts $(\mathsf{com}, \mathsf{chl}, \mathsf{rsp})$ whose distribution is computationally indistinguishable from the transcripts generated by an honest interaction between $\mathcal{P}(x, w)$ and an honest verifier $\mathcal{V}(x)$.

Furthermore, a Σ-protocol is said to be *special HVZK* if there exists a simulator $\mathcal{S}$ which additionally takes chl as input and outputs $(\mathsf{com}, \mathsf{rsp})$ such that $(\mathsf{com}, \mathsf{chl}, \mathsf{rsp})$ is indistinguishable from the real transcripts.

Ring Signatures A ring signature scheme allows a signer to anonymously sign a message on behalf of a set of public keys called a *ring*. The verifier is convinced that the signature was produced by one of the ring members but cannot identify which one. A ring signature scheme consists of the following algorithms.

- $\mathsf{KeyGen}(1^\lambda) \to (\mathsf{pk}, \mathsf{sk})$: Generates a public/secret key pair.
- $\mathsf{Sign}(\mathsf{sk}_i, m, R) \to \sigma$: Given a secret key sk_i corresponding to a public key pk_i, a message m, and a ring $R = \{\mathsf{pk}_1, \ldots, \mathsf{pk}_N\}$ containing pk_i, outputs a ring signature σ.
- $\mathsf{Verify}(m, R, \sigma) \to \{0, 1\}$: Outputs 1 if σ is a valid signature on message m with respect to ring R.

In addition, a ring signature must satisfy the following properties.

Correctness. A ring signature scheme is said to be *correct* if for all $(\mathsf{pk}_i, \mathsf{sk}_i)$ generated by KeyGen, all messages m, and all rings R containing pk_i, it holds

$$\Pr[\mathsf{Verify}(m, R, \sigma) = 1] = 1$$

where $\sigma \leftarrow \mathsf{Sign}(\mathsf{sk}_i, m, R)$.

Unforgeability. A ring signature scheme is said to be *unforgeable with respect to insider corruption* if any probabilistic polynomial-time adversary $\mathcal{A}$ has negligible probability of winning the following game played against a challenger.

1. The challenger generates key pairs $(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{KeyGen}(1^\lambda; \mathsf{r}_i)$ for $i \in [N]$ using random coin r_i and sends $\mathsf{PK} = \{\mathsf{pk}_i\}_{i\in[N]}$ to $\mathcal{A}$.
2. The challenger initializes two empty sets S and C.
3. The adversary $\mathcal{A}$ can access to the following two oracles an arbitrary polynomial number of times:
   - $\mathsf{OSign}(i, m, R)$: If $\mathsf{pk}_i \in R$, it returns $\sigma \leftarrow \mathsf{Sign}(\mathsf{sk}_i, m, R)$ and adds (i, m, R) to S.
   - $\mathsf{OCorrupt}(i)$: It returns r_i and adds pk_i to C.
4. The adversary $\mathcal{A}$ outputs (m^*, R^*, σ^*). If $R^* \subset \mathsf{PK} \setminus C$, $(-, m^*, R^*) \notin S$, and $\mathsf{Verify}(m^*, R^*, \sigma^*) = 1$, $\mathcal{A}$ wins the game.

Anonymity. A ring signature scheme is said to be anonymous if any probabilistic polynomial-time adversary $\mathcal{A}$ has negligible advantage in the following game played against a challenger.

1. The challenger generates key pairs $(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{KeyGen}(1^\lambda; \mathsf{r}_i)$ for $i \in [N]$ using random coin r_i and sends $\mathsf{PK} = \{\mathsf{pk}_i\}_{i\in[N]}$ to $\mathcal{A}$.
2. The challenger samples a random bit $b \xleftarrow{\$} \{0, 1\}$.
3. The adversary $\mathcal{A}$ outputs (i_0, i_1, m, R) such that $\mathsf{pk}_{i_0}, \mathsf{pk}_{i_1} \in R$.
4. The challenger computes $\sigma^* \leftarrow \mathsf{Sign}(\mathsf{sk}_{i_b}, m, R)$ and sends σ^* to $\mathcal{A}$.
5. The adversary $\mathcal{A}$ outputs b^*. The advantage of $\mathcal{A}$ is defined as

$$\mathsf{Adv}(\mathcal{A}) := \left| \Pr[b^* = b] - \frac{1}{2} \right|.$$

In addition, a ring signature is said to be *full* anonymous if any probabilistic polynomial-time adversary $\mathcal{A}$ still has negligible advantage in this game where the challenger sends also $\{\mathsf{r}_i\}_{i\in[N]}$ to $\mathcal{A}$ in Step 1.

Ring Signatures from Σ-Protocols Ring signatures can be constructed from Σ-protocols using AOS sequential OR-proofs [3]. Suppose we have a special sound and special HVZK Σ-protocol for a relation $\mathcal{R}$ with a simulator $\mathcal{S}$.

Let $(\mathsf{pk}_i, \mathsf{sk}_i) := (x_i, w_i) \in \mathcal{R}$ for $i \in [N]$ and let $R = \{\mathsf{pk}_i\}_{i\in[N]}$ be a ring of public keys. Then we obtain a ring signature from the Σ-protocol as follows.

$\mathsf{Sign}(\mathsf{sk}_i, m, R) \to \sigma$:

1. The signer computes the commitment:

$$(\mathsf{com}_i, \mathsf{st}_i) \leftarrow \mathsf{P}_1(\mathsf{pk}_i, \mathsf{sk}_i).$$

2. For $j = i+1, \ldots, N, 1, \ldots, i-1$, the signer sequentially generates transcripts $(\mathsf{com}_j, \mathsf{chl}_j, \mathsf{rsp}_j)$ by using a hash function $H : \{0,1\}^* \to \mathcal{C}$ and the simulator $\mathcal{S}$ as follows:

$$\mathsf{chl}_j \leftarrow H(m||\mathsf{com}_{j-1})$$
$$(\mathsf{com}_j, \mathsf{rsp}_j) \leftarrow \mathcal{S}(\mathsf{pk}_j, \mathsf{chl}_j)$$

3. The signer generates a challenge by using the hash function:

$$\mathsf{chl}_i \leftarrow H(m||\mathsf{com}_{i-1}).$$

4. The signer computes the response:

$$\mathsf{rsp}_i \leftarrow \mathsf{P}_2(\mathsf{pk}_i, \mathsf{sk}_i, \mathsf{st}_i, \mathsf{chl}_i).$$

5. The signature is

$$\sigma = (\mathsf{chl}_1, \mathsf{com}_1, \ldots, \mathsf{com}_N, \mathsf{rsp}_1, \ldots, \mathsf{rsp}_N).$$

$\mathsf{Verify}(m, R, \sigma) \to \{0,1\}$:

1. For $j \in [N]$, the verifier generates each challenge:

$$\mathsf{chl}_{j+1} \leftarrow H(m||\mathsf{com}_j),$$

2. If the following two conditions hold, the verifier accepts.
   (i) $\mathsf{V}(\mathsf{pk}_j, \mathsf{com}_j, \mathsf{chl}_j, \mathsf{rsp}_j) = 1 \quad$ for all j,
   (ii) $\mathsf{chl}_{N+1} = \mathsf{chl}_1$.

Regarding the security of the ring signature obtained through the above transformation, the following facts are known.

Proposition 1. *If the underlying Σ-protocol is correct, special sound, and special HVZK, the resulting ring signature is correct, unforgeable, and anonymous.*

This proposition is straightforward from [10, Proposition 2.3 & Proposition 2.4]. Note that although [10, Proposition 2.4] assumes a different condition [10, Definition A.1] in place of the special soundness of the Σ-protocol, this condition follows immediately from special soundness. (See [2, Figure 1] for example.)

2.3 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 [11, 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 [30]. 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.

2.4 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 $n(\alpha)$.

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 $I = J\beta$.

Deuring Correspondence. Deuring [15] 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 $\mathcal{O}_0 \coloneqq \mathbb{Z}\langle 1, \mathbf{i}, \frac{\mathbf{i}+\mathbf{j}}{2}, \frac{1+\mathbf{k}}{2}\rangle$. 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 [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 $\phi : E_1 \to E_2$ 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 $\mathcal{O}_2$. Moreover, two isogenies $\phi, \psi : E_1 \to E_2$ that have the same domain and codomain correspond to equivalent ideals $I_\phi \sim I_\psi$.

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. Then, for $\alpha \in I \setminus \{0\}$, we have a connecting ideal $\chi_I(\alpha)$ from $\mathcal{O}_1$ to $\mathcal{O}_2$ defined by $\chi_I(\alpha) := I\frac{\bar{\alpha}}{n(I)}$. Then, the norm of $\chi_I(\alpha)$ is $q_I(\alpha) := \frac{n(\alpha)}{n(I)} \in \mathbb{Z}$. The corresponding isogeny $\varphi_{\chi_I(\alpha)} : E_1 \to E_2$ satisfies $\widehat{\varphi}_{\chi_I(\alpha)} \circ \varphi_I = \alpha$.

2.5 Subroutines Related to Deuring Correspondence.

Here, we introduce some existing algorithms using quaternion algebras. As in the above, we let $\mathcal{O}_0$ be the maximal order of $\mathcal{B}_{p,\infty}$ with basis $(1, \mathbf{i}, \frac{\mathbf{i}+\mathbf{j}}{2}, \frac{1+\mathbf{k}}{2})$.

$\texttt{StrongApproximation}_M(N, C, D)$: This algorithm was proposed in [21,27]. It takes as input an integer M, a prime N, and $(C : D) \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ such that $\left(\frac{p(C^2+D^2)}{N}\right) = \left(\frac{M}{N}\right)$ holds, and outputs an element $\alpha \in \mathcal{O}_0$ such that $n(\alpha) = M$ and

$$\alpha = u(C\mathbf{j} + D\mathbf{k}) + N\mu_0,$$

where $u \in \mathbb{Z}$ and $\mu_0 \in \mathcal{O}_0$. For the algorithm to succeed, the integer M must be at least of size $O(pN^3)$. Moreover, if the parity condition $\left(\frac{p(C^2+D^2)}{N}\right) = \left(\frac{M}{N}\right)$ does not hold, by replacing M with a divisor $M' \mid M$ such that $\left(\frac{p(C^2+D^2)}{N}\right) = \left(\frac{M'}{N}\right)$, we can obtain $\alpha \in \mathcal{O}_0$ of norm M'. Therefore, this algorithm can output an element α whose norm divides M, provided that M has sufficiently many divisors, regardless of the parity condition. Note that this algorithm can be extended to the case where N is composite, provided that the factorization of N is known.

$\texttt{Qlapoti}(I)$: This is an algorithm to convert an ideal to its corresponding isogeny proposed in [8]. It takes a left $\mathcal{O}_0$-ideal I as input and outputs an efficient representation of an isogeny φ_I corresponding to I. More precisely, this algorithm is designed for the case where p is of the form $p = 2^e \cdot f - 1$, and it returns the evaluation of φ_I on $E_0[2^e]$ as an efficient representation of φ_I. Moreover, the algorithm internally performs a $(2^e, 2^e)$-isogeny computation.

$\texttt{GeneralizedKLPT}_M(I, I')$: This algorithm is proposed as a subroutine of SQIsign-v1.0 [14]. It takes as input a left $\mathcal{O}_0$-ideal I of norm N, a left $\mathcal{O}_R(I)$-ideal I' of norm N' coprime to N, and an integer M. Then it outputs an equivalent ideal $J \sim I'$ of norm dividing M. For this algorithm to succeed, M must be at least of size $O(p^2N^3(N')^2)$. In practice, the norm N' of I' is often of size $O(\sqrt{p})$. In this case, M must be at least of size $O(p^3N^3)$. Furthermore, the algorithm tweaked so that the output ideal has norm exactly M is referred to as SigningKLPT.

Δ-$\texttt{KLPT}_M(I_1, I_2)$: This algorithm is a variant of `GeneralizedKLPT` proposed in [25]. It takes as input two left $\mathcal{O}_0$-ideals I_1 and I_2 of prime norm N and an integer M. Then it outputs an equivalent ideal $I \sim \bar{I}_1 I_2$ of norm dividing M. The overview of this algorithm is as follows:

1. Computes $\alpha_0 = C_0\mathbf{j} + D_0\mathbf{k}$ such that $[\alpha_0]_*\varphi_1 = \varphi_2$, where φ_1, φ_2 are the isogenies corresponding to I_1, I_2.
2. Computes $\alpha \in \mathbb{Z}\alpha_0 + N\mathcal{O}_0$ of norm dividing M as follows:

$$\alpha \leftarrow \texttt{StrongApproximation}_M(N, C_0, D_0).$$

3. Outputs $I = I_1^{-1} \cdot I_2\alpha$.

Note that this algorithm is based on the following commutative diagram.

$$\begin{array}{ccc} E_0 & \xrightarrow{\alpha} & E_0 \\ {\scriptstyle\varphi_1}\downarrow & & \downarrow{\scriptstyle\varphi_2} \\ E_1 & \xrightarrow{\varphi_I} & E_2 \end{array}$$

Since we use `StrongApproximation`, the integer M must be at least of size $O(pN^3)$.

2.6 SQIsign1.0

SQIsign1.0 is an isogeny-based signature scheme proposed by De Feo, Kohel, Leroux, Petit, and Wesolowski in [14] and was one of the candidates in Round 1 of the NIST additional signature competition [11]. SQIsign1.0 is obtained by applying the Fiat–Shamir transform on the Σ-protocol based on the following diagram.

$$\begin{array}{ccc} E_0 & \xrightarrow{\varphi_{\mathsf{com}}} & E_{\mathsf{com}} \\ {\scriptstyle\varphi_{\mathsf{sk}}}\downarrow & & \downarrow{\scriptstyle\varphi_{\mathsf{chl}}} \\ E_{\mathsf{pk}} & \xrightarrow[\varphi_{\mathsf{rsp}}]{} & E_{\mathsf{chl}} \end{array}$$

The public parameter for SQIsign1.0 is as follows.

- A prime p such that $p \approx 2^{2\lambda}$.
- A smooth integer T such that $T \approx p^{5/4}$ and $T|(p^2 - 1)$. We divide T as $T = D'_c \cdot T'$, where $T' \approx p$. In addition, let $D_c = 2^f \cdot D'_c$ so that $D_c \approx 2^\lambda$.
- An integer B_{sk} such that $B_{\mathsf{sk}} \approx p^{1/4}$.
- A supersingular elliptic curve $E_0/\mathbb{F}_{p^2} : y^2 = x^3 + x$.
- $\mathcal{O}_0 = \mathbb{Z}\langle 1, \mathbf{i}, \frac{\mathbf{i}+\mathbf{j}}{2}, \frac{1+\mathbf{k}}{2}\rangle$, which is isomorphic to $\mathrm{End}(E_0)$.

The underlying Σ-protocol of SQIsign1.0 is as follows.

- **Key generation.** The prover samples a random prime $N_{\mathsf{sk}} < B_{\mathsf{sk}}$ and computes a random N_{sk}-isogeny $\varphi_{\mathsf{sk}} : E_0 \to E_{\mathsf{pk}}$ with its corresponding ideal I_{sk}.
- **Commitment.** The prover computes a random T'-isogeny $\varphi_{\mathsf{com}} : E_0 \to E_{\mathsf{com}}$ with its corresponding ideal I_{com}. Then it sends E_{com} to the verifier.
- **Challenge.** The verifier sends a random D_c-isogeny $\varphi_{\mathsf{chl}} : E_{\mathsf{com}} \to E_{\mathsf{chl}}$.
- **Response.** Let I_{chl} be the ideal corresponding to φ_{chl} and let $I' = \bar{I}_{\mathsf{sk}} \cdot I_{\mathsf{com}} \cdot I_{\mathsf{chl}}$. The signer executes $I_{\mathsf{rsp}} \leftarrow \mathsf{SigningKLPT}_{\mathsf{2^\bullet}}(I, I')$ and sends its corresponding isogeny $\varphi_{\mathsf{rsp}} : E_{\mathsf{pk}} \to E_{\mathsf{chl}}$ to the verifier.
- **Verify.** The verifier computes φ_{chl} and φ_{rsp} and checks that these isogeny have the same codomain E_{chl}.

For $\mathsf{SigningKLPT}_{\mathsf{2^\bullet}}(I, I')$ in the response to succeed, the norm of I_{rsp} must be at least of size $O(p^3 N_{\mathsf{sk}}^3) = O(p^{3.75})$. Therefore, the degree of φ_{rsp} is also of size $O(p^{3.75})$.

2.7 Erebor

Erebor is an isogeny-based ring signature proposed by Borin, Lai, and Leroux [10]. Roughly speaking, Erebor is obtained by applying AOS framework on the Σ-protocol underlying the SQIsign1.0. However, to apply AOS framework, they use the challenge φ_{chl} from E_{pk} instead of E_{com}. Therefore, the diagram for Erebor is as follows.

$$\begin{array}{ccc} E_0 & \xrightarrow{\varphi_{\mathsf{com}}} & E_{\mathsf{com}} \\ {\scriptstyle \varphi_{\mathsf{sk}}}\downarrow & & \downarrow{\scriptstyle \varphi_{\mathsf{rsp}}} \\ E_{\mathsf{pk}} & \xrightarrow[\varphi_{\mathsf{chl}}]{} & E_{\mathsf{chl}} \end{array}$$

By swapping E_{pk} and E_{com}, we can easily construct a simulator $\mathcal{S}$ for a special HVZK as follows.

- $\mathcal{S}(\mathsf{pk} := E_{\mathsf{pk}}, \mathsf{chl} := \varphi_{\mathsf{chl}}) \to (\mathsf{com}, \mathsf{rsp})$:
  1. Compute $\varphi_{\mathsf{chl}} : E_{\mathsf{pk}} \to E_{\mathsf{chl}}$.
  2. Compute a random $2^\bullet$-isogeny $\varphi : E_{\mathsf{chl}} \to E_{\mathsf{com}}$.
  3. Return $(\mathsf{com} = E_{\mathsf{com}}, \mathsf{rsp} = \widehat{\varphi}_{\mathsf{rsp}})$.

Erebor has two variants: Erebor-full and Erebor-short. In Erebor-full, to achieve full anonymity, the ideal I_{com} corresponding to φ_{com} is randomized; that is, one samples a random ideal equivalent to I_{com} with sufficiently large norm. This randomization ensures that the response isogeny φ_{rsp} obtained via $\mathsf{SigningKLPT}$ is sufficiently randomized. However, as a consequence of taking the norm of I_{com} to be large, the degree of φ_{rsp} becomes significantly larger than $O(p^{3.75})$, which is the degree achieved in SQIsign1.0.

On the other hand, Erebor-short reduces the signature size at the cost of full anonymity. In Erebor-short, the degree of φ_{com} is chosen to be about $p^{1/4}$, similarly to φ_{sk} in SQIsign1.0, so that the degree of φ_{rsp} is reduced to about $O(p^{3.75})$.

3 Our Construction

In this section, we introduce our new ring signature. Before constructing the ring signature, we first give the underlying Σ-protocol in subsection 3.1. Then we construct our new ring signature in subsection 3.2.

3.1 Construction of Σ-Protocol

In this subsection, we show our new Σ-protocol, based on which we construct our ring signature. We first give parameters of our Σ-protocol against a security parameter λ.

- A prime $p = f \cdot 2^e - 1$, where $e \approx 2\lambda$ and f is a positive integer as small as possible.
- A supersingular elliptic curve $E_0 : y^2 = x^3 + x$ defined over $\mathbb{F}_{p^2}$.
- A prime N_{sk} such that $N_{\mathsf{sk}} \approx 2^\lambda$.
- A prime N_{chl} such that $N_{\mathsf{chl}} \approx 2^\lambda$ and $N_{\mathsf{chl}} | p^2 - 1$. Note that the latter constraint induces $E_0[N_{\mathsf{chl}}] \subset E_0(\mathbb{F}_{p^4})$.

Overview of our construction. Our Σ-protocol is based on the following diagram, where E_{pk} is public key, φ_{sk} is secret key, and E_{com} is commitment.

$$\begin{array}{ccc} E_0 & & \\ {\scriptstyle \varphi_{\mathsf{sk}}}\downarrow & \searrow^{\varphi_{\mathsf{com}}} & \\ E_{\mathsf{pk}} & \xrightarrow[\varphi_{\mathsf{rsp}}]{} & E_{\mathsf{com}} \end{array}$$

The diagram is the same as that of Δ-SQIsign; however, in Δ-SQIsign the challenge specifies the degree of φ_{rsp}, whereas in our protocol the challenge specifies the image of a N_{chl}-torsion point under φ_{rsp}. More precisely, the verifier choose a random point $R_{\mathsf{com}} \in E_{\mathsf{com}}[N_{\mathsf{chl}}]$ and send it to the prover as a challenge. Then the prover finds an isogeny $\varphi_{\mathsf{rsp}} : E_{\mathsf{pk}} \to E_{\mathsf{com}}$ satisfying $\varphi_{\mathsf{rsp}}(P_{\mathsf{pk}}) \in \langle R_{\mathsf{com}} \rangle$, where P_{pk} is a deterministic point in $E_{\mathsf{pk}}[N_{\mathsf{chl}}]$.

To construct such an isogeny φ_{rsp}, we follow an approach similar to that of Δ-KLPT. We consider two N_{chl}-isogenies $\varphi'_{\mathsf{sk}} : E_{\mathsf{pk}} \to E'_{\mathsf{pk}} = E_{\mathsf{pk}}/\langle P_{\mathsf{pk}} \rangle$ and $\varphi'_{\mathsf{com}} : E_{\mathsf{com}} \to E'_{\mathsf{com}} = E_{\mathsf{com}}/\langle R_{\mathsf{com}} \rangle$. Then, we compute an endomorphism $\alpha : E_0 \to E_0$ of norm dividing M that makes the following diagram commute for an isogeny φ.

$$\begin{array}{ccc} E_0 & \xrightarrow{\alpha} & E_0 \\ {\scriptstyle \varphi_{\mathsf{sk}}}\downarrow & & \downarrow{\scriptstyle \varphi_{\mathsf{com}}} \\ E_{\mathsf{pk}} & & E_{\mathsf{com}} \\ {\scriptstyle \varphi'_{\mathsf{sk}}}\downarrow & & \downarrow{\scriptstyle \varphi'_{\mathsf{com}}} \\ E'_{\mathsf{pk}} & \xrightarrow{\varphi} & E'_{\mathsf{com}} \end{array}$$

We can compute such α in a similar way to Δ-KLPT by letting $I_1 = I_{\mathsf{sk}} \cdot I'_{\mathsf{sk}}$ and $I_2 = I_{\mathsf{com}} \cdot I'_{\mathsf{com}}$. Then, the isogeny $\varphi_{\mathsf{rsp}} := [\varphi_{\mathsf{sk}}]_*\alpha$ satisfies

$$\varphi_{\mathsf{rsp}}(\ker \varphi'_{\mathsf{sk}}) = \varphi_{\mathsf{rsp}}(\ker \varphi'_{\mathsf{com}}),$$

that is, $\varphi_{\mathsf{rsp}}(P_{\mathsf{pk}}) \in \langle R_{\mathsf{com}} \rangle$.

The difference from Δ−KLPT is that the norm N of the input ideals I_1, I_2 is not prime but $N = N_{\mathsf{sk}} \cdot N_{\mathsf{com}}$. In addition, we do not allow the degree of φ_{rsp} to be non-smooth as in the other high-dimensional signatures such as SQIsign2.0. Instead, we choose $M = 2^{4e}$ so that the degree of φ_{rsp} is a power of 2 like in SQIsign1.0.

In our setting, two issues arise about (i) the parity condition and (ii) the handling of N_{chl}-torsion points.

Parity condition: There are four possible combinations of the parity (i.e., whether it is a quadratic residue or non-residue) of $p(C^2 + D^2)$ in $\mathbb{Z}/N_{\mathsf{sk}}\mathbb{Z}$ and $\mathbb{Z}/N_{\mathsf{chl}}\mathbb{Z}$, whereas the parity of a divisor M' of M can take at most two values (namely, for $M' = 2^{4e}$ or 2^{4e-1}). Therefore, it may not be possible to choose an M' satisfying the required parity condition. There are two possible approaches to address this issue.

1. Include an additional prime factor in M, for example, taking $M = 2^{4e} \cdot 3$. In this case, M' can take four possible parities, namely $2^{4e} \cdot 3$, $2^{4e-1} \cdot 3$, 2^{4e}, and 2^{4e-1}, thereby matching all parity combinations.
2. Choose $(\varphi_{\mathsf{sk}}, \varphi_{\mathsf{com}})$ so that the parity condition is satisfied. In this case, it suffices to consider only the parity in $\mathbb{Z}/N_{\mathsf{chl}}\mathbb{Z}$.

In this paper, we prioritize keeping the degree of φ_{rsp} a power of 2, and thus adopt the second approach. To do so, we assume that $\left(\frac{2}{N_{\mathsf{sk}}}\right) = 1$ and $\left(\frac{2}{N_{\mathsf{chl}}}\right) = -1$ in advance.

N_{chl}-torsion points: To compute $\alpha_0 = C\mathbf{j} + D\mathbf{k}$ satisfying the above commutative diagram given P_{pk} and R_{com}, we have to find $(C_0 : D_0)$ such that

$$C_0(\varphi_{\mathsf{com}} \circ \mathbf{j} \circ \widehat{\varphi}_{\mathsf{sk}}(P_{\mathsf{pk}})) + D_0(\varphi_{\mathsf{com}} \circ \mathbf{k} \circ \widehat{\varphi}_{\mathsf{sk}}(P_{\mathsf{pk}})) \in \langle R_{\mathsf{com}} \rangle.$$

This means that we have to solve the BiDLP over N_{chl}-torsion subgroup. However, we cannot solve the BiDLP since N_{chl} is a large prime. To address this issue, we use

$$P_{\mathsf{com}} := \varphi_{\mathsf{com}} \circ \mathbf{j} \circ \widehat{\varphi}_{\mathsf{sk}}(P_{\mathsf{pk}})),\ Q_{\mathsf{com}} := \varphi_{\mathsf{com}} \circ \mathbf{k} \circ \widehat{\varphi}_{\mathsf{sk}}(P_{\mathsf{pk}}))$$

as a basis of $E_{\mathsf{com}}[N_{\mathsf{chl}}]$, and take as the challenge the coefficients of R_{com} with respect to this basis. In this way, a pair $(C_0 : D_0)$ satisfying the above condition can be obtained immediately without solving the BiDLP. However, for security reasons, $P_{\mathsf{com}}, Q_{\mathsf{com}}$ cannot be made public, so we randomize them using a random matrix $\mathbf{A}$.

In the following, we give details of our construction.

Key generation. In the key generation phase, we compute a random N_{sk}-isogeny φ_{sk} and a basis of $E_0[N_{\mathsf{chl}}]$.

1. Take a left $\mathcal{O}_0$-ideal I_{sk} of norm N_{sk}.
2. Compute a corresponding isogeny $\varphi_{\mathsf{sk}} : E_0 \to E_{\mathsf{pk}}$ of I_{sk} via `Qlapoti`.
3. Let $P_0, Q_0 = \mathbf{j}(\hat{\varphi}_{\mathsf{sk}}(P_{\mathsf{pk}})), \mathbf{k}(\hat{\varphi}_{\mathsf{sk}}(P_{\mathsf{pk}}))$ for a deterministic point $P_{\mathsf{pk}} \in E_{\mathsf{pk}}[N_{\mathsf{chl}}]$.
4. Let $\mathsf{pk} = E_{\mathsf{pk}}, \mathsf{sk} = (I_{\mathsf{sk}}, \varphi_{\mathsf{sk}}, P_0, Q_0)$.

Commitment($\mathbf{P_1}$). In the commitment, we compute a random N_{sk}-isogeny $\varphi_{\mathsf{com}} : E_0 \to E_{\mathsf{com}}$ such that there exists an endomorphism of E_0 of the form $\gamma = C\mathbf{j} + D\mathbf{k}$ satisfying $[\gamma]_*\varphi_{\mathsf{sk}} = \varphi_{\mathsf{com}}$ and $\left(\frac{\deg \gamma}{N_{\mathsf{sk}}}\right) = \left(\frac{2^{4e}}{N_{\mathsf{sk}}}\right) = 1$. Then we compute a basis of $E_{\mathsf{com}}[N_{\mathsf{chl}}]$.

1. Let $(C_{\mathsf{sk}} : D_{\mathsf{sk}}) \xleftarrow{\$} \left\{(c : d) \in \mathbb{P}^1(\mathbb{Z}/N_{\mathsf{sk}}\mathbb{Z}) \mid \left(\frac{p(c^2+d^2)}{N_{\mathsf{sk}}}\right) = 1\right\}$.
2. Let $\gamma = C_{\mathsf{sk}}\mathbf{j} + D_{\mathsf{sk}}\mathbf{k} \in \mathcal{O}_0$.
3. Let $I_{\mathsf{com}} = (\mathcal{O}_0\gamma \cap I_{\mathsf{sk}})\gamma^{-1}$, a left $\mathcal{O}_0$-ideal corresponding to $[\gamma]_*\varphi_{\mathsf{sk}}$.
4. Compute a corresponding isogeny $\varphi_{\mathsf{com}} : E_0 \to E_{\mathsf{com}}$ of I_{com} via `Qlapoti`.
5. Let $\mathbf{A} \xleftarrow{\$} \mathrm{GL}_2(\mathbb{Z}/N_{\mathsf{chl}}\mathbb{Z})$.
6. Let $(P_{\mathsf{com}}, Q_{\mathsf{com}}) = (\varphi_{\mathsf{com}}(P_0), \varphi_{\mathsf{com}}(Q_0))\mathbf{A}$.
7. Send $\mathsf{com} = (E_{\mathsf{com}}, P_{\mathsf{com}}, Q_{\mathsf{com}})$ and store $\mathsf{st} = (I_{\mathsf{com}}, \varphi_{\mathsf{com}}, (C_{\mathsf{sk}} : D_{\mathsf{sk}}), \mathbf{A})$ secretly.

Challenge. We use $\mathcal{C} := \mathbb{P}^1(\mathbb{Z}/N_{\mathsf{chl}}\mathbb{Z})$ as a challenge space.

1. Let $(s : t) \xleftarrow{\$} \mathcal{C}$.
2. Send $\mathsf{chl} = (s : t)$ to the prover.

Against this challenge $(s : t)$, we define $R_{\mathsf{com}} := sP_{\mathsf{com}} + tQ_{\mathsf{com}} \in E_{\mathsf{com}}[N_{\mathsf{chl}}]$. Note that the size of this challenge space is $N_{\mathsf{chl}} + 1 \approx 2^\lambda$.

Response($\mathbf{P_2}$). For a deterministic point $P_{\mathsf{pk}} \in E_{\mathsf{pk}}[N_{\mathsf{chl}}]$ and the challenge $R_{\mathsf{com}} \in E_{\mathsf{com}}[N_{\mathsf{chl}}]$, our goal is to compute an isogeny φ_{rsp} satisfying $\varphi_{\mathsf{rsp}}(P_{\mathsf{pk}}) \in \langle R_{\mathsf{com}}\rangle$. To do so, we give the following observation. Let $(C_{\mathsf{chl}}, D_{\mathsf{chl}})^\top = \mathbf{A}(s, t)^\top$. Then we have

$$\begin{aligned} R_{\mathsf{com}} &= C_{\mathsf{chl}}\varphi_{\mathsf{com}}(P_0) + D_{\mathsf{chl}}\varphi_{\mathsf{com}}(Q_0) \\ &= \varphi_{\mathsf{com}} \circ (C_{\mathsf{chl}}\mathbf{j} + D_{\mathsf{chl}}\mathbf{k}) \circ \hat{\varphi}_{\mathsf{sk}}(P_{\mathsf{pk}}). \end{aligned}$$

In addition, we already know $C_{\mathsf{sk}}, D_{\mathsf{sk}}$ satisfying

$$[C_{\mathsf{sk}}\mathbf{j} + D_{\mathsf{sk}}\mathbf{k}]_*\varphi_{\mathsf{sk}} = \varphi_{\mathsf{com}}.$$

Therefore, by taking $\alpha_0 \in \mathcal{O}_0\langle C_{\mathsf{chl}}\mathbf{j} + D_{\mathsf{chl}}\mathbf{k}, N_{\mathsf{chl}}\rangle \cap \mathcal{O}_0\langle C_{\mathsf{sk}}\mathbf{j} + D_{\mathsf{sk}}\mathbf{k}, N_{\mathsf{sk}}\rangle$, we obtain an isogeny $\varphi := [\varphi_{\mathsf{sk}}]_*\alpha_0$ from E_{pk} to E_{com} such that $\varphi(P_{\mathsf{pk}}) \in \langle R_{\mathsf{com}}\rangle$.

We can take such α_0 by using the Chinese Remainder Theorem. We write such α_0 as $C_0\mathbf{j} + D_0\mathbf{k}$.

$$\begin{array}{ccc} E_0 & \xrightarrow{\alpha_0} & E_0 \\ {\scriptstyle \varphi_{\mathsf{sk}}}\downarrow & & \downarrow{\scriptstyle \varphi_{\mathsf{com}}} \\ E_{\mathsf{pk}} & \xrightarrow{\varphi} & E_{\mathsf{com}} \end{array}$$

The remaining job is to find $\alpha \in \mathbb{Z}\alpha_0 + \mathcal{O}_0 N_{\mathsf{sk}} N_{\mathsf{chl}}$ of norm $2^\bullet$. We can find such α by executing $\texttt{StrongApproximation}_{2^{4e}}(C, D, N_{\mathsf{sk}}N_{\mathsf{chl}})$. Note here that the target degree 2^{4e} must be of size $O(p(N_{\mathsf{sk}}N_{\mathsf{chl}})^3)$ for `StrongApproximation` succeed. In our setting, we have $N \approx N_{\mathsf{chl}} \approx 2^\lambda \approx p^{1/2}$ and $2^e \approx p$. Thus we have $2^{4e} = O(p^4) = O(p(N_{\mathsf{sk}}N_{\mathsf{chl}})^3)$. In addition, since we already have

$$\left(\frac{p(C_{\mathsf{sk}}^2 + D_{\mathsf{sk}}^2)}{N_{\mathsf{sk}}}\right) = \left(\frac{2}{N_{\mathsf{sk}}}\right) = 1,$$

it is sufficient to take $M' \in \{2^{4e}, 2^{4e-1}\}$ so that $\left(\frac{p(C^2+D^2)}{N_{\mathsf{chl}}}\right) = \left(\frac{M'}{N_{\mathsf{chl}}}\right)$ holds. Therefore, we can compute α of norm 2^{4e} or 2^{4e-1}.

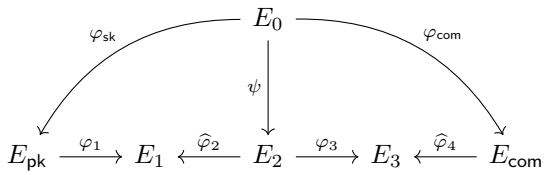
In the light of the above, we can compute φ_{rsp} as follows.

1. Let $(C_{\mathsf{chl}}, D_{\mathsf{chl}})^\top = \mathbf{A}(s,t)^\top$.
2. Let $C = \mathrm{CRT}_{N_{\mathsf{sk}},N_{\mathsf{chl}}}(C_{\mathsf{sk}}, C_{\mathsf{chl}})$ and $D = \mathrm{CRT}_{N_{\mathsf{sk}},N_{\mathsf{chl}}}(D_{\mathsf{sk}}, D_{\mathsf{chl}})$.
3. Let $\alpha \leftarrow \texttt{StrongApproximation}_{2^{4e}}(C, D, N_{\mathsf{sk}}N_{\mathsf{chl}})$.
4. Let $J = I_{\mathsf{sk}}^{-1} \cdot I_{\mathsf{com}}\alpha$.
5. Compute an efficient representation of φ_{rsp} corresponding to J using `Qlapoti` as in Δ-SQIsign. (Details will be provided later.)
6. Send φ_{rsp} to the verifier.

Degree of φ_{rsp}: Now we discuss the degree of φ_{rsp}. As described above, the degree of the response isogeny φ_{rsp} is $2^{4e} \approx p^4$. This degree is a bit larger than SQIsign1.0 and Erebor-shor, where the degree of the response is in $O(p^{3.75})$. However, in SQIsign1.0 and Erebor-short, the verifier has to compute not only the response isogeny φ_{rsp} but also the challenge isogeny φ_{chl}, whose degree is in $O(p^{0.5})$. Therefore, the total degree of the isogenies that the verifier computes is in $O(p^{4.25})$. This means that the verifying cost of our protocol is smaller than SQIsign1.0 and Erebor-short. Moreover, in generating a ring signature with N users, the transcript simulator $\mathcal{S}$ is invoked $N-1$ times, and thus the cost of simulation dominates the overall signing cost. As in verification, the simulator for Erebor computes both φ_{rsp} and φ_{chl}, whereas our protocol only requires the computation of φ_{rsp}. Consequently, the overall signing cost is also reduced.

How to compute φ_{rsp} from J: For simplicity, we consider the case where $\deg \varphi_{\mathsf{rsp}} = 2^{4e}$. We can decompose the response isogeny φ_{rsp} as $\varphi_{\mathsf{rsp}} = \varphi_4 \circ \cdots \circ \varphi_1$, where $\deg \varphi_1 = \cdots = \deg \varphi_4 = 2^e$. Thus, we can represent φ_{rsp} by the basis $K_1, \ldots, K_4$ of $\ker \varphi_1, \ldots, \ker \varphi_4$. In the following, we show how to compute such $K_1, \ldots, K_4$ from the ideal J.

1. Decompose the ideal J as $J = J_1 \cdot J_2 \cdot J_3 \cdot J_4$, where $J_1, \ldots, J_4$ correspond to $\varphi_1 \ldots, \varphi_4$, respectively.
2. Find an equivalent ideal $L \sim I_{\mathsf{sk}} \cdot J_1 \cdot J_2$ of odd norm q.
3. Compute the isogeny $\psi : E_0 \to E_2$ corresponding to L via Qlapoti.
4. Compute a basis K_1' of $E_0[I_{\mathsf{sk}} J_1 + 2^e \mathcal{O}_0] = \ker(\varphi_1 \circ \varphi_{\mathsf{sk}}) \cap E_0[2^e]$ and let $K_1 = \varphi_{\mathsf{sk}}(K_1')$, a basis of $\ker \varphi_1$.
5. Compute a basis $\widehat{K}_2'$ of $E_0[L\bar{J}_2 + 2^e \mathcal{O}_0] = \ker(\widehat{\varphi}_2 \circ \psi) \cap E_0[2^e]$ and let $\widehat{K}_2 = \psi(\widehat{K}_2')$, a basis of $\ker \widehat{\varphi}_2$.
6. Compute $\widehat{\varphi}_2 : E_2 \to E_1 = E_2/\langle \widehat{K}_2 \rangle$ and obtain a basis K_2 of $\ker \varphi_2 = \widehat{\varphi}_2(E_2[2^e])$.
7. Compute a basis K_3' of $E_0[LJ_3 + 2^e \mathcal{O}_0] = \ker(\varphi_3 \circ \psi) \cap E_0[2^e]$ and let $K_3 = \psi(K_3')$, a basis of $\ker \varphi_3$.
8. Compute a basis $\widehat{K}_4'$ of $E_0[I_{\mathsf{com}} \bar{J}_4 + 2^e \mathcal{O}_0] = \ker(\widehat{\varphi}_4 \circ \varphi_{\mathsf{com}}) \cap E_0[2^e]$ and let $\widehat{K}_4 = \varphi_{\mathsf{com}}(\widehat{K}_4')$, a basis of $\ker \widehat{\varphi}_4$.
9. Compute $\widehat{\varphi}_4 : E_{\mathsf{com}} \to E_3 = E_{\mathsf{com}}/\langle \widehat{K}_4 \rangle$ and obtain a basis K_4 of $\ker \varphi_4 = \widehat{\varphi}_4(E_{\mathsf{com}}[2^e])$.



We show the detail of the response algorithm in Algorithm 1.

Verify(V). The verification procedure is as follows.

1. Let P_{pk} be a deterministic point of $E_{\mathsf{pk}}[N_{\mathsf{chl}}]$.
2. For $i = 1, \ldots, 4$: compute an isogeny φ_i with the kernel $\langle K_i \rangle$.
3. Let $\varphi_{\mathsf{rsp}} = \varphi_4 \circ \varphi_3 \circ \varphi_2 \circ \varphi_1$.
4. If $\varphi_{\mathsf{rsp}}(P_{\mathsf{pk}}) \in \langle R_{\mathsf{com}} \rangle$, accept; otherwise, reject.

3.2 Construction of Our Ring Signature

Now we can construct our ring signature from the above Σ-protocol by using the transformation described in subsection 2.2.

To apply the transformation, we have to construct a transcript simulator $\mathcal{S}$ of the Σ-protocol. We consider the following simulator.

– $\mathcal{S}(x := E_{\mathsf{pk}}, \mathsf{chl} := (s,t)) \to (\mathsf{com}, \mathsf{rsp})$:
  1. Let P_{pk} be a deterministic point of $E_{\mathsf{pk}}[N_{\mathsf{chl}}]$.
  2. Let $b \xleftarrow{\$} \{0,1\}$.
  3. Compute a 2^{4e-b}-isogeny $\varphi_{\mathsf{rsp}} : E_{\mathsf{pk}} \to E_{\mathsf{com}}$ uniformly at random among all 2^{4e-b}-isogenies from E_{pk}.
  4. Let $P_{\mathsf{com}} \xleftarrow{\$} E_{\mathsf{com}}[N_{\mathsf{chl}}]$.

Algorithm 1 Response

Require: A secret key $\mathsf{sk} = (I_{\mathsf{sk}}, \varphi_{\mathsf{sk}}, P_0, Q_0)$, a state $\mathsf{st} = (I_{\mathsf{com}}, \varphi_{\mathsf{com}}, (C_{\mathsf{sk}} : D_{\mathsf{sk}}), \mathbf{A})$, and a challenge $\mathsf{chl} = (s, t)$.
Ensure: Response rsp or $\perp$.
1: Let $(C_{\mathsf{chl}}, D_{\mathsf{chl}})^\top = \mathbf{A}(s, t)^\top$.
2: Let $C = \mathrm{CRT}_{N_{\mathsf{sk}}, N_{\mathsf{chl}}}(C_{\mathsf{sk}}, C_{\mathsf{chl}})$ and $D = \mathrm{CRT}_{N_{\mathsf{sk}}, N_{\mathsf{chl}}}(D_{\mathsf{sk}}, D_{\mathsf{chl}})$.
3: Let $\alpha \leftarrow \mathtt{StrongApproximation}_{2^{4e}}(C, D, N_{\mathsf{sk}} N_{\mathsf{chl}})$.
4: Let $J = I_{\mathsf{sk}}^{-1} \cdot I_{\mathsf{com}} \alpha$.
5: Let $J = J_1 \cdot J_2 \cdot J_3 \cdot J_4$, where $n(J_i) = 2^e$ for $i = 1, \ldots, 4$.
6: Find an equivalent ideal $L \sim I_{\mathsf{sk}} \cdot J_1 \cdot J_2$ of odd norm q.
7: Compute the isogeny $\psi : E_0 \to E_2$ corresponding to L via `Qlapoti`.
8: Let K_1' be a basis of $E_0[I_{\mathsf{sk}} J_1 + 2^e \mathcal{O}_0]$ and let $K_1 = \varphi_{\mathsf{sk}}(K_1')$.
9: Let $\widehat{K}_2'$ be a basis of $E_0[L \bar{J}_2 + 2^e \mathcal{O}_0]$ and let $\widehat{K}_2 = \psi(\widehat{K}_2')$.
10: Compute $\widehat{\varphi}_2 : E_2 \to E_1 = E_2 / \langle \widehat{K}_2 \rangle$ and let K_2 be a basis of $\widehat{\varphi}_2(E_2[2^e])$.
11: Let K_3' be a basis of $E_0[L J_3 + 2^e \mathcal{O}_0]$ and let $K_3 = \psi(K_3')$.
12: Let $\widehat{K}_4'$ be a basis of $E_0[I_{\mathsf{com}} \bar{J}_4 + 2^e \mathcal{O}_0]$ and let $\widehat{K}_4 = \varphi_{\mathsf{com}}(\widehat{K}_4')$.
13: Compute $\widehat{\varphi}_4 : E_{\mathsf{com}} \to E_3 = E_{\mathsf{com}} / \langle \widehat{K}_4 \rangle$ and let K_4 be a basis of $\widehat{\varphi}_4(E_{\mathsf{com}}[2^e])$.
14: **return** (K_1, K_2, K_3, K_4).

5. Let $Q_{\mathsf{com}} = t^{-1}(u \varphi_{\mathsf{rsp}}(P_{\mathsf{pk}}) - s P_{\mathsf{com}})$ for $u \xleftarrow{\$} (\mathbb{Z}/N_{\mathsf{chl}}\mathbb{Z})^*$.
6. Return $(\mathsf{com} := (E_{\mathsf{com}}, P_{\mathsf{com}}, Q_{\mathsf{com}}), \mathsf{rsp} := \varphi_{\mathsf{rsp}})$.

Now we can apply the transformation in subsection 2.2. For the ring of N users, the signature σ consists of:

- A challenge: $\mathsf{chl}_1 := (s_1 : t_1)$,
- N commitments: $\{\mathsf{com}_i := (E_{\mathsf{com}}^{(i)}, P_{\mathsf{com}}^{(i)}, Q_{\mathsf{com}}^{(i)})\}_{i \in [N]}$,
- N responses: $\{\mathsf{rsp}_i := (K_1^{(i)}, K_2^{(i)}, K_3^{(i)}, K_4^{(i)})\}_{i \in [N]}$.

However, we can omit $E_{\mathsf{com}}^{(i)}$ and represent $Q_{\mathsf{com}}^{(i)}$ by $u_i \in \mathbb{Z}/N_{\mathsf{chl}}\mathbb{Z}$ for $i \in [N]$ since we can recover them as follows:

- By computing the 2^{4e}-isogeny $\varphi_{\mathsf{rsp}}^{(i)} : E_0 \to E_{\mathsf{com}}^{(i)}$ represented by rsp_i, we obtain its codomain $E_{\mathsf{com}}^{(i)}$.
- Let $\mathsf{pk}_i = E_{\mathsf{pk}}^{(i)}$, $\mathsf{chl}_i = (s_i : t_i)$, and let $P_{\mathsf{pk}}^{(i)}$ be a deterministic point of $E_{\mathsf{pk}}^{(i)}[N_{\mathsf{chl}}]$. Since $\varphi_{\mathsf{rsp}}^{(i)}(P_{\mathsf{pk}}^{(i)}) = u_i(s_i P_{\mathsf{com}}^{(i)} + t_i Q_{\mathsf{com}}^{(i)})$ for a scaler $u_i \in \mathbb{Z}/N_{\mathsf{chl}}\mathbb{Z}$, we can compute $Q_{\mathsf{com}}^{(i)}$ as follows:

$$Q_{\mathsf{com}}^{(i)} = (t_i)^{-1}(u_i \varphi_{\mathsf{rsp}}^{(i)}(P_{\mathsf{pk}}^{(i)}) - s_i P_{\mathsf{com}}^{(i)}).$$

Therefore, the signature is σ consists of $(s_1 : t_1)$ and $\{P_{\mathsf{com}}^{(i)}, u_i, (K_1^{(i)}, K_2^{(i)}, K_3^{(i)}, K_4^{(i)})\}_{i \in [N]}$.

4 Security Analysis

In this section, we give a security analysis on our ring signature scheme. To ensure that our scheme is 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.

4.1 Special-Soundness

We show that Σ is special-sound with respect to the following relation:

$$\mathcal{R}_{\texttt{0neEnd}} = \{(E, \alpha) \mid E/\mathbb{F}_{p^2} : \text{supersingular }, \alpha \in \mathrm{End}(E) \backslash \mathbb{Z}\}.$$

Proof. Let $(\mathsf{com}, \mathsf{chl}, \mathsf{rsp})$ and $(\mathsf{com}, \mathsf{chl}', \mathsf{rsp}')$ be two transcripts for the statement E_{pk} with the same commitment com but different challenges $\mathsf{chl} \neq \mathsf{chl}'$. Then rsp and rsp' provide efficient representations of two isogenies $\varphi_{\mathsf{rsp}}, \varphi_{\mathsf{rsp}'} : E_{\mathsf{pk}} \to E_{\mathsf{com}}$ of degree 2^{4e-b} and $2^{4e-b'}$ for $b.b' \in \{0, 1\}$. Thus, we obtain an endomorphism $\alpha = \widehat{\varphi}_{\mathsf{rsp}'} \circ \varphi_{\mathsf{rsp}} \in \mathrm{End}(E_{\mathsf{pk}})$ of degree $2^{8e-b-b'}$. It suffices to show that α is non-scalar.

Assume, for the sake of contradiction, that α is a scalar. Then the degree of α should be square. Therefore, we have $\deg \varphi_{\mathsf{rsp}} = \deg \varphi'_{\mathsf{rsp}} =: M'$ and $\alpha = \pm[M']$. This implies that $\varphi_{\mathsf{rsp}} = \pm\varphi_{\mathsf{rsp}'}$. In that case, we have $\varphi_{\mathsf{rsp}}(P_{\mathsf{pk}}) = \pm\varphi_{\mathsf{rsp}'}(P_{\mathsf{pk}})$, which contradicts $\mathsf{chl} \neq \mathsf{chl}'$. □

4.2 Honest-Verifier Zero-Knowledge

We have already constructed a simulator $\mathcal{S}$ for Σ in subsection 3.2. Therefore, under the hardness of the following problem, which means that the output distribution of $\mathcal{S}$ is computationally indistinguishable from that of real transcripts, Σ satisfies HVZK.

Problem 1. Given a supersingular elliptic curve $\mathsf{pk} = E_{\mathsf{pk}}$ over $\mathbb{F}_{p^2}$ and a transcript $\pi = (\mathsf{com}, \mathsf{chl}, \mathsf{rsp})$ sampled with probability $1/2$ from either distribution:

- $\mathcal{D}_0 = (\mathsf{pk}, \pi)$, where $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathtt{KeyGen}(1^\lambda)$, $(\mathsf{com}, \mathsf{st}) \leftarrow \mathsf{P}_1(\mathsf{sk})$, $\mathsf{chl} \xleftarrow{\$} \mathbb{P}^1(\mathbb{Z}/N_{\mathsf{chl}}\mathbb{Z})$, $\mathsf{rsp} \leftarrow \mathsf{P}_2(\mathsf{pk}, \mathsf{sk}, \mathsf{st}, \mathsf{chl})$, $\pi = (\mathsf{com}, \mathsf{chl}, \mathsf{rsp})$.
- $\mathcal{D}_1 = (\mathsf{pk}, \pi)$, where $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathtt{KeyGen}(1^\lambda)$, $\mathsf{chl} \xleftarrow{\$} \mathcal{C}$, $(\mathsf{com}, \mathsf{rsp}) \leftarrow \mathcal{S}(\mathsf{pk}, \mathsf{chl})$, $\pi = (\mathsf{com}, \mathsf{chl}, \mathsf{rsp})$.

Determine from which distribution the transcript π is sampled.

4.3 Hardness Analysis

We analyze the hardness of Problem 1. Since the distribution of the challenge chl is identical in $\mathcal{D}_0$ and $\mathcal{D}_1$, it suffices to consider the distributions of com and rsp. From now on, we denote the set of all supersingular elliptic curves over $\mathbb{F}_{p^2}$ by $\mathcal{E}$.

We first consider the commitment com. In $\mathcal{D}_0$, the distribution of E_{com} is uniform over exactly half of the set of codomains of N_{sk}-isogenies from E_0; denote this subset by $\mathcal{E}'$. The size of $\mathcal{E}'$ is $(N_{\mathsf{sk}}+1)/2 = O(2^\lambda)$. On the other hand, in $\mathcal{D}_1$, E_{com} is obtained as the codomain of a random 2^{4e}-isogeny from E_{pk}. By the Ramanujan property of supersingular isogeny graphs [28], the distribution of E_{com} is statistically close to the uniform distribution over $\mathcal{E}$. Therefore, distinguishing between $\mathcal{D}_0$ and $\mathcal{D}_1$ reduces to deciding whether E_{com} is sampled from $\mathcal{E}$ or from its subset $\mathcal{E}'$. However, no efficient method for making this distinction is known. The basis $(P_{\mathsf{com}}, Q_{\mathsf{com}})$ is generated uniformly among all the basis of $E_{\mathsf{com}}[N_{\mathsf{chl}}]$ in $\mathcal{D}_0$ since we randomize it by a matrix $\mathbf{A} \in \mathrm{GL}_2(\mathbb{Z}/N_{\mathsf{chl}}\mathbb{Z})$. In $\mathcal{D}_1$, the basis $(P_{\mathsf{com}}, Q_{\mathsf{com}})$ is also considered to be uniform assuming that $\varphi_{\mathsf{rsp}}(P_{\mathsf{pk}})$ is uniformly distributed over $E_{\mathsf{com}}[N_{\mathsf{chl}}] \setminus \{O\}$ for a uniformly chosen φ_{rsp}.

Next, we consider the response rsp. In $\mathcal{D}_0$, the isogeny φ_{rsp} is generated by the way similar to Δ-KLPT. In $\mathcal{D}_1$, the isogeny φ_{rsp} is uniformly chosen among all isogenies from E_{pk} to E_{com} of degree 2^{4e} or 2^{4e-1}. As mentioned in [25], distinguishing these two distribution 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}.

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 our ring signature scheme. First, we provide our concrete parameters. We recall that our parameters must satisfy the following conditions:

- $e \approx 2\lambda$.
- p is a prime of the form $p = f \cdot 2^e - 1$ for some small integer f.
- N_{sk} is a prime satisfying $N_{\mathsf{sk}} \approx 2^\lambda$ and $\left(\frac{2}{N_{\mathsf{sk}}}\right) = 1 \Leftrightarrow N_{\mathsf{sk}} \equiv 1, 7 \pmod 8$.
- N_{chl} is a prime satisfying $N_{\mathsf{chl}} \approx 2^\lambda$, $\left(\frac{2}{N_{\mathsf{chl}}}\right) = -1 \Leftrightarrow N_{\mathsf{chl}} \equiv 3, 5 \pmod 8$, and $N_{\mathsf{chl}} \mid (p-1)$.

The concrete parameters corresponding to NIST security level I are as follows.

- Parameters for NIST security level I ($\lambda = 128$):

$$e = 247,\ p = 79 \cdot 2^{247} - 1,\ N_{\mathsf{sk}} = 2^{118} - 111,$$
$$N_{\mathsf{chl}} = 168118140144706967996895604212334429.$$

Table 1. Signature sizes (in bytes) comparison for the NIST security level I

Protocol (NIST I)	Signature
Erebor-full [10]	$16 + N \cdot 170$
Erebor-short [10]	$16 + N \cdot 130$
Ours	$16 + N \cdot 207$

5.1 Signature sizes

In this subsection, we analyze the signature sizes of our protocol. The signature of our protocol consists of $(s_1 : t_1) \in \mathbb{P}^1(\mathbb{Z}/N_{\mathsf{chl}}\mathbb{Z})$, N points $\{P_{\mathsf{com}}^{(i)}\}_{i\in[N]}$, N integers $\{u_i\}_{i\in[N]}$, and $4N$ points $\{K_1^{(i)}, \ldots, K_4^{(i)}\}_{i\in[N]}$.

Each 2^e-torsion point $K_j^{(i)} \in E_j^{(i)}[2^e]$ for $i \in [N], j \in [4]$ can be represented by a coefficient $c_j^{(i)} \in \mathbb{Z}/2^e\mathbb{Z}$ such that $\langle K_j^{(i)} \rangle = \langle P_j^{(i)} + c_j^{(i)} Q_j^{(i)} \rangle$ or $\langle K_j^{(i)} \rangle = \langle c_j^{(i)} P_j^{(i)} + Q_j^{(i)} \rangle$ for a deterministic basis $P_j^{(i)}, Q_j^{(i)}$ of $E_j^{(i)}[2^e]$ with additional 1-bit indicating whether $s_j^{(i)}$ is the coefficient of $P_j^{(i)}$ or $Q_j^{(i)}$. On the other hand, we cannot compress each N_{chl}-torsion point $P_{\mathsf{com}}^{(i)} \in E_{\mathsf{com}}^{(i)}[N_{\mathsf{chl}}]$ since we cannot solve BiDLP over $E_{\mathsf{com}}^{(i)}[N_{\mathsf{chl}}]$ for a non-smooth integer N_{chl}. Therefore, we represent $P_{\mathsf{com}}^{(i)} \in E_{\mathsf{com}}^{(i)}[N_{\mathsf{chl}}]$ by its x-coordinate, which is an element of $\mathbb{F}_{p^2}$.

Therefore, the signature requires $\lceil \log_2 N_{\mathsf{chl}} \rceil \approx \lambda$ bits for $(s_1 : t_1)$, $N\lceil \log_2 p^2 \rceil \approx 4N\lambda$ bits for $\{P_{\mathsf{com}}^{(i)}\}_{i\in[N]}$, $N\lceil \log_2 N_{\mathsf{chl}} \rceil \approx N\lambda$ bits for $\{u_i\}_{i\in[N]}$, and $4N(e+1) \approx 8N\lambda$ bits for $\{K_1^{(i)}, \ldots, K_4^{(i)}\}_{i\in[N]}$, and . Totally, the signature size is $(13N+1)\lambda$ bits. Table 1 shows the signature size in bytes for each security level. Unfortunately, our signature size is about 1.6 times of that of Erebor-short.

5.2 Computational Cost

In this subsection, we analyze the computational costs of our protocol by counting the number of isogeny computations of dimension 1 and 2.

KeyGen. Our key generation invokes Qlapoti once. Therefore our key generation requires e computations of $(2, 2)$-isogenies.

Sign. Our signing procedure for a ring of N parties invokes one commitment algorithm P_1, one response algorithm P_2, and $N-1$ transcript simulators $\mathcal{S}$. In the commitment algorithm P_1, Qlapoti is invoked once. In the response algorithm P_2, Qlapoti is invoked once. In addition, we compute a 2^e-isogeny twice. Finally, each transcript simulator $\mathcal{S}$ invokes a 2^{4e}-isogeny computation. In total, our signing procedure requires $2e$-times $(2, 2)$-isogeny computations and $(2e+4e(N-1))$-times 2-isogeny computations.

Table 2. Number of isogeny computation of each degree for NIST security level I.

	KeyGen	Sign	Verify
2-isogeny	0	$N \cdot 988 - 494$	$N \cdot 988$
$(2,2)$-isogeny	247	494	0

Verify. Our verification requires a 2^{4e}-isogeny computation for each party. Therefore, our verification for a ring of N parties requires $4eN$-times 2-isogeny computations.

We summarize the concrete number of isogeny computations of our protocol for NIST security level I in Table 2. Focusing on the parts that depend on N, our protocol requires, for both signing and verification, the computation of 2^{988}-isogeny per user. In contrast, Erebor-short requires, for both signing and verification, the computation of $2^{1054} \cdot 3^{40}$-isogeny per user. Therefore, our protocol is expected to have a lower computational cost.

6 Conclusion

In this paper, we constructed a new Σ-protocol that satisfies special HVZK. By applying the AOS framework on our Σ-protocol, we obtain a new ring signature scheme. Compared to the existing isogeny-based ring signature Erebor, our ring signature achieves lower computational costs for both signing and verification. On the other hand, our ring signature has about 1.6 times larger signature sizes.

Exploring methods to reduce the signature size and developing an optimized implementation of our protocol remain important directions for future work. Achieving full anonymity is also an interesting direction 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. Michel Abdalla, Jee Hea An, Mihir Bellare, and Chanathip Namprempre. From identification to signatures via the Fiat-Shamir transform: Minimizing assumptions for security and forward-security. In Lars R. Knudsen, editor, *EUROCRYPT 2002*, volume 2332 of *LNCS*, pages 418–433. Springer, Berlin, Heidelberg, April / May 2002.
3. Masayuki Abe, Miyako Ohkubo, and Koutarou Suzuki. 1-out-of-n signatures from a variety of keys. In Yuliang Zheng, editor, *ASIACRYPT 2002*, volume 2501 of *LNCS*, pages 415–432. Springer, Berlin, Heidelberg, December 2002.

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. Ward Beullens, Samuel Dobson, Shuichi Katsumata, Yi-Fu Lai, and Federico Pintore. Group signatures and more from isogenies and lattices: Generic, simple, and efficient. In Orr Dunkelman and Stefan Dziembowski, editors, *EUROCRYPT 2022, Part II*, volume 13276 of *LNCS*, pages 95–126. Springer, Cham, May / June 2022.
6. Ward Beullens, Shuichi Katsumata, and Federico Pintore. Calamari and Falafl: Logarithmic (linkable) ring signatures from isogenies and lattices. In Shiho Moriai and Huaxiong Wang, editors, *ASIACRYPT 2020, Part II*, volume 12492 of *LNCS*, pages 464–492. Springer, Cham, December 2020.
7. Dan Boneh, Craig Gentry, Ben Lynn, and Hovav Shacham. Aggregate and verifiably encrypted signatures from bilinear maps. In Eli Biham, editor, *EUROCRYPT 2003*, volume 2656 of *LNCS*, pages 416–432. Springer, Berlin, Heidelberg, May 2003.
8. 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 *ASIACRYPT 2025, Part IV*, LNCS, pages 174–205. Springer, Singapore, December 2025.
9. Giacomo Borin, Luca De Feo, Guido Maria Lido, and Sina Schaeffler. The SQInstructor: a guide to SQIsign and the deuring correspondence with level structures. Cryptology ePrint Archive, Paper 2026/493, 2026.
10. Giacomo Borin, Yi-Fu Lai, and Antonin Leroux. Erebor and durian: Full anonymous ring signatures from quaternions and isogenies. *CiC*, 1(4):4, 2024.
11. 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`.
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. Max Deuring. Die typen der multiplikatorenringe elliptischer funktionenkörper. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 14:197–272, 1941.
16. 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.
17. Muhammed F. Esgin, Ron Steinfeld, and Raymond K. Zhao. MatRiCT$^+$: More efficient post-quantum private blockchain payments. In *2022 IEEE Symposium on Security and Privacy*, pages 1281–1298. IEEE Computer Society Press, May 2022.
18. Phillip Gajland, Jonas Janneck, and Eike Kiltz. Ring signatures for deniable AKEM: Gandalf's fellowship. In Leonid Reyzin and Douglas Stebila, editors, *CRYPTO 2024, Part I*, volume 14920 of *LNCS*, pages 305–338. Springer, Cham, August 2024.
19. Jens Groth and Markulf Kohlweiss. One-out-of-many proofs: Or how to leak a secret and spend a coin. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part II*, volume 9057 of *LNCS*, pages 253–280. Springer, Berlin, Heidelberg, April 2015.
20. Jonathan Katz, Vladimir Kolesnikov, and Xiao Wang. Improved non-interactive zero knowledge with applications to post-quantum signatures. In David Lie, Mohammad Mannan, Michael Backes, and XiaoFeng Wang, editors, *ACM CCS 2018*, pages 525–537. ACM Press, October 2018.
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. Joseph K. Liu, Victor K. Wei, and Duncan S. Wong. Linkable spontaneous anonymous group signature for ad hoc groups (extended abstract). In Huaxiong Wang, Josef Pieprzyk, and Vijay Varadharajan, editors, *ACISP 04*, volume 3108 of *LNCS*, pages 325–335. Springer, Berlin, Heidelberg, July 2004.
23. Xingye Lu, Man Ho Au, and Zhenfei Zhang. Raptor: A practical lattice-based (linkable) ring signature. In Robert H. Deng, Valérie Gauthier-Umaña, Martín Ochoa, and Moti Yung, editors, *ACNS 19International Conference on Applied Cryptography and Network Security*, volume 11464 of *LNCS*, pages 110–130. Springer, Cham, June 2019.
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. Kohei Nakagawa and Ryo Yoshizumi. Δ-SQIsign: A new isogeny-based signature scheme using degree challenges. Cryptology ePrint Archive, Paper 2026/852, 2026.
26. Shen Noether. Ring signature confidential transactions for monero. Cryptology ePrint Archive, Report 2015/1098, 2015.
27. Christophe Petit and Spike Smith. An improvement to the quaternion analogue of the ℓ-isogeny path problem, 2018. Conference talk at MathCrypt.
28. Arnold K. Pizer. Ramanujan graphs and Hecke operators. *Bulletin of the American Mathematical Society*, 23(1):127–137, 1990.
29. Ronald L. Rivest, Adi Shamir, and Yael Tauman. How to leak a secret. In Colin Boyd, editor, *ASIACRYPT 2001*, volume 2248 of *LNCS*, pages 552–565. Springer, Berlin, Heidelberg, December 2001.
30. Jacques Vélu. Isogénies entre courbes elliptiques. *Comptes-Rendus de l'Académie des Sciences*, 273:238–241, 1971.
31. Zheng Xu, Kaizhan Lin, Chang-An Zhao, and Yi Ouyang. SQIsign2D^2: New SQIsign2D variant by leveraging power smooth isogenies in dimension one. In *ASIACRYPT 2025, Part IV*, LNCS, pages 341–371. Springer, Singapore, December 2025.

32. Tsz Hon Yuen, Muhammed F. Esgin, Joseph K. Liu, Man Ho Au, and Zhimin Ding. DualRing: Generic construction of ring signatures with efficient instantiations. In Tal Malkin and Chris Peikert, editors, *CRYPTO 2021, Part I*, volume 12825 of *LNCS*, pages 251–281, Virtual Event, August 2021. Springer, Cham.