SQIsign2D-East: A New Signature Scheme Using 2-dimensional Isogenies

Kohei Nakagawa[1] and Hiroshi Onuki[2]

[1] NTT Social Informatics Laboratories, Japan
[2] The University of Tokyo, Japan

Abstract. Isogeny-based cryptography is cryptographic schemes whose security is based on the hardness of a mathematical problem called the isogeny problem, and is attracting attention as one of the candidates for post-quantum cryptography. A representative isogeny-based cryptography is the signature scheme called SQIsign, which was submitted to the NIST PQC standardization competition. SQIsign has attracted much attention because of its very short signature and key size among the candidates for the NIST PQC standardization. Recently, a lot of new schemes have been proposed that use high-dimensional isogenies. Among them, the signature scheme called SQIsignHD has an even shorter signature size than SQIsign. However, it requires 4-dimensional isogeny computations for the signature verification. In this paper, we propose a new signature scheme, SQIsign2D-East[3], which requires only two-dimensional isogeny computations for verification, thus reducing the computational cost of verification. First, we generalized an algorithm called RandIsogImg, which computes a random isogeny of non-smooth degree. Then, by using this generalized RandIsogImg, we construct a new signature scheme SQIsign2D-East.

1 Introduction

In recent years, isogeny-based cryptography has been actively studied as one of the candidates for post-quantum cryptography (PQC). One of the representative isogeny-based cryptographies is the signature scheme called SQIsign [11], which was submitted to the NIST PQC standardization competition. SQIsign has attracted much attention because of its very short signature and key size among the candidates for the NIST PQC standardization. Another well-known isogeny-based cryptography is SIDH [17], which is proposed by De Feo and Jao. Additionally, SIKE [1], a key encapsulation scheme based on SIDH, remained an alternative candidate for the NIST PQC standardization competition until Round 4. However, recent attacks [5,20,24] broke the security of SIDH and

[3] Originally, our protocol was named SQIsign2D, but Andrea Basso, Luca De Feo, Pierrick Dartois, Antonin Leroux, Luciano Maino, and Benjamin Wesolowski also studied a signature of the same name independently of us. After discussions with them, we decided to name our protocol SQIsign2D-East and theirs SQIsign2D-West, based on their respective locations.

SIKE. These attacks find the secret isogeny from the two point images under the isogeny by computing high dimensional isogenies.

In response, a number of cryptographic applications of attacks on SIDH have been studied, such as SQIsignHD [9], FESTA [3], QFESTA [22] SCALLOP-HD [7], and IS-CUBE [21]. Among them, SQIsignHD is a variant of SQIsign that has a shorter signature size and higher singing performance than SQIsign. However, it requires 4-dimensional isogeny computations for signature verification, which leads to a large computational cost. Since NIST calls for signature schemes that have short signatures and fast verification, reducing the verification cost of SQIsignHD is an important issue.

1.1 Contribution

In this paper, we make the following contributions:

1. We construct a new algorithm **GenRandIsogImg**, which is a generalization of the algorithm called **RandIsogImg** proposed in [22], which computes the codomain and point images of a given degree isogeny from a *special* elliptic curve E_0. Our **GenRandIsogImg** computes the codomain and point images of a given degree isogeny from a *given* elliptic curve E.
2. Using **GenRandIsogImg** as a building block, we propose a new variant of SQIsignHD, which only requires 2-dimensional isogeny computations for the verification. We name this signature scheme 'SQIsign2D-East'.
3. We give concrete parameters of SQIsign2D for the NIST security level 1, 3, and 5. Under these parameter settings, we analyse the signature sizes and show that our signature sizes are smaller than SQIsign and larger than SQIsignHD.
4. We analyse the computational cost of SQIsign2D-East under the parameter for the NIST security level 1 and show that the verification cost of SQIsign2D is smaller than that of SQIsignHD.

1.2 Related works

At the same time as this work, [2] and [14] also proposed a variant of SQIsignHD based on 2-dimensional isogeny. The former one is called 'SQIsign2D-West' and the later one is called 'SQIPrime'. These protocols are similar to ours, but they were proposed independently of us. Our protocol has a stronger security assumption than their protocol but seems to be more efficient. we leave the comparison with their protocol as future work.

Recently, [23] proposed an algorithm called **IdealToIsogenyIQO** that makes the key generation and the signing procedure in SQIsign at least twice as fast. However, their costs are still lager than SQIsignHD and SQIsign2D-East as described in their paper.

1.3 Organizations

In Section 2, we give some notation and background knowledge used in our protocol. In Section 3, we construct a generalized **RandIsogImg**. In Section 4, we propose our new signature scheme SQIsign2D-East and its security is analysed in Section 5. In Section 6, we give some concrete parameters for SQIsign2D-East and analyse the data size and the computational cost of SQIsign2D-East. Finally, in Section 7, we give the conclusion of this paper.

2 Preliminaries

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

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. $f(x)$ is *negligible* if $|f(x)| < x^{-c}$ for all positive integers c and sufficiently large x. We write $f(x) < \mathrm{negl}(x)$ if $f(x)$ is negligible. For a finite set S, we write $x \in_U S$ if x is sampled uniformly at random from S. Let $\perp$ be the symbol indicating failure of an algorithm.

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 and has finite kernel. The *degree* of an isogeny φ is its degree as a rational map and denoted it 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 a unique *dual isogeny* $\hat{\varphi}$ such that $\hat{\varphi} \circ \varphi$ is equal to the multiplication-by-$\deg \varphi$ map on A.

Let $\varphi : A \to B$, $\psi : A \to C$, and $\psi' : B \to D$ be isogenies. If $\ker \psi' = \varphi(\ker \psi)$ holds, we say that ψ' is the push-forward of ψ by φ and denote it by $\psi' = [\varphi]_* \psi$. Under the same situation, we say that ψ is the pull-back 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 $\mathbb{F}_{p^2}$. Among the isomorphism class of E, we can chose a Montgomery curve as a canonical representative by using [6, Algorithm 1]. We call this curve the *normalized curve* of E. In this paper, we assume that all elliptic curves are normalized. Moreover, we can compute a canonical basis of the n-torsion subgroup $E[n]$ defined over $\mathbb{F}_{p^2}$ by using [6, Algorithm 3].

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 [26]. 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. These computational costs are improved to $\tilde{O}(\sqrt{\ell})$ by Bernstein, De Feo, Leroux, and Smith [4].

For an isogeny $\varphi : A \to B$, we say that information $\mathcal{I}_\varphi$ is an *efficient representation* of φ when we can compute $\varphi(P)$ efficiently 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.

If A is the Jacobian of a hyperelliptic curve of genus two and $\ell = 2$ then we can compute $(2, 2)$-isogeny by formulas in Smith's Ph.D thesis [25]. Formulas of $(2, 2)$-isogenies for the case A is the product of two elliptic curves is given by Howe, Leprévost, and Poonen [16]. In 2023, more efficient formulas of $(2, 2)$-isogenies is proposed by Dartois, Maino, Pope, and Robert [10]. An algorithm to compute (ℓ, ℓ)-isogenies for a general ℓ was given by [8] and later improved by [19]. The computational cost of this algorithm is $O(\ell^2)$ operations on a field containing the points in G.

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 *canonical involution* 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 $\mathcal{O}$, the (integral) *left $\mathcal{O}$-ideal* I is a $\mathbb{Z}$-lattice of rank 4 satisfying $I \subset \mathcal{O}$ and $\mathcal{O} \cdot I \subset I$. The *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 ideal I, defined as (the unique positive generator of) $\mathbb{Z}$-module generated by the reduced norms of the elements of I. The 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 [13] showed that the endomorphism ring of a supersingular elliptic curve over $\mathbb{F}_{p^2}$ is isomorphic to a maximal order of $\mathcal{B}_{p,\infty}$ and gave a correspondence (*Deuring correspondence*) where a supersingular elliptic E curve over $\mathbb{F}_{p^2}$ corresponds to a maximal order isomorphic to $\mathrm{End}(E)$.

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

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

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

Eichler order and $\mathfrak{O} = \mathbb{Z} + I_\phi$ holds. Moreover, two isogenies $\phi, \psi : E_1 \to E_2$ that have same domain and codomain correspond to the equivalent ideals $I_\phi \sim I_\psi$.

Let I_τ be a connecting ideal of norm d from $\mathcal{O}_0 \cong \mathrm{End}(E_0)$ to $\mathcal{O}_1 \cong \mathrm{End}(E_1)$ and let $\tau : E_0 \to E_1$ be the corresponding isogeny. In our protocol, we need to compute the image under an endomorphism $\alpha_1 \in \mathrm{End}(E_1)$ represented as an element $\alpha \in \mathcal{O}_0 \cap \mathcal{O}_1$. Since $\alpha \in \mathcal{O}_0$, we can compute the image under the corresponding endomorphism $\alpha_0 \in \mathrm{End}(E_0)$ as described above. Then, if the order n of $P \in E_1$ is coprime to d, we can compute $\alpha_1(P)$ as follow:

$$\alpha_1(P) = \frac{1}{d} \tau \circ \alpha_0 \circ \hat{\tau}(P),$$

where $\dfrac{1}{d}$ is an inversion of d modulo n.

Algorithms Using Quaternion Algebra. As in the above, we let $\mathcal{O}_0$ be the maximal order of $\mathcal{B}_{p,\infty}$ with basis $(1, \mathbf{i}, \frac{\mathbf{i}+\mathbf{j}}{2}, \frac{1+\mathbf{k}}{2})$. Here, we introduce some existing algorithms using quaternion algebra necessary for the construction of our SQIsign2D-East. These algorithms are used in SQISign (see the official document [6] for detail).

- $\mathbf{RandomEquivalentIdeal}_M(I)$: Take an integer M and a left-$\mathcal{O}_0$ ideal I as input, output an uniformly random equivalent ideal $J \sim I$ such that $n(J) < M$. When $M \approx p^{1/2}$, there exists such an ideal J with the high probability.
- $\mathbf{FullRepresentInteger}_{\mathcal{O}_0}(M)$: Take an integer $M > p$ as input, output $\alpha \in \mathcal{O}_0$ such that $n(\alpha) = M$.
- $\mathbf{EichlerModConstraint}(I, \gamma, \delta)$: Take a left-$\mathcal{O}_0$ ideal I of prime norm N and $\gamma, \delta \in \mathcal{O}_0$ as input, output $(C_0 : D_0) \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ such that $\gamma(C_0\mathbf{j} + D_0\mathbf{k})\delta \in \mathbb{Z} + I$.
- $\mathbf{StrongApproximation}_M(N, C_0, D_0)$: Take integers M, N, C_0 and D_0 as input, 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 $\mu_1 \in \mathcal{O}_0$.

2.4 Computing Isogenies of Dimension one from Dimension Two

In this subsection, we give an algorithm to compute isogenies of dimension one by using an isogeny of dimension two, which is an important sub-algorithm for our protocol. This algorithm comes from recent attacks to SIDH by [5,20,24]. We use the following theorem, which is based on Kani's criterion [18].

Theorem 1 ([20, Theorem 1]). *Let N_1, N_2, and D be pairwise coprime integers such that $D = N_1 + N_2$, and let E_0, E_1, E_2, and E_3 be elliptic curves* *connected by the following diagram of isogenies:*

$$\begin{tikzcd} E_0 \arrow[r, "\psi_2"] \arrow[d, "\psi_1"'] & E_2 \arrow[d, "\psi_1'"] \\ E_1 \arrow[r, "\psi_2'"'] \arrow[ur, "f"] & E_3, \end{tikzcd}$$

where $\psi_2' \circ \psi_1 = \psi_1' \circ \psi_2$, $f = \psi_2 \circ \hat{\psi}_1$, $\deg(\psi_1) = \deg(\psi_1') = N_1$, *and* $\deg(\psi_2) = \deg(\psi_2') = N_2$. *Then, the isogeny*

$$\Phi = \begin{pmatrix} \hat{\psi}_1 & -\hat{\psi}_2 \\ \psi_2' & \psi_1' \end{pmatrix} : E_1 \times E_2 \to E_0 \times E_3 \tag{1}$$

is a (D, D)*-isogeny with respect to the natural product polarizations on* $E_1 \times E_2$ *and* $E_0 \times E_3$*, and has kernel* $\{([N_2]P, f(P)) \mid P \in E_1[D]\}$.

Conversely, a (D, D)-isogeny with kernel $\{([N_2]P, f(P)) \mid P \in E_1[D]\}$ is of the form $\iota \circ \Phi$ with an isomorphism ι from $E_0 \times E_3$. To construct algorithms to evaluate the isogenies in the matrix in Equation (1), we need to restrict the possibility of ι. In particular, we assume that the codomain E_3 of ψ_1' and ψ_2' is not isomorphic to E_0. This assumption is plausible because there exist about $p/12$ supersingular elliptic curves over $\mathbb{F}_{p^2}$ up to isomorphism and ψ_1' seems to be a random isogeny unless we intend to have $E_1 \cong E_3$. Under this assumption, an isomorphism from $E_0 \times E_3$ is represented by $\begin{pmatrix} \iota_0 & 0 \\ 0 & \iota_3 \end{pmatrix}$ or $\begin{pmatrix} 0 & \iota_3 \\ \iota_0 & 0 \end{pmatrix}$, where ι_0 is an isomorphism from E_0 and ι_3 is an isomorphism from E_3. Since we assume that E_0 and E_3 are normalized, we can determine the codomain of Φ in only two ways: $E_0 \times E_3$ or $E_3 \times E_0$.

Using Theorem 1 and assuming the above assumption, we construct an algorithm to evaluate the isogenies in the matrix in Equation (1) by computing a (D, D)-isogeny. We denote the algorithm by **KaniCod**.

Let N_1, N_2 be integers coprime with each other and $D = N_1 + N_2$. Let E_1, E_2 supersingular elliptic curves over $\mathbb{F}_{p^2}$, (P_1, Q_1) a basis of $E_1[D]$, (P_2, Q_2) a basis of $E_2[D]$, S_1 a finite subset of E_1, and S_2 a finite subset of E_2. If there exist isogenies $\psi_1 : E_0 \to E_1$ and $\psi_2 : E_0 \to E_2$ such that $\deg \psi_1 = N_1$ $\deg \psi_2 = N_2$, $P_2 = \psi_2 \circ \hat{\psi}_1(P_1)$, and $Q_2 = \psi_2 \circ \hat{\psi}_1(Q_1)$, then **KaniCod** with input $(N_1, N_2, E_1, E_2, P_1, Q_1, P_2, Q_2; S_1; S_2)$ returns the curve E_0, the image of S_1 under $\hat{\psi}_1$, and the image of S_2 under $\hat{\psi}_2$. If such isogenies do not exist then **KaniCod** returns $\perp$. The procedure for **KaniCod** is as follows:

1. Compute a (D, D)-isogeny Φ with kernel $\langle([N_2]P_1, P_2), ([N_2]Q_1, Q_2)\rangle$.
2. If the codomain of Φ is not the product of elliptic curves then return $\perp$.
3. Otherwise let $F_1 \times F_2$ be the codomain of Φ.
4. Let P_1' and Q_1' be first components of $\Phi((P_1, O_{E_2}))$ and $\Phi((Q_1, O_{E_2}))$.
5. Compute the D-Weil pairings $e_D(P_1, Q_1)$ and $e_D(P_1', Q_1')$.

6. If $e_D(P_1, Q_1)^{N_1} = e_D(P_1', Q_1')$ then return F_1 and the first components of $\Phi((R_1, O_{E_2}))$ and $\Phi((O_{E_1}, R_2))$ for $R_1 \in S_1$ and $R_2 \in S_2$.
7. If $e_D(P_1, Q_1)^{N_2} = e_D(P_1', Q_1')$ then return F_2 and the second components of $\Phi((R_1, O_{E_2}))$ and $\Phi((O_{E_1}, R_2))$ for $R_1 \in S_1$ and $R_2 \in S_2$.
8. Otherwise, return $\perp$.

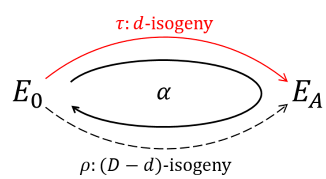
When D is smooth, $P_1, Q_1 \in E_1(\mathbb{F}_{p^2})$, $S_1 \subset E_1(\mathbb{F}_{p^2})$, $P_2, Q_2 \in E_2(\mathbb{F}_{p^2})$, and $S_2 \subset E_2(\mathbb{F}_{p^2})$ the computational costs of **KaniCod** are $O((\#S_1 + \#S_2) \log D)$ operations on $\mathbb{F}_{p^2}$ by using the methods stated in Section 2.2. Especially, D is a power of 2 in our case.

2.5 RandIsogImg

Here, we describe the conventional algorithm **RandIsogImg** which evaluates the codomain of a random isogeny of *non-smooth* degree and some point images under the isogeny. This algorithm was proposed in the paper of QFESTA [22] and is an important component of our SQIsign2D-East.

Let E_0 be the elliptic curve over $\mathbb{F}_{p^2}$ defined as $E_0 : y^2 = x^3 + x$. Let D be a smooth integer satisfying $E_0[D] \subset E_0(\mathbb{F}_{p^2})$ and $D \approx p$, and let d be an integer coprime to D satisfying $D - d \approx p$. **RandIsogImg** takes integers d, D satisfying these conditions and a finite subset S of E_0 as input, and outputs the codomain of a random d-isogeny τ and the images of the points in S under τ.

In this algorithm, we first compute an endomorphism $\alpha \in \mathrm{End}(E_0)$ of degree $d \cdot (D - d)$ using **FullRepresentInteger** and decompose it into $\alpha = \hat{\rho} \circ \tau$, where τ and ρ are the isogenies whose domains are E_0 and whose degrees are d and $D - d$, respectively. (See the following diagram.) Since $\deg \tau + \deg \rho = D$ and $\gcd(\deg \tau, \deg \rho) = 1$, we can evaluate point images under the isogeny τ by using **KaniCod**. We describe the pseudo code of **RandIsogImg** in Algorithm 1.



Algorithm 1 $\mathbf{RandIsogImg}_{\mathcal{O}_0}(d, D; S)$

Require: Relatively prime Integers d, D such that $D - d \approx p$ and $E_0[D] \subset E_0(\mathbb{F}_{p^2})$ and a finite subset $S \subset E_0$.
Ensure: $(E_A, \tau(S))$ for a random d-isogeny $\tau : E_0 \to E_A$.
Let $\alpha \leftarrow \mathbf{FullRepresentInteger}_{\mathcal{O}_0}(d \cdot (D - d))$.
Take a basis P_0, Q_0 of $E_0[D]$.
$(E_A, \tau(S), \emptyset) \leftarrow \mathbf{KaniCod}(d, D - d, E_0, E_0, P_0, Q_0, \alpha(P_0), \alpha(Q_0); S; \emptyset)$.
return $(E_A, \tau(S))$.

In addition, we can compute the left $\mathcal{O}_0$-ideal $I_\tau = \mathcal{O}_0\langle \alpha, d \rangle$, which corresponds to the isogeny τ. We denote the algorithm which outputs $(E_A, \tau(S), I_\tau)$ by **RandIsogImgWithIdeal**.

2.6 SQIsignHD

SQIsignHD is a signature scheme proposed in [9] in 2023, which is based on SQIsign and utilizes an attack on SIDH to achieve a smaller signature length than SQIsign. There are two types of SQIsignHD, one using 4-dimensional isogenies and the other using 8-dimensional isogenies for the verification. In this section, we introduce an overview of SQIsignHD using 4-dimensional isogenies. For more details, refer to [9].

First, we show the system parameters of SQIsignHD. Let a, b be integers satisfying $2^a \approx 3^b \approx 2^\lambda$, and let p be a prime satisfying $p = 2^a 3^b f - 1$ for a sufficiently small integer f. Let E_0 be the elliptic curve over $\mathbb{F}_{p^2}$ defined as $E_0 : y^2 = x^3 + x$. Furthermore, we say that an odd integer q is 2^a*-good* if there exist integers m_1, m_2 satisfying $m_1^2 + m_2^2 = 2^a - q$.

SQIsignHD is obtained by applying Fiat-Shamir transform [15] on the identification scheme based on the following diagram. In the following, we describe the

$$\begin{tikzcd} E_0 \arrow[r, dashed, "\psi"] \arrow[d, dashed, "\tau"'] & E_1 \arrow[d, "\phi"] \\ E_A \arrow[r, "\sigma"] & E_2 \end{tikzcd}$$

τ: secret key
ψ: commitment
ϕ: challenge
σ: response

overview of SQIsignHD identification protocol, which is similar to our protocol.

keygen: The prover generates a random 3^{2b}-isogeny $\tau : E_0 \to E_A$ and publishes the curve E_A as the public key.

commit: The prover generates a random 3^{2b}-isogeny $\psi : E_0 \to E_1$ and sends E_1 to the verifier as the commitment.

challenge: The verifier generates a random 3^b-isogeny $\phi : E_1 \to E_2$ and sends it to the prover.

response: The prover computes the ideal J corresponds to $\phi \circ \psi \circ \hat{\tau}$ and finds a random equivalent ideal $I_\sigma \sim J$ whose norm q is 2^a-good. Then, the prover sends to the verifier an efficient representation of the q-isogeny $\sigma : E_A \to E_2$ corresponds to I_σ.

verify: The verifier checks that the response send by the prover correctly represents a q-isogeny $\sigma : E_A \to E_2$.

As an efficient representation of the q-isogeny σ, the prover sends $(q, \sigma|_{E_A[2^a]})$. Then, the verifier recovers the isogeny σ using Theorem 1. To apply Theorem 1, the verifier needs to compute a $(2^a - q)$-isogeny from E_A. However, this task is hard since the degree $2^a - q$ is generally non-smooth. The verifier instead computes the 2-dimensional endomorphism over $E_A \times E_A$ of degree $2^a - q$ as follows:

1. Find two integers m_1, m_2 satisfying $m_1^2 + m_2^2 + q = 2^a$.

2. Let ω be the 2-dimensional endomorphism of degree $m_1^2+m_2^2 = 2^a - q$ defined as follow:
$$\omega = \begin{pmatrix} m_1 & -m_2 \\ m_2 & m_1 \end{pmatrix}.$$

Let I_2 be the 2×2 identity matrix. Under the following diagram, the verifier can recover σ by computing 4-dimensional 2^a-isogeny. In this step, the verifier uses an extension of Theorem 1 to higher dimension by Robert [24].

$$\begin{tikzcd}
E_A \times E_A \arrow[r, "\sigma I_2"] \arrow[d, "\omega"'] & E_2 \times E_2 \arrow[d, "\omega'"] \\
E_A \times E_A \arrow[r, "\sigma I_2"'] & E_2 \times E_2.
\end{tikzcd}$$

Security. In [9], the following oracle and problem are defined to discuss the security of SQIsignHD.

Definition 1 *A random uniform good degree isogeny oracle (RUGDIO) is an oracle taking as input a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$ and returning an efficient representation of a random isogeny $\sigma : E \to E'$ of 2^e-good degree prime to 3 such that:*

(i) The distribution of E' is uniform in the supersingular isogeny graph.
(ii) The conditional distribution of σ given E' is uniform among isogenies $E \to E'$ of 2^e-good degree prime to 3.

Problem 1 (Supersingular Endomorphism Problem) *Given a supersingular elliptic curve $E/\mathbb{F}_{p^2}$, find an efficient representation of a non-scalar endomorphism $\alpha \in \mathrm{End}(E)$.*

Then, SQIsignHD is proven to be universally unforgeable under chosen message attacks secure in the random oracle model under the following assumptions.

Assumption 1 *The commitment curve E_1 is computationally indistinguishable from an elliptic curve chosen uniformly at random in the supersingular isogeny graph.*

Assumption 2 *Problem 1 is computationally hard to solve even with the access to the RUGDIO.*

3 Building Block for SQIsign2D-East

In this section, we give an algorithmic building block for SQIsign2D-East. We assume that we have a prime $p = 2^{a+b}f - 1$ with $a \approx b \approx \lambda$ and $c \in \mathbb{N}$ as small as possible. We use the same notation $q := \deg(\sigma)$ as in subsection 2.6. Note that the degree q is approximately $p^{1/2}$. In SQIsignHD, the verifier required a

4-dimensional isogeny computations since the auxiliary path ω of degree $(2^a - q)$ is a 2-dimensional isogeny. Our main idea is to generate the auxiliary path ω as 1-dimensional isogeny of degree $2^a - q$ using **RandIsogImg**. However, the conventional **RandIsogImg** can only compute an isogeny from a specific elliptic curve E_0. Since the auxiliary path we need is the isogeny from the public key E_A, we have to construct a generalized **RandIsogImg**.

3.1 Generalized RandIsogImg

We construct a generalized **RandIsogImg** so that we can compute an isogeny from arbitrary curves. Let E be an elliptic curve isogenous to E_0 and let $\mathcal{O} \cong \mathrm{End}(E)$. Let τ be an N-isogeny from E_0 to E and let I_τ be a left $\mathcal{O}_0$-ideal corresponding to τ. We propose an algorithm to compute an isogeny of non-smooth degree from E.

In the procedure of $\mathbf{RandIsogImg}_{\mathcal{O}_0}(d, D; S)$, we use $\mathcal{O}_0$ only in step 1, where we find $\alpha \in \mathcal{O}_0$ satisfying $n(\alpha) = d \cdot (D - d)$. Therefore, to construct a generalized **RandIsogImg**, we have to find $\alpha \in \mathcal{O}$ satisfying $n(\alpha) = d \cdot (D - d)$. This can be achieved by using **EichlerModConstraint** and **StrongApproximation** as follows:

1. Using $\mathbf{EichlerModConstraint}(I_\tau, 1, 1)$, obtain $(C_0 : D_0) \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ such that $C_0 j + D_0 k \in \mathbb{Z} + I_\tau = \mathcal{O}_0 \cap \mathcal{O}$.
2. Using $\mathbf{StrongApproximation}_{d(D-d)}(N, C_0, D_0)$, we can find $\alpha \in \mathcal{O}_0 \cap \mathcal{O}$ satisfying $n(\alpha) = M$.

The above approach is used in the key generation algorithm of SQIsign [12]. Since we use **StrongApproximation**, the degree N of τ must be prime and $d(D - d) > pN^3$ must hold. If we assume that $D - d \approx p$ as with the original **RandIsogImg**, the requirement on the degree d will be $d > N^3$. In addition, if we fix D around p, the condition $D - d \approx d$ holds for almost all d satisfying $d < D$. From the above argument, a generalized **RandIsogImg** for E is as shown in Algorithm 2.

Algorithm 2 $\mathbf{GenRandIsogImg}_{\tau, I_\tau}(d, D; S)$

Require: An isogeny $\tau : E_0 \to E$ of prime degree N, its corresponding ideal I_τ, relatively prime integers d, D such that $D \approx p$, $d > N^3$, $d < D$, and $E[D] \subset E(\mathbb{F}_{p^2})$, and a finite set $S \subset E$.

Ensure: $(F, \iota(S))$ for a random d-isogeny $\iota : E \to F$.

1: $(C_0 : D_0) \leftarrow \mathbf{EichlerModConstraint}(I_\tau, 1, 1)$.
2: $\alpha \leftarrow \mathbf{StrongApproximation}_{d \cdot (D-d)}(N, C_0, D_0)$.
3: Let P, Q be a basis of $E[D]$.
4: $(F; \iota(S); \emptyset) \leftarrow \mathbf{KaniCod}(d, D - d, E, E, P, Q, \alpha(P), \alpha(Q); S, \emptyset)$.
5: **return** $(F, \iota(S))$.

3.2 Computing Auxiliary Path

Unfortunately, the requirement $d > N^3$ is too strong to compute an auxiliary path of degree $d = 2^a - q \approx p^{1/2}$. To allow the use of smaller d, we take the following approach:

1. Let D_1 be a smooth integer such that $d(D_1 - d) > N^3$ and $d(D_1 - d) < D$.
2. Compute a $d(D_1 - d)$-isogeny using **GenRandIsogImg**.
3. By computing a (D_1, D_1)-isogeny, obtain a d-isogeny.

Then, the lower bound of d decreases from N^3 to approximately N^3/D_1.

Remark 1. Strictly speaking, the lower bound of d is $B = D_1/2 - \sqrt{(D_1/2)^2 - N^3} = (D_1/2) \cdot (1 - \sqrt{1 - 4N^3/D_1^2})$. Especially when $D_1^2 \gg N^3$, we have $B \approx N^3/D_1$, where we used $\sqrt{1-\epsilon} \approx 1 - \epsilon/2$ for $\epsilon \ll 1$.

We show the algorithm to compute an auxiliary path in Algorithm 3.

Algorithm 3 $\textbf{AuxiliaryPath}_{\tau, I_\tau}(d, D_1, D; S)$

Require: An isogeny $\tau : E_0 \to E$ of prime degree N, its corresponding ideal I_τ, integers d, D_1, D such that d is coprime to both D_1 and D, $D \approx p$, $d(D_1 - d) > N^3$, $d(D_1 - d) < D$, and $E[D] \subset E(\mathbb{F}_{p^2})$, and a finite set $S \subset E$.
Ensure: $(F, \omega(S))$ for a random d-isogeny $\omega : E \to F$.
1: Let P, Q be a basis of $E[D_1]$.
2: $(F', \iota(P), \iota(Q)) \leftarrow \textbf{GenRandIsogImg}_{I_\tau}(d(D_1 - d), D; P, Q)$.
3: $(F; \omega(S); \emptyset) \leftarrow \textbf{KaniCod}(d, D_1 - d, E, F', P, Q, \iota(P), \iota(Q); S; \emptyset)$.
4: **return** $(F, \omega(S))$.

Especially in our protocol, we use $D_1 = 2^a \approx p^{1/2}$ and $D = 2^{a+b} \approx p$. Since the degree $d = 2^a - q$ of the auxiliary path we need is around $p^{1/2}$, we have $d(D_1 - d) \approx p$ for almost all $d < D_1$. Hence, the condition $d(D_1 - d) > N^3$ is satisfied when $N < p^{1/3}$.

Now the remaining requirements on the degree d are as follows:

$$d \text{ is odd integer smaller than } 2^a,$$
$$d(2^a - d) < 2^{a+b}.$$

Since $d = 2^a - q$, the requirements on the degree q of σ are also as follows:

$$q \text{ is odd integer smaller than } 2^a,$$
$$q(2^a - q) < 2^{a+b}.$$

When q satisfies the above conditions, we say that q is '$(2^a, 2^b)$-nice'

Remark 2. The odd integer $q < 2^a$ is always $(2^a, 2^b)$-nice when $a \le b + 2$ from the following inequality:

$$q \cdot (2^a - q) = 2^{2a-2} - (2^{a-1} - q)^2 < 2^{2a-2} \le 2^{a+b}.$$

Additional constraint on the norm q. In fact, there is an additional constraint on the norm q other than the $(2^a, 2^b)$-niceness. In Algorithm 2, we use $\mathbf{StrongApproximation}_{d(2^{a+b}-d)}(N, C_0, D_0)$ with $d = q(2^a - q)$, $N = N_\tau$, and $(C_0, D_0) \leftarrow \mathbf{EichlerModConstraint}(I_\tau, 1, 1)$ to generate an auxiliary path. Then, $\mathbf{StrongApproximation}_{d(2^{a+b}-d)}(N, C_0, D_0)$ outputs $\mu \in \mathcal{O}_0$ such that

$$n(\mu) = d(2^{a+b} - d) \text{ and } \mu = m(C_0\mathbf{j} + D_0\mathbf{k}) + N_\tau \mu_1,$$

where $m \in \mathbb{Z}$ and $\mu_1 \in \mathcal{O}_0$. Therefore, the following equation holds:

$$n(\mu) = m^2 p(C_0^2 + D_0^2) = d(2^{a+b} - d) \mod N_\tau.$$

For such an integer m to exist, the following condition must be satisfied:

$$\left(\frac{d(2^{a+b} - d)}{N_\tau}\right) = \left(\frac{p(C_0^2 + D_0^2)}{N_\tau}\right),$$

where $\left(\frac{a}{N}\right)$ is the quadratic residue symbol. On the other hand, from the definition of **EichlerModConstraint**, there exists an integer m' satisfying

$$m' + C_0\mathbf{j} + D_0\mathbf{k} \in I_\tau.$$

Hence, we have

$$n(m' + C_0\mathbf{j} + D_0\mathbf{k}) = (m')^2 + p(C_0^2 + D_0^2) = 0 \mod N_\tau,$$

which means that

$$\left(\frac{p(C_0^2 + D_0^2)}{N_\tau}\right) = \left(\frac{-1}{N_\tau}\right).$$

Summarizing the above discussion, $d = q(2^a - q)$ must satisfy

$$\left(\frac{d(2^{a+b} - d)}{N_\tau}\right) = \left(\frac{-1}{N_\tau}\right).$$

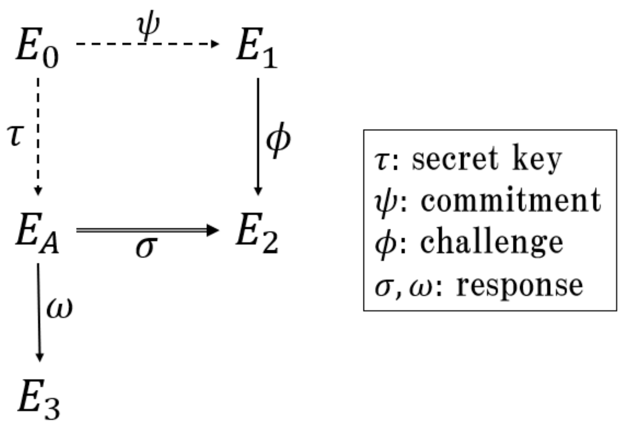
This condition is expected to hold with approximately 1/2 probability. We say the integer q is '$(2^a, 2^b, N_\tau)$-nice' when q is $(2^a, 2^b)$-nice and satisfies the above condition.

4 New Signature Scheme: SQIsign2D-East

In this section, we describe our new signature scheme SQIsign2D-East. First, we describe the detailed algorithm for SQIsign2D-East and then we propose its variant named 'CompactSQIsign2D-East', which has smaller signature size than the original SQIsign2D-East.

4.1 Description of SQIsign2D-East

We first describe the identification protocol underlying SQIsign2D-East. SQIsign2D-East identification protocol is based on the following diagram.



We show the algorithms for the SQIsign2D-East identification scheme blow.

Parameter setting. The public parameter of SQIsign2D-East is taken as follows:

1. Let p be a prime of the form $p = 2^{a+b}f - 1$, where f is a small integer and $a \approx b \approx \lambda$.
2. Let E_0 be the elliptic curve over $\mathbb{F}_{p^2}$ defined as $E_0 : y^2 = x^3 + x$.
3. Let P_0, Q_0 be a basis of $E_0[2^{a+b}]$.
4. Let $\mathcal{O}_0 = \mathbb{Z}\langle 1, \mathbf{i}, \frac{\mathbf{i}+\mathbf{j}}{2}, \frac{1+\mathbf{k}}{2} \rangle$, which is isomorphic to $\mathrm{End}(E_0)$.
5. Let $\mathrm{param} = (p, a, b, E_0, P_0, Q_0, \mathcal{O}_0)$.

Key generation. As we stated in subsection 3.2, we have to take the degree N_τ of the secret isogeny τ smaller than $p^{1/3}$. Fortunately, we can take N as small as approximately $p^{1/4}$ while achieving λ-bits security as follows:

1. Take a random prime $N < p^{1/4}$.
2. Compute a random N-isogeny $\tau : E_0 \to E$.

This method is also used in the key generation of SQIsign [11].

Since N_τ is a large prime, we cannot compute τ efficiently from $\ker \tau$ using Vélu's formulas. Instead, we compute an efficient representation $(N_\tau, \tau(P_0), \tau(Q_0))$ of τ using **RandIsogImg**. By using $(N_\tau, \tau(P_0), \tau(Q_0))$, we can efficiently compute $\tau(T_0)$ for any $T_0 \in E_0[2^{a+b}]$ as follow:

1. Compute $s, t \in \mathbb{Z}/2^{a+b}\mathbb{Z}$ such that $T_0 = sP_0 + tQ_0$.

2. Return $\tau(T_0) = s\tau(P_0) + t\tau(Q_0)$.

Now we show the key generation algorithm in Algorithm 4.

Algorithm 4 keygen(param) $\to (pk, sk)$

Require: Public parameter param $= (p, a, b, E_0, P_0, Q_0, \mathcal{O}_0)$.
Ensure: Public key pk and secret key sk.
1: Take a random prime $N_\tau < p^{1/4}$.
2: $(E_A, R_A, S_A, I_\tau) \leftarrow$ **RandIsogImgWithIdeal**$_{\mathcal{O}_0}(N_\tau, 2^{a+b}; P_0, Q_0)$.
3: **return** $pk = E_A, sk = (\tau = (N_\tau, R_A, S_A), I_\tau)$.

Commitment. The commitment phase is similar to the key-generation. However, the degree N_ψ need not to be prime smaller than $p^{1/4}$ unlike N_τ. Hence, we just chose an odd integer N_ψ smaller than $2^{2\lambda}$.

As with the key generation, we compute $(N_\psi, \psi(P_0), \psi(Q_0))$ as an efficient representation of ψ using **RandIsogImg**. As described above, we can efficiently evaluate ψ over the 2^{a+b}-torsion subgroup using this representation. In addition, we can compute $\hat{\psi}(T_1)$ for any $T_1 \in E_1[2^{a+b}]$, where E_1 is the codomain of ψ as follow:

1. Compute $s, t \in \mathbb{Z}/2^{a+b}\mathbb{Z}$ such that $T_1 = s\psi(P_0) + t\psi(Q_0)$.
2. Return $\hat{\psi}(T_A) = sN_\psi P_0 + tN_\psi Q_0$.

Now, we show the commitment algorithm in Algorithm 5.

Algorithm 5 commit(param) $\to (com, s)$

Require: Public parameter param.
Ensure: Commitment com and secret information s.
1: Take a random odd integer $N_\psi < 2^{2\lambda}$.
2: $(E_1, R_1, S_1, I_\psi) \leftarrow$ **RandIsogImgWithIdeal**$_{\mathcal{O}_0}(N_\psi, 2^{a+b}; P_0, Q_0)$.
3: **return** $com = E_1, s = (\psi = (N_\psi, R_1, S_1), I_\psi)$.

Remark 3. We can fix N_ψ to an odd integer around $2^{2\lambda}$ and include it in the system parameter without any security loss.

Challenge. We just compute a random 2^b-isogeny from E_1 using Vélu's formulas. We show the challenge algorithm in Algorithm 6.

Response. In the response phase, we first compute the ideal I_ϕ. This can be done by using **IsogToIdeal** algorithm [9, Algorithm 10], which takes two isogenies $\psi : E_0 \to E_1$ and $\phi : E_1 \to E_2$ and the ideal I_ψ corresponds to ψ as input and return the ideal I_ϕ corresponds to ϕ. Then, we compute the ideal J corresponds to $\phi \circ \psi \circ \hat{\tau}$ and finds a random equivalent ideal $I_\sigma \sim J$ whose

Algorithm 6 **challenge**$(pk, \text{param}) \to ch$

Require: Public key pk and public parameter param.
Ensure: Challenge ch.
1: Take a random integer $u \in_U \mathbb{Z}/2^b\mathbb{Z}$.
2: Let P_1', Q_1' be the canonical basis of $E_1[2^b]$.
3: $K_1' \leftarrow P_1' + uQ_1'$.
4: **return** $ch = K_1'$, a generator of the kernel of $\phi : E_1 \to E_2$.

norm q is $(2^a, 2^b, N_\tau)$-nice. Next, we compute an efficient representation of the q-isogeny $\sigma : E_A \to E_2$ corresponds to I_σ. Finally, we generate an auxiliary path $\omega : E_A \to E_3$ and return an efficient representation of $\sigma \circ \hat{\omega}$. We show the response algorithm in Algorithm 7.

Algorithm 7 **response**$(sk, s, ch, \text{param}) \to resp$

Require: Secret key sk, secret information s, challenge ch, and public parameter param.
Ensure: Response $resp$.
1: Let $I_\phi \leftarrow$ **IsogToIdeal**(ϕ, ψ, I_ψ).
2: Let $J = \bar{I}_\tau I_\psi I_\phi$ and $I_\sigma = J\dfrac{\bar{\alpha}}{N_\tau N_\psi 2^b} \leftarrow$ **RandomEquivalentIdeal**$_{2^a}(J)$.
3: Let $q = n(I_\sigma)$ and $r = 2^a - q$. (If q is not $(2^a, 2^b, N_\tau)$-nice, go back to step 2.)
4: Let P_A, Q_A be the canonical basis of $E_A[2^{a+b}]$ and let $(P_A', Q_A') = 2^b(P_A, Q_A)$.
5: Compute $R_2' = \frac{1}{N_\tau N_\psi}\phi \circ \psi \circ \hat{\tau} \circ \hat{\alpha}(P_A)$ and $S_2' = \frac{1}{N_\tau N_\psi}\phi \circ \psi \circ \hat{\tau} \circ \hat{\alpha}(Q_A)$.
6: Let $(E_3, R_3', S_3') \leftarrow$ **AuxiliaryPath**$_{I_\tau}(r, 2^a, 2^{a+b}; P_A', Q_A')$.
7: Let P_3', Q_3' be the canonical basis of $E_3[2^a]$ and compute the change of basis matrix M such that $(P_3', Q_3') = (R_3', S_3')M$.
8: Compute $(U_2', V_2') = -(R_2', S_2')M$.
9: **return** $resp = (E_3, U_2', V_2')$.

Applying the Deuring correspondence on the equation $I_\sigma = \bar{I}_\tau I_\psi I_\phi \cdot \frac{\bar{\alpha}}{N_\tau N_\psi 2^b}$ in step 2, we obtain the following equation:

$$\sigma \circ [2^b] = \frac{1}{N_\tau N_\psi}\phi \circ \psi \circ \hat{\tau} \circ \hat{\alpha}.$$

Therefore, the point R_2' in step 5 in Algorithm 7 satisfies the following equation:

$$\begin{aligned} R_2' &= \frac{1}{N_\psi N_\tau}\phi \circ \tau \circ \hat{\psi} \circ \hat{\alpha}(P_A) \\ &= \sigma(2^b P_A) \\ &= \sigma(P_A'). \end{aligned}$$

Similarly, $S_2' = \sigma(Q_A')$ also holds. In step 7, we compute $R_3' = \omega(P_A')$ and $S_3' = \omega(Q_A')$ for an r-isogeny $\omega : E_A \to E_3$. From the equation $(P_3', Q_3') = (R_3', S_3')M = (\omega(P_A'), \omega(Q_A'))M$ in step 7, the following equation holds:

$$(\hat{\omega}(P_3'), \hat{\omega}(Q_3')) = (rP_A', rQ_A')M = (-qP_A', -qQ_A')M,$$

where we used $r = 2^a - q \equiv -q \mod 2^a$. By taking the image under the isogeny σ of both sides, we obtain

$$(\sigma \circ \hat{\omega}(P'_3), \sigma \circ \hat{\omega}(Q'_3)) = (-qR'_2, -qS'_2)M.$$

Therefore, we obtain the following equation:

$$(U'_2, V'_2) = -(R'_2, S'_2)M = \left(\frac{1}{q}\sigma \circ \hat{\omega}(P'_3), \frac{1}{q}\sigma \circ \hat{\omega}(Q'_3)\right). \tag{2}$$

Verify. We show the response algorithm in Algorithm 8.

Algorithm 8 verify$(pk, com, ch, resp, \text{param}) \to$ accept/reject

Require: Public key pk, commitment com, challenge ch, response $resp$, and public parameter param.
Ensure: accept or reject.
1: Let P'_3, Q'_3 be the canonical basis of $E_3[2^a]$.
2: Compute a $(2^a, 2^a)$-isogeny $\Phi : E_3 \times E_2 \to A$ with kernel $K = \langle (P'_3, U'_2), (Q'_3, V'_2) \rangle$.
3: **if** $A \cong E_A \times F$ or $A \cong F \times E_A$ for an elliptic curve F **then**
4: **return** accept.
5: **else**
6: **return** reject.
7: **end if**

Correctness. We prove that SQIsign2D-East is correct. Assume here that the prover computes the response honestly. From Equation 2, the subgroup K of $E_A \times F$ satisfies the following equation:

$$\begin{aligned} K &= \langle (P'_3, U'_2), (Q'_3, V'_2) \rangle \\ &= \left\langle \left(P'_3, \frac{1}{q}\sigma \circ \hat{\omega}(P'_3)\right), \left(Q'_3, \frac{1}{q}\sigma \circ \hat{\omega}(Q'_3)\right) \right\rangle \\ &= \langle (qP'_3, \sigma \circ \hat{\omega}(P'_3)), (qQ'_3, \sigma \circ \hat{\omega}(Q'_3)) \rangle. \end{aligned}$$

Let $\sigma' = [\omega]_*\sigma, \omega' = [\sigma]_*\omega$, and F be the codomain of σ' and ω'. From Theorem 1, a $(2^a, 2^a)$-isogeny Φ with kernel K has the following form:

$$\Phi = \begin{pmatrix} \hat{\omega} & -\hat{\sigma} \\ \sigma' & \omega' \end{pmatrix} : E_3 \times E_2 \to E_A \times F$$

up to isomorphism. Therefore, the verifier accepts the honest response.

4.2 Reducing Signature Size

Applying the Fiat-Shamir transform, the signature of our protocol is made of the data (E_1, E_3, R'_2, S'_2), where E_1 is the commitment elliptic curve, E_3 is the codomain of the auxiliary path, and $R'_2, S'_2 \in E_2[2^a]$. E_1 and E_3 can be determined by their j-invariant $j(E_1), j(E_3) \in \mathbb{F}_{p^2}$. Therefore, storing E_1 and E_3 takes $2\log_2 p^2 \approx 8\lambda$ bits. The points R'_2 and S'_2 can be compressed as SIKE. Using this compression, R'_2 and S'_2 requires $4a \approx 4\lambda$ bits. Totally, the signature size is 12λ bits.

Actually, we can reduce the signature size by about 2λ bits by using the same method as SQIsign: include $\ker \hat{\phi}$ instead of the commitment E_1 in the signature. We name this variant 'CompactSQIsign2D-East'. To apply this method, we compute $\omega' = [\sigma]_*\omega$ using **KaniCod**. Now we explain how the CompactSQIsign2D-East works. Let $H : \{0,1\}^* \times \mathbb{F}_{p^2} \to \mathbb{Z}/2^b\mathbb{Z} \times \{0,1\}$ be a cryptographic hash function and let **GenKernel** be an algorithm defined as follows:

GenKernel$(m, E_1) \to K'_1$:

1. $h, \mathrm{bin} \leftarrow H(m, j(E_1))$.
2. Let P'_1, Q'_1 be the canonical basis of $E_1[2^b]$.
3. If $\mathrm{bin} = 0$, return $K'_1 = hP'_1 + Q'_1$.
4. Otherwise, return $K'_1 = P'_1 + hQ'_1$.

In the following, we regard $\mathbb{F}_{p^2}$ as a totally ordered set under an appropriate order relation. We show the explicit algorithms for CompactSQIsign2D-East in Algorithm 9 and 10. Note that the key generation algorithm for CompactSQIsign2D-East is same as Algorithm 4.

Next, we discuss the signature size of CompactSQIsign2D-East. The reduced signature of CompactSQIsign2D-East is made of the data $(E_4, R'_4, S'_4, b_2, s_2, t_1)$, where $(R'_4, S'_4) = ([r^{-1}] \circ \omega' \circ \sigma(P'_A), [r^{-1}] \circ \omega' \circ \sigma(Q'_A))$ for the canonical basis P'_A, Q'_A of $E_A[2^a]$, b_2 is a bit, and s_2, t_1 are two elements of $\mathbb{Z}/2^a\mathbb{Z}$, Therefore, the signature size is $\log_2 p^2 + 4a + 1 + a + a \approx 10\lambda$ bits.

4.3 Increasing the possibility that there exists an equivalent ideal I_σ whose norm q is $(2^a, 2^b, N_\tau)$-nice

In step 2 and 3 of the response algorithm shown in Algorithm 7, we have to find an equivalent ideal I_σ whose norm q is $(2^a, 2^b, N_\tau)$-nice. If there is no such an ideal, we fail the response and have to return to the commitment phase. To avoid the failure of the response or reduce the possibility of failure at least, we discuss how to increase the possibility that there exists an equivalent ideal I_σ whose norm q is $(2^a, 2^b, N_\tau)$-nice.

From now on, we assume that $b \le a - 2$, which means that about half of odd integers smaller than 2^a are $(2^a, 2^b, N_\tau)$-nice (see Remark 2). In the previous subsections, we have assumed that there exists an equivalent ideal I_σ whose norm q is odd and $q < 2^a$ in high probability, since $2^a \approx p^{1/2}$. Strictly speaking, however, 2^a is less than $p^{1/2}$ when $f > 4$ since $p = 2^{a+b}f - 1 = 2^{2a-2}f - 1$. Therefore, depending on the value of f, the probability of existing such an ideal I_σ becomes small. We give two solutions for this problem below:

(i) Use $q' = q/\gcd(q, f)$ instead of q. This reduces the constraint of q from $q < 2^a$ to $q' < 2^a \Leftrightarrow q < \gcd(q, f) \cdot 2^a$.

Algorithm 9 $\textbf{CompactSign}(pk, sk, m, \text{param}) \to sig$

Require: The public key pk, the secret key sk, the message m, and the public parameter param.
Ensure: The signature sig.

```
(E_1, N_ψ, R_1, S_1, I_ψ) ← commit(param).
K'_1 ← GenKernel(m, E_1).
For the canonical basis P'_2, Q'_2 of E_2[2^a], find u, v satisfying ker(ψ̂) = ⟨uP'_2 + vQ'_2⟩.

if 2|u then
    s ← uv^{-1}, bin_1 ← 0.
    Find t satisfying K'_1 = tφ̂(P'_2).
else
    s ← u^{-1}v, bin_1 ← 1.
    Find t satisfying K'_1 = tφ̂(Q'_2).
end if
Compute P'_3, Q'_3, R'_2, S'_2, and resp = (E_3, U'_2, V'_2) using Algorithm 7.
(E_4; ∅; R'_4, S'_4) ← KaniCod(q, r, E_3, E_2, P'_3, Q'_3, U'_2, V'_2; ∅; R'_2, S'_2).
Let M_3 and M_4 be the Montgomery coefficient of E_3 and E_4, respectively.
if M_3 ≤ M_4 then
    bin_2 ← 0.
else
    bin_2 ← 1.
end if
return sig = (E_4, R'_4, S'_4, bin_1, bin_2, s, t).
```

(ii) Allow q to be even. This makes the number of usable q about twice.

In our implementation, we only used the method (i). In the following, we explain the method (i) in detail. The method (ii) is described in Appendix A.

Let σ be a q-isogeny computed as in Algorithm 7. Let $g = \gcd(q, f)$, $q = g \cdot q'$, and $r = 2^a - q'$. We formally decompose the q-isogeny σ to a g-isogeny $\sigma_g : E_A \to E'_A$ and a q'-isogeny $\sigma' : E'_A \to E_2$. The procedure of the method (ii) is as follows:

1. Compute $\ker \sigma_g$ by evaluating σ over $E_A[g]$.
2. Compute $\sigma_g : E_A \to E'_A$ using Vélu's formulas.
3. Obtain a r-isogeny $\omega : E_A \to E_3$ using **AuxiliaryPath**.
4. Let $\sigma'_g = [\omega]_* \sigma_g$.
5. Compute $\ker \sigma'_g = \omega(\ker \sigma_g)$.
6. Compute $\sigma'_g : E_3 \to E'_3$ using Vélu's formulas.
7. Evaluate σ' and ω' over $E'_A[2^a]$ by using $\sigma' = \dfrac{1}{g}\sigma \circ \hat{\sigma_g}$ and $\omega' = \dfrac{1}{g}\sigma'_g \circ \omega \circ \hat{\sigma_g}$.

When using this method, we have to include a generator of $\ker \sigma_g$ to the signature.

Algorithm 10 **CompactVerify**$(pk, m, sig, \mathrm{param}) \to$ accept/reject

Require: The public key pk, the message m, the signature sig, and the public parameter param.
Ensure: accept or reject.

Let P'_A, Q'_A be the canonical basis of $E_A[2^a]$.
Compute a $(2^a, 2^a)$-isogeny $\Phi : E_A \times E_4 \to A$ with kernel $\langle (P'_A, R'_4), (Q'_A, S'_4) \rangle$.
if not $A \cong F_0 \times F_1$ for elliptic curves F_0 and F_1 **then**
  return reject.
end if
Let M_0 and M_1 be the Montgomery coefficient of F_0 and F_1, respectively.
if $M_0 > M_1$ **then**
  $F_0, F_1 \leftarrow F_1, F_0$.
end if
$E_2 \leftarrow F_{\mathrm{bin}_2}$.
Let P'_2, Q'_2 be the canonical basis of $E_2[2^a]$.
if $\mathrm{bin}_1 = 0$ **then**
  Compute a 2^a-isogeny $\hat{\phi} : E_2 \to E_1 = E_2/\langle sP'_2 + Q'_2 \rangle$.
  $L'_1 \leftarrow \hat{\phi}(P'_2)$.
else
  Compute a 2^a-isogeny $\hat{\phi} : E_2 \to E_1 = E_2/\langle P'_2 + sQ'_2 \rangle$.
  $L'_1 \leftarrow \hat{\phi}(Q'_2)$.
end if
$K'_1 \leftarrow$ **GenKernel**(m, E_1).
if $K'_1 = tL'_1$ **then**
  return accept.
else
  return reject.
end if

$$
\begin{tikzcd}
E_0 \arrow[rr, dotted, "\psi"'] \arrow[d, dotted, "\tau"] & & E_1 \arrow[d, "\phi"] \\
E_A \arrow[r, "\sigma_g"] \arrow[rr, bend left, "\sigma"] \arrow[d, "\omega"] & E'_A \arrow[r, "\sigma'"] \arrow[d, "\omega'"] & E_2 \\
E_3 \arrow[r, "\sigma'_g"] & E'_3, &
\end{tikzcd}
$$

Note that there is a concern that $\deg \sigma_g = g$ is not coprime to $\deg \omega = r$. This means that the degree of $\omega' = [\sigma_g]_* \omega$ may not be equal to r but reduces to $\tilde{r} = r/h$ for a factor h of $\gcd(g, r)$. In this case, we additionally compute a random h-isogeny ι from E'_3 and use $\iota \circ \omega'$ as an auxiliary path.

5 Security Analysis

In this section, we give the security analysis for CompactSQIsign2D-East. The analysis for the normal SQIsign2D-East is considered to be similar.

5.1 Security Proof

Our protocol mainly differs from SQIsignHD in the following three ways:

(i) We compute the commitment using **RandIsogImg**.
(ii) The degree q of σ is not 2^a-good but $(2^a, 2^b, N_\tau)$-nice.
(iii) We compute an auxiliary path ω using **AuxiliaryPath** and include it into the signature.

First, to cover the difference (i), we use the following assumption instead of Assumption 1.

Assumption 3 *The commitment curve E_1 computed by* **RandIsogImg** *is computationally indistinguishable from an elliptic curve chosen uniformly at random in the supersingular isogeny graph.*

This assumption is considered to be reasonable for the same reasons stated in [22]. Next, to cover the differences (ii) and (iii), we define the following two oracles. The former one is an analogy of RUGDIO in SQIsignHD and the latter one is the oracle that simulates **AuxiliaryPath**.

Definition 2 *A random uniform nice degree isogeny oracle (RUNDIO) is an oracle taking as input a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$ and returning an efficient representation of a random isogeny $\sigma : E \to E'$ of $(2^a, 2^b)$-nice degree prime such that:*

(i) The distribution of E' is uniform in the supersingular isogeny graph.
(ii) The conditional distribution of σ given E' is uniform among isogenies $E \to E'$ of $(2^a, 2^b)$-nice degree.

Definition 3 *An auxiliary path oracle (APO) is an oracle taking as input a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$ and a $(2^a, 2^b, N_\tau)$-nice integer q and returning an efficient representation of a $(2^a - q)$-isogeny $\omega : E \to E'$ such that the distribution of ω is same as* $\mathbf{AuxiliaryPath}_{I_\psi}(q, 2^{a+b})$.

Remark 4. Since $(2^a, 2^b)$-nice integer q is $(2^a, 2^b, N_\tau)$-nice with approximately $1/2$ probability, we can obtain a random isogeny of $(2^a, 2^b, N_\tau)$-nice degree by executing RUNDIO several times. From Remark 2, especially when $a \leq b + 2$, RUNDIO can be seen as the oracle that returns a random isogeny whose degree q is smaller than 2^a. In this sense, RUNDIO is a weaker oracle than RUGDIO.

Finally, we prepare the following assumption instead of Assumption 2.

Assumption 4 *Problem 1 is computationally hard to solve even with the access to the RUNDIO and APO.*

Now, we have the following theorem.

Theorem 1 *CompactSQIsign2D-East is universally unforgeable under chosen message attacks in the random oracle model. secure in the random oracle model under Assumption 3 and Assumption 4.*

Proof. By [27, Theorem 7], it is sufficient to prove that the underlying identification scheme is knowledge sound and honest-verifier zero knowledge.

Soundness: The proof of soundness of our protocol is quite similar to that of SQIsignHD. Let $(E_1, \phi, E_4, R_4, S_4)$ and $(E_1, \phi', E_4', R_4', S_4')$ are two Compact-SQIsign2D-East transcripts with the same commitment E_1 but different challenges $\phi \neq \phi'$. From (E_4, R_4, S_4) and (E_4', R_4', S_4'), we can compute efficient representations of $\sigma : E_A \to E_2$ and $\sigma' : E_A \to E_2'$, where E_2 and E_2' are codomains of ϕ and ϕ', respectively.

Therefore, we obtain an efficient representation of $\alpha = \hat{\sigma'} \circ \phi' \circ \hat{\phi} \circ \sigma \in \mathrm{End}(E_A)$. Finally, the proof that α is non-scalar is exactly same as SQIsignHD since it depends only on the fact that $q = \deg(\sigma)$ and $q' = \deg(\sigma')$ are coprime to $\deg(\phi) = \deg(\phi')$.

Zero knowledge: We now prove that there exists a random polynomial time simulator S with access to a RUNDIO and APO that simulates transcripts $(E_1, \phi, E_4, R_4, S_4)$ with a computationally indistinguishable distribution from the transcripts of the CompactSQIsign2D-East identification protocol.

First, the simulator applies the RUNDIO several times with the input E_A and obtains an efficient representation of a random isogeny $\sigma' : E_A \to E_2'$ of $(2^a, 2^b, N_\tau)$-nice degree. Then, it selects a 2^a-isogeny $\hat{\phi}' : E_2' \to E_1'$ uniformly at random among all 2^a-isogenies from E_2'. Finally, it applies the APO with the input E_2' and $q' = \deg(\sigma')$ and obtains an efficient representation of a $(2^a - q)$-isogeny $\omega' : E_2' \to E_4'$. Hence, we can compute $(R_4', S_4') = (\sigma' \circ \omega'(P_A), \sigma' \circ \omega'(Q_A))$, where P_A, Q_A is the canonical basis of $E_A[2^a]$ and obtain the transcripts $(E_1', \phi', E_4', R_4', S_4')$.

We now prove that the transcripts $(E_1', \phi', E_4', R_4', S_4')$ of S are computationally indistinguishable from the transcripts $(E_1, \phi, E_4, R_4, S_4)$ of the Compact-SQIsign2D-East identification protocol. By the definition of the RUNDIO, E_2' is uniformly random in the supersingular isogeny graph. From the uniformity of E_2' and $\hat{\phi}'$, E_1' is also uniform and ϕ' can be regarded as uniformly selected among all 2^a-isogenies from E_1'. Besides, E_1 is statistically close to uniformly random as well by assumption and ϕ is also uniformly selected by construction. Consequently, the distribution of E_2 is also uniform.

Next, conditionally to E_2', σ' is uniformly random among isogenies $E_A \to E_2'$ of $(2^a, 2^b, N_\tau)$-nice degree by the definition of RUNDIO. Besides, conditionally to E_2, σ has the same distribution by construction.

Finally, (E_4, ω) and (E'_4, ω') have the same distribution by the definition of APO. Since (σ, ω) and (σ', ω') have the same distribution as described above, $(R_4, S_4) = (\sigma \circ \omega(P_A), \sigma \circ \omega(Q_A))$ and $(R'_4, S'_4) = (\sigma' \circ \omega'(P_A), \sigma' \circ \omega'(Q_A))$ also have the same distribution. $\square$

5.2 Hardness Analysis

We now discuss the hardness of the supersingular endomorphism problem with access to the RUNDIO and the APO. In this subsection, we assume $a \leq b+2$. In this case, the RUNDIO can been seen as a weaker oracle than the RUGDIO as noted in Remark 4. Therefore, by the same argument in [9, Section 5.3], we can expect that the RUNDIO does not help solve the supersingular endomorphism problem. Similarly, we believe that the APO does not help either, but we leave a detailed analysis as a future work.

6 Efficiency

In this section, we analyse the efficiency of SQIsign2D-East and CompactSQIsign-2D-East. First, we provide concrete parameters for these protocols, then compare the data sizes of these protocols such as public key size and ciphertext size with SQIsign and SQIsignHD. Finally, we analyse the computational cost of SQIsign2D-East and CompactSQIsign2D-East.

6.1 Parameters

We give concrete parameters for SQIsign2D-East and CompactSQIsign2D-East satisfying the NIST security level 1, 3, and 5:

– Level 1:

$$a = 127,\ b = 126,\ p = 2^{253} \cdot 27 - 1.$$

– Level 3:

$$a = 191,\ b = 189,\ p = 2^{380} \cdot 35 - 1.$$

– Level 5:

$$a = 261,\ b = 259,\ p = 2^{520} \cdot 2 - 1.$$

6.2 Data Sizes

In this subsection, we compare the signature sizes of SQIsign, SQIsignHD, SQIsign-2D-East, and CompactSQIsign2D-East using the above parameters. Table 1 shows each signature size. Note that we do not give the signature size of SQIsignHD for the level 3 and 5 since sufficient information to evaluate the signature sizes are not given in [9]. As shown in Table 1, the signature size of SQIsign2D-East is larger than both SQIsign and SQIsignHD for every security level. On the other hand, the signature size of CompactSQIsign2D-East is smaller than SQIsign and lager than SQIsignHD for every security level.

Security	Protocol	Signature (bytes)
Level 1	SQIsign	177
	SQIsignHD	109
	SQIsign2D-East	**197**
	CompactSQIsign2D-East	**164**
Level 3	SQIsign	263
	SQIsignHD	-
	SQIsign2D-East	**294**
	CompactSQIsign2D-East	**245**
Level 5	SQIsign	335
	SQIsignHD	-
	SQIsign2D-East	**396**
	CompactSQIsign2D-East	**331**

Table 1. Signature size comparison

6.3 Computational Cost

We compare the computational costs of SQIsignHD, SQIsign2D-East, and CompactSQIsign2D-East for the security level 1. Table 2 shows the number of isogeny computations of each degree. As Table 2 shows, our protocol does not require

Protocol (Security level 1)		2	3	$(2,2)$	$(2,2,2,2)$
SQIsignHD	**keygen**	378	234	-	-
	sign	252	312	-	-
	verify	-	78	-	142
SQIsign2D-East	**keygen**	-	-	253	-
	sign	126	0-3	633	-
	verify	126	0-3	127	-
CompactSQIsign2D-East	**keygen**	-	-	253	-
	sign	126	0-3	760	-
	verify	126	0-3	127	-

Table 2. Number of isogeny computations of each degree

any 4-dimensional isogeny computation for the verification. In addition, the number of 2-dimensional isogeny computations is smaller than the number of 4-dimensional isogeny computations in SQIsignHD. Therefore, the verification cost of our protocol is clearly smaller than that of SQIsignHD. As for the key generation and signing, our protocol requires 2-dimensional isogeny computations, whereas SQIsignHD only requires 1-dimensional isogeny computations. Therefore, our protocol is likely to have a larger cost for the key generation and signing.

Finally, in Table 3, we show the actual computational times of SQIsign2D-East and CompactSQIsign2D-East implemented in Julia. The implementation is available at: `https://github.com/hiroshi-onuki/SQIsign2D-East.jl`. These are the averages of 100 run times. The computational times are measured on a computer with an Intel Core i7-10700K CPU@3.70Hz without Turbo Boost. The cost evaluation through an optimized implementation is a future work.

Security	Protocol	**keygen**	**sign**	**verify**
Level 1	SQIsign2D-East	0.55	1.50	0.20
	CompactSQIsign2D-East	0.60	1.80	0.28
Level 3	SQIsign2D-East	1.00	2.68	0.58
	CompactSQIsign2D-East	0.95	3.28	0.49
Level 5	SQIsign2D-East	1.38	5.16	0.62
	CompactSQIsign2D-East	1.47	6.42	0.71

Table 3. Computational times (sec.)

7 Conclusion

In this paper, we introduce SQIsign2D-East, a new variant of SQIsignHD, which requires only 2-dimensional isogeny computations for the verification, while the conventional SQIsignHD requires 4-dimensional isogeny computations. As a building block of SQIsign2D-East, we construct a new algorithm, which is a generalization of the conventional algorithm called **RandIsogImg**. In addition, we propose CompactSQIsign2D-East, which has shorter signature size but has larger signing cost.

Both SQIsign2D-East and CompactSQIsign2D-East have less verification costs than SQIsignHD. On the other hand, the signing costs are expected to be larger than SQIsignHD though they are expected to be smaller than SQIsign. The signature size of SQIsign2D-East is longer than both SQIsign and SQIsignHD. The signature size of CompactSQIsign2D-East is shorter than SQIsign but longer than SQIsignHD.

As a future work, we need more detailed analysis on the security of our protocol. The cost evaluation of SQIsign2D-East through an optimized implementation is also a future work.

Acknowledgments

We would like to thank Andrea Basso, Luca De Feo, Pierrick Dartois, Antonin Leroux, Luciano Maino, and Benjamin Wesolowski for sharing their work on SQIsign2D-West, and Max Duparc and Tako Boris Fouotsa for sharing their work on SQIPrime with us prior to publication.

References

1. Reza Azarderakhsh, Matthew Campagna, Craig Costello, Luca De Feo, Basil Hess, Amir Jalali, David Jao, Brian Koziel, Brian LaMacchia, Patrick Longa, et al. Supersingular isogeny key encapsulation. *Submission to the NIST Post-Quantum Standardization project*, 152:154–155, 2017.
2. Andrea Basso, Luca De Feo, Pierrick Dartois, Antonin Leroux, Luciano Maino, Giacomo Pope, Damien Robert, and Benjamin Wesolowski. SQIsign2D-West: the Fast, the Small, and the Safer. Cryptology ePrint Archive, Paper 2024/760, 2024. `https://eprint.iacr.org/2024/760`.
3. Andrea Basso, Luciano Maino, and Giacomo Pope. FESTA: Fast encryption from supersingular torsion attacks. In *ASIACRYPT 2023*, pages 98–126, 2023.
4. Daniel J Bernstein, Luca De Feo, Antonin Leroux, and Benjamin Smith. Faster computation of isogenies of large prime degree. *Open Book Series*, 4(1):39–55, 2020.
5. Wouter Castryck and Thomas Decru. An efficient key recovery attack on SIDH. In *EUROCRYPT 2023*, pages 423–447, 2023.
6. 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. Submission to NIST standardization of additional digital signature schemes. `https://sqisign.org`, 2023.
7. Mingjie Chen, Antonin Leroux, and Lorenz Panny. SCALLOP-HD: group action from 2-dimensional isogenies. In *PKC 2024*, pages 190–216. Springer, 2024.
8. Romain Cosset and Damien Robert. Computing (l, l)-isogenies in polynomial time on Jacobians of genus 2 curves. *Mathematics of Computation*, 84(294):1953–1975, 2015.
9. Pierrick Dartois, Antonin Leroux, Damien Robert, and Benjamin Wesolowski. SQISignHD: new dimensions in cryptography. In *EUROCRYPT 2024*, pages 3–32. Springer, 2024.
10. Pierrick Dartois, Luciano Maino, Giacomo Pope, and Damien Robert. An Algorithmic Approach to $(2, 2)$-isogenies in the Theta Model and Applications to Isogeny-based Cryptography. Cryptology ePrint Archive, Paper 2023/1747, 2023. `https://eprint.iacr.org/2023/1747`.
11. Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski. SQISign: Compact post-quantum signatures from quaternions and isogenies. In *ASIACRYPT 2020*, pages 64–93, 2020.
12. Luca De Feo, Antonin Leroux, Patrick Longa, and Benjamin Wesolowski. New algorithms for the deuring correspondence: towards practical and secure sqisign signatures. In *EUROCRYPT 2023*, pages 659–690. Springer, 2023.
13. Max Deuring. Die typen der multiplikatorenringe elliptischer funktionenkörper. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 14:197–272, 1941.
14. Max Duparc and Tako Boris Fouotsa. SQIPrime: A dimension 2 variant of SQISignHD with non-smooth challenge isogenies. Cryptology ePrint Archive, Paper 2024/****, 2024. `https://eprint.iacr.org/2024/****`.
15. Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In *CRYPTO 1986*, pages 186–194. Springer, 1986.

16. Everett W. Howe, Franck Leprévost, and Bjorn Poonen. Large torsion subgroups of split Jacobians of curves of genus two or three. *Forum Mathematicum*, 12(3):315–364, 2000.
17. David Jao and Luca De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In *PQCrypto 2011*, pages 19–34, 2011.
18. Ernst Kani. The number of curves of genus two with elliptic differentials. 1997.
19. David Lubicz and Damien Robert. Computing isogenies between abelian varieties. *Compositio Mathematica*, 148(5):1483–1515, 2012.
20. Luciano Maino, Chloe Martindale, Lorenz Panny, Giacomo Pope, and Benjamin Wesolowski. A direct key recovery on SIDH. *EUROCRYPT 2023*, pages 448–471, 2023.
21. Tomoki Moriya. IS-CUBE: An isogeny-based compact KEM using a boxed SIDH diagram. Cryptology ePrint Archive, Paper 2023/1506, 2023. `https://eprint.iacr.org/2023/1506`.
22. Kohei Nakagawa and Hiroshi Onuki. QFESTA: Efficient Algorithms and Parameters for FESTA using Quaternion Algebras. Cryptology ePrint Archive, Paper 2023/1468, 2023. `https://eprint.iacr.org/2023/1468`.
23. Hiroshi Onuki and Kohei Nakagawa. Ideal-to-isogeny algorithm using 2-dimensional isogenies and its application to SQIsign. Cryptology ePrint Archive, Paper 2024/****, 2024. `https://eprint.iacr.org/2024/****`.
24. Damien Robert. Breaking SIDH in polynomial time. In *EUROCRYPT 2023*, pages 472–503, 2023.
25. Benjamin Andrew Smith. *Explicit endomorphisms and correspondences*. Phd thesis, University of Sydney, 2005.
26. Jacques Vélu. Isogénies entre courbes elliptiques. *Comptes-Rendus de l'Académie des Sciences*, 273:238–241, 1971.
27. Antonio Villani. Zero-knowledge proofs and applications. 2015. `http://danieleventuri.altervista.org/files/zero-knowledge.pdf`.

A Allow q to be even

Assume that q is an even integer smaller than 2^a. Let $q = 2^e \cdot q_{\mathrm{odd}}$, where q_{odd} is odd integer and let $r = 2^{a-e} - q_{\mathrm{odd}}$. Note here that q_{odd} is smaller than 2^{a-e} since $q < 2^a$. Next, we decompose the q-isogeny σ to a 2^e-isogeny $\sigma_2 : E_A \to E'_A$ and a q_{odd}-isogeny $\sigma_{\mathrm{odd}} : E'_A \to E_2$. SQIsign2D-East using the method (i) is based on the following diagram:

$$\begin{tikzcd}
E_0 \arrow[rr, dotted, "\psi"'] \arrow[d, dotted, "\tau"] & & E_1 \arrow[d, "\phi"] \\
E_A \arrow[r, "\sigma_2"] \arrow[rr, bend left, "\sigma"] \arrow[d, "\omega"] & E'_A \arrow[r, "\sigma_{\mathrm{odd}}"] \arrow[d, "\omega'"] & E_2 \\
E_3 \arrow[r, "\sigma'_2"] & E'_3, &
\end{tikzcd}$$

where ω is an r-isogeny, $\sigma'_2 = [\omega]_*\sigma_2$, and $\omega' = [\sigma_2]_*\omega$. In this diagram, we can compute σ_2 by using Vélu's formulas. In addition, we can evaluate σ over $E_A[2^a]$ as in Algorithm 7. Therefore, we can evaluate σ_{odd} over $E'_A[2^{a-e}]$ by evaluating $\sigma \circ \hat{\sigma_2} = [2^e] \circ \sigma_{\mathrm{odd}}$ over $E'_A[2^a]$. We can also evaluate ω' over $E'_A[2^{a-e}]$ as follow:

1. Obtain $\omega|_{E_A[2^a]}$ for an r-isogeny $\omega : E_A \to E_3$ using **AuxiliaryPath**.
2. Compute $\omega'|_{E'_A[2^{a-e}]}$ by evaluating $\sigma'_2 \circ \omega \circ \hat{\sigma_2} = [2^e] \circ \omega'$ over $E'_A[2^a]$. (We can compute σ'_2 from its kernel $\omega(\ker \sigma_2)$ by using Vélu's formulas.)

Then, the response is $(E'_3, R'_2 = [q_{\mathrm{odd}}^{-1}] \circ \sigma_{\mathrm{odd}} \circ \hat{\omega}'(P'_3), S'_2 = [q_{\mathrm{odd}}^{-1}] \circ \sigma_{\mathrm{odd}} \circ \hat{\omega}'(Q'_3), \ker \sigma_2)$ for the canonical basis of $E'_3[2^{a-e}]$. Note that we have to chose σ so that $\ker(\hat{\phi} \circ \sigma)$ is cyclic. This can be done by choosing $\alpha = \hat{\tau} \circ \hat{\sigma} \circ \phi \circ \psi \in \mathcal{O}_0$ so that $\alpha \notin 2\mathcal{O}_0$ when running **RandomEquivalentIdeal** in step 2 of Algorithm 7.

For the verification, we first compute the short path $\sigma_2 : E_A \to E'_A$ using Vélu's formulas. Then we compute $(2^{a-e}, 2^{a-e})$-isogeny $\Phi : E'_3 \times E_2 \to A$ with kernel $\langle (P'_3, R'_2), (Q'_3, S'_2) \rangle$. Finally, we check if $A \cong E'_A \times F$ for a curve F.