SQIsign2D^2: New SQIsign2D Variant by Leveraging Power Smooth Isogenies in Dimension One

Zheng Xu[1], Kaizhan Lin✉[2], Chang-An Zhao[2,3], and Yi Ouyang[1,4]

[1] Hefei National Laboratory, University of Science and Technology of China, Hefei 230088, China
xuzheng1@mail.ustc.edu.cn
yiouyang@ustc.edu.cn
[2] School of Mathematics, Sun Yat-sen University, Guangzhou, China
linkzh5@mail2.sysu.edu.cn
zhaochan3@mail.sysu.edu.cn
[3] Guangdong Key Laboratory of Information Security, Guangzhou, China
[4] School of Mathematical Sciences, Wu Wen-Tsun Key Laboratory of Mathematics, University of Science and Technology of China, Hefei 230026, China

Abstract. In this paper, we propose SQIsign2D^2, a novel digital signature scheme within the SQIsign2D family. Unlike other SQIsign2D variants, SQIsign2D^2 employs the prime $p = CD - 1$ as the field characteristic, where $D = 2^{e_2}$, $C = 3^{e_3}$ and $C \approx D \approx \sqrt{p}$. By leveraging accessible C-isogenies, SQIsign2D^2 significantly reduces the degree requirements for two-dimensional isogeny computations, thereby lowering the overall computational overhead compared to other SQIsign2D variants.
We also provide a proof-of-concept implementation of SQIsign2D^2, and give an efficiency comparison between SQIsign2D^2 and other SQIsign2D variants. In particular, the experimental results demonstrate that the key generation and signing phases of SQIsign2D^2 are more than twice as fast as those of SQIsign2D-East at the NIST-I security level, respectively. Additionally, the verification performance in SQIsign2D^2 exhibits marginally improved efficiency.

Keywords: SQIsign · Post-quantum cryptography · Isogeny · Signature

1 Introduction

Isogeny-based cryptography constitutes a significant part of post-quantum cryptography. With the breaking of SIDH and SIKE [21,1,10,24,31], isogeny-based cryptography has been compelled to seek new directions. In response to these attacks, several new SIDH-like schemes are proposed, such as M-SIDH [20] and binSIDH [5]. Basso et al. developed a trapdoor mechanism and proposed FESTA [7], an efficient public-key encryption protocol, by using the techniques developed in the SIDH attacks.

Despite the vulnerabilities in SIDH, certain isogeny-based protocols remain secure. Notably, in 2020 De Feo et al. [16] proposed SQIsign, a novel isogeny-based digital signature scheme, which has emerged as one of the most promising candidates and is currently under consideration in the NIST PQC standardization process [11].

SQIsign is highly attractive due to its compact signature size. However, this advantage comes at the cost of relatively low computational efficiency compared to other signatures, primarily because of the expensive isogeny computations. To address this issue, several techniques [17,23] have been proposed to improve the SQIsign implementation, but the ideal-to-isogeny translation remains the efficiency bottleneck. Recently, Onuki and Nakagawa [29] further optimized the ideal-to-isogeny translation in SQIsign by utilizing isogenies in dimension two.

On the other hand, novel variants of SQIsign have been proposed to circumvent the expensive ideal-to-isogeny translation. In 2023, Dartois, Leroux, Robert and Wesolowski proposed SQIsignHD [14], which takes advantage of high-dimensional isogenies during the verification process to recover the response isogeny. Instead of translating the response ideal into an isogeny, the prover simply provides the response isogeny evaluations on torsion points, thereby reducing the computational complexity of the signing phase. Moreover, SQIsign2D-West, SQIsign2D-East and SQIPrime were respectively presented by Basso et al. [4], Nakagawa et al. [28], Duparc and Fouotsa [18]. These protocols employ the construction of auxiliary isogenies to compute two-dimensional isogenies instead of the four-dimensional isogenies required in SQIsignHD, thus improving the overall computational efficiency.

Motivation* & *Contribution. Currently, all the SQIsign2D variants use the prime $p = f \cdot D - 1$ as the field characteristic, where f is a small cofactor and D is a power of two. The specific setting enables the efficient generation of non-smooth isogenies by leveraging accessible (D, D)-isogenies. However, compared to isogeny computations in dimension one, two-dimensional isogeny computations are significantly more expensive and constitute the main efficiency bottlenecks of the SQIsign2D variants.

In this paper, we set $p = CD - 1$ to be the field characteristic, where $D = 2^{e_2}$, $C = 3^{e_3}$, $D' = 2^{\bullet}$ and $C \approx D \approx \sqrt{p}$, $D' \approx p^{1/4}$. Under this parameter setting, while efficient computation of $(2^{\bullet}, 2^{\bullet})$-isogenies with chain lengths $\approx p$ is infeasible, isogenies in dimension one with degree coprime to 2 become accessible. Leveraging this observation, we propose an efficient algorithm, abbreviated as **ImRanIso**, that can be used to generate a non-smooth isogeny starting from E_0. **ImRanIso** adapts an CD'-isogeny to reduce the degree requirement for two-dimensional isogenies. Furthermore, we propose **GenImRanIso**, an algorithm designed to efficiently generate non-smooth isogenies from a curve E_A. **GenImRanIso** exploits the accessible C-isogenies to reduce the degree requirements for two-dimensional isogenies. We emphasize that both algorithms successfully reduce the degree of the two-dimensional isogenies to a magnitude comparable to that of non-smooth isogenies in dimension one, and thus they are more efficient compared to other algorithms in the literature.

Building on these algorithms, we propose SQIsign2D^2, an efficient isogeny-based signature scheme[5]. Unlike other SQIsign2D variants in the literature, our protocol takes the prime $p = 2^{e_2}3^{e_3} - 1$ as the field characteristic. The security analysis of SQIsign2D^2 parallels that of SQIsign2D-East. In particular, we provide several alternative approaches to strengthen the plausibility of the assumption that the commitment curve is computational indistinguishable from an elliptic curve chosen uniformly at random in the supersingular isogeny graph.

We provide an efficiency comparison between SQIsign2D^2 and other SQIsign2D variants, demonstrating that SQIsign2D^2 is the fastest SQIsign2D variant to date. We also provide a proof-of-concept implementation in Julia. The experimental results show that the key generation and signing phases of SQIsign2D^2 are more than twice as fast as those of SQIsign2D-East, respectively.

Related Work. Recently, Basso et al. [3] proposed a new signature scheme called PRISM-sig. PRISM-sig offers a faster signing time compared to SQIsign2D-West and SQIsign2D-East, while the verification is slower. Based on our cost estimates, we expect that SQIsign2D^2 is still more efficient than PRISM-sig.

Very recently, Nakagawa and Onuki proposed SQIsign2DPush [27], a new variant of SQIsign. We note that their work and ours are independent. Further comparisons are left as future work.

Organization. The rest of this paper is organized as follows. Section 2 provides the necessary preliminaries, including isogenies, Deuring correspondence, etc. We also introduce the SQIsign2D family by taking SQIsign2D-East as an instance. Before introducing SQIsign2D^2 in Section 4, we propose two new algorithms as the building blocks in Section 3. Section 5 analyzes the security of SQIsign2D^2, while Section 6 presents an efficiency comparison between SQIsign2D^2 and other SQIsign2D variants. Finally, we conclude in Section 7.

2 Notations and Preliminaries

In this section, we present the necessary background, including isogenies, ideals, the Deuring correspondence, and isogeny computations in dimension two. For more detail, we refer to [33,25,35]. We also provide a description of SQIsign2D-East [28].

2.1 Basic knowledge

Isogenies. An isogeny φ is a morphism between elliptic curves that preserves the group structure and maps the point at infinity to the point at infinity. An isogeny φ is separable if $\#\ker(\varphi) = \deg(\varphi)$. We abbreviate a separable isogeny of degree n as an n-isogeny. One can compute a separable isogeny by Vélu's

[5] The notation "2D^2" comes from $2D^2 = 2D \times 1D$, indicating that the signature scheme is a fast SQIsign2D variant which benefits from isogenies in dimension one.

formula [34,8]. Given an n-isogeny $\varphi : E_1 \to E_2$, its dual isogeny is denoted by $\hat{\varphi}$, satisfying that $\hat{\varphi} \circ \varphi = \varphi \circ \hat{\varphi} = [n]$. If the kernel of φ is a cyclic group, we call the isogeny φ cyclic. Moreover, if φ is a cyclic isogeny with kernel $\langle P \rangle$ for some $P \in E_1[n]$, then the kernel of $\hat{\varphi}$ equals to $\langle \varphi(Q) \rangle$, where Q is a rational point such that $\langle P, Q \rangle = E_1[n]$.

Endomorphism rings. An endomorphism is either the zero map [0] or an isogeny from E to itself. An endomorphism ring of E, denoted by $\mathrm{End}(E)$, is the ring formed by all endomorphisms of E under addition and composition. Let p be a prime with $p \equiv 3 \pmod 4$. A quaternion algebra ramified at p and ∞ is given by $B_{p,\infty} = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$, where $i^2 = -1, j^2 = -p, k = ij = -ji$. Supersingular elliptic curves are a special type of elliptic curves over finite fields, whose endomorphism rings are maximal orders in quaternion algebra. Given a fractional ideal I of maximal order $\mathcal{O}$, the left order of I is defined as $\mathcal{O}_L(I) = \{\alpha \in B_{p,\infty} \mid \alpha I \subseteq I\}$, and the right order of I is defined as $\mathcal{O}_R(I) = \{\alpha \in B_{p,\infty} \mid I\alpha \subseteq I\}$. It should be noted that both $\mathcal{O}_L(I)$ and $\mathcal{O}_R(I)$ are maximal orders in $B_{p,\infty}$.

Given $\alpha = a + bi + cj + dk \in B_{p,\infty}$, define its conjugate as $\bar{\alpha} = a - bi - cj - dk$. The reduced trace and reduced norm of α are defined as $\mathrm{Trd}(\alpha) = \alpha + \bar{\alpha}$ and $\mathrm{Nrd}(\alpha) = \alpha\bar{\alpha}$, respectively. Similarly, given a left ideal I of a maximal order in $B_{p,\infty}$, the conjugate of I, denoted by $\bar{I}$, is defined as the set $\bar{I} = \{\bar{\alpha} \mid \alpha \in I\}$. The reduced norm of left ideal I is defined as $\mathrm{Nrd}(I) = \gcd(\{\mathrm{Nrd}(\alpha) | \alpha \in I\})$. We have $I\bar{I} = \mathrm{Nrd}(I)\mathcal{O}_L(I), \bar{I}I = \mathrm{Nrd}(I)\mathcal{O}_R(I)$. We say two left ideals I, J are equivalent if there exists $\alpha \in B_{p,\infty}^*$ such that $I = J\alpha$, and use the notation $I \sim J$ to represent equivalence.

Deuring correspondence. The Deuring correspondence establishes a one-to-one correspondence between isogeny classes of elliptic curves and ideal classes. Let E_1 be a supersingular elliptic curve, $\mathrm{End}(E_1) \cong \mathcal{O}$ be the endomorphism ring of E_1 and $\varphi : E_1 \to E_2$ be an isogeny. Then the ideal $I_\varphi = \{\alpha \in \mathcal{O} \mid \alpha(P) = \infty \text{ for all } P \in \ker(\varphi)\}$ corresponds to the isogeny φ with $\mathcal{O}_L(I_\varphi) = \mathcal{O} \cong \mathrm{End}(E_1)$ and $\mathcal{O}_R(I_\varphi) \cong \mathrm{End}(E_2)$. Conversely, if there is a left $\mathcal{O}$-ideal I, then one can compute φ_I with kernel $E[I] = \{P \in E_1 \mid \alpha(P) = \infty \text{ for all } \alpha \in I\}$, which corresponds to the left $\mathcal{O}$-ideal I. Furthermore, we have $\deg(\varphi_I) = \mathrm{Nrd}(I)$. In particular, the isogeny φ is an endomorphism if and only if I_φ is a principal ideal. Moreover, assume that $\varphi_1 : E \to E_1$ and $\varphi_2 : E \to E_2$ are two isogenies that correspond to the left ideals I_1 and I_2, respectively. Then E_1 and E_2 belong to the same isomorphism class if and only if I_1 and I_2 are equivalent.

Let I be an integral ideal of maximal order $\mathcal{O}$. Then the ideal I can be generated by an $\alpha \in I$ and the reduced norm $\mathrm{Nrd}(I)$. Moreover, the kernel of the ideal I satisfies $E[I] = E[\mathrm{Nrd}(I)] \cap \ker(\alpha)$.

Eichler orders. Let $\mathcal{O}$ be a maximal order in $B_{p,\infty}$ and I be a left $\mathcal{O}$-ideal connecting $\mathcal{O}$ and $\mathcal{O}'$(i.e. $\mathcal{O}_L(I) = \mathcal{O}$, $\mathcal{O}_R(I) = \mathcal{O}'$). The Eichler order of I is defined as $\mathcal{O} \cap \mathcal{O}'$. Besides, the Eichler order of I equals $\mathfrak{O} = \mathbb{Z} + I$. Let I be a left $\mathcal{O}$-ideal and $\varphi_I : E_1 \to E_2$ be an isogeny corresponding to I with degree d.

If $\alpha \in \mathfrak{O}$, then α is also an endomorphism of E_2 and for any $P \in E_2[n]$, we have $\alpha(P) = [d^{-1}] \circ \varphi_I \circ \alpha \circ \hat{\varphi}_I(P)$, where d^{-1} is the inverse of d modulo n.

Pushforward and pullback. Consider the commutative isogeny diagram as shown in Figure 1. For separable isogenies $\varphi_1 : E \to E_1$ and $\varphi_2 : E \to E_2$ satisfying $\gcd(\deg(\varphi_1), \deg(\varphi_2)) = 1$, define the pushforward isogeny of φ_2 through φ_1 as $\psi_2 = [\varphi_1]_*(\varphi_2)$, where $\ker([\varphi_1]_*(\varphi_2)) = \varphi_1(\ker(\varphi_2))$. Conversely, we call φ_2 the pullback isogeny of ψ_2 through φ_1, denoted by $\varphi_2 = [\varphi_1]^*(\psi_2)$. Similarly, we can define $\psi_1 = [\varphi_2]_*(\varphi_1)$ and $\varphi_1 = [\varphi_2]^*(\psi_1)$ the pushforward isogeny of φ_1 through φ_2 and the pullback isogeny of ψ_1 through φ_2, respectively.

$$\begin{tikzcd} & E_1 \arrow[dr, "\psi_2"] & \\ E \arrow[ur, "\varphi_1"] \arrow[dr, "\varphi_2"'] & & E_3 \\ & E_2 \arrow[ur, "\psi_1"'] & \end{tikzcd}$$

Fig. 1: A commutative isogeny diagram.

Suppose that the ideals $I_{\varphi_1}, I_{\varphi_2}$ correspond to isogenies φ_1, φ_2, respectively. Under the Deuring correspondence, the ideal corresponding to $[\varphi_1]_*\varphi_2$ is defined as $[I_{\varphi_1}]_* I_{\varphi_2} = \frac{1}{\mathrm{Nrd}(I_{\varphi_1})} \overline{I_{\varphi_1}} (I_{\varphi_1} \cap I_{\varphi_2})$. The ideal corresponding to the pullback isogeny $[\varphi_1]^*\psi_2$ is $[I_{\varphi_1}]^*[I_{\psi_2}] = [\overline{I_{\varphi_1}}]_*[I_{\psi_2}]$. Similarly, we can also define the ideals $[I_{\varphi_2}]_* I_{\varphi_1}$ and $[I_{\varphi_2}]^* I_{\psi_1}$ corresponding to $[\varphi_2]_*\varphi_1$ and $[\varphi_2]^*\psi_1$, respectively.

2.2 Key algorithms in the SQIsign family

In the following, we review the key algorithms in the SQIsign family, which are also fundamental to our protocol. For simplicity, we assume that $\mathrm{End}(E_0) \cong \mathcal{O}_0$.

RandomEquivalentIdeal$_N(J)$: Given a left ideal I of maximal order $\mathcal{O}$ and $N \in \mathbb{N}$, outputs an equivalent ideal $J \sim I$ with $\mathrm{Nrd}(J) < N$.
FullRepresentInteger$_{\mathcal{O}_0}(M)$: Given an integer $M > p$, outputs $\alpha \in \mathcal{O}_0$ such that $\mathrm{Nrd}(\alpha) = M$.
EichlerModConstraint(I, γ, δ): Given a left-$\mathcal{O}_0$ ideal I of prime reduced norm N and $\gamma, \delta \in \mathcal{O}_0$, outputs $(C_0, D_0) \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ such that $\gamma(C_0 j + D_0 k)\delta \in \mathbb{Z} + I$.
FullStrongApproximation$_M(N, C_0, D_0)$: Given $M, N, C_0, D_0 \in \mathbb{N}$, outputs $\mu \in \mathcal{O}_0$ such that $\mu = m(C_0 j + D_0 k) + N\mu_1$ and $\mathrm{Nrd}(\mu) = M$, where $m \in \mathbb{Z}$ and $\mu_1 \in \mathcal{O}_0$.
IsogenyToIdeal(φ, ψ, I_ψ): Given an N_φ-isogeny $\varphi : E_1 \to E_2$, an N_ψ-isogeny $\psi : E_0 \to E_1$ with $\gcd(N_\varphi, N_\psi) = 1$ and its corresponding ideal I_ψ, outputs the ideal I_φ corresponding to φ.

Currently, two-dimensional isogenies, i.e., isogenies between principally polarized superspecial abelian varieties, serve as powerful tools in isogeny-based cryptography. Based on Kani's lemma [22], Maino et al. proposed the following theorem to break the SIDH protocol.

Theorem 1 ([24], Theorem 1). *Let A, B be coprime integers and $D = A + B$. Assume that E_0, E_1, E_2 and E_3 are supersingular elliptic curves over $\mathbb{F}_{p^2}$, connected by the isogeny diagram as illustrated in Figure 2,*

$$\begin{tikzcd}
E_0 \arrow[r, "\psi"] \arrow[d, "\varphi"'] \arrow[dr, "\theta"] & E_1 \arrow[d, "\varphi'"] \\
E_2 \arrow[r, "\psi'"'] & E_3
\end{tikzcd}$$

Fig. 2: A sketch of Theorem 1.

where $\deg(\psi) = A$, $\deg(\varphi) = B$, $\psi' = [\varphi]_*\psi$, $\varphi' = [\psi]_*\varphi$, $\theta = \psi' \circ \varphi = \varphi' \circ \psi$. *Then the isogeny*

$$\Phi = \begin{pmatrix} \psi & -\widehat{\varphi'} \\ \varphi & \widehat{\psi'} \end{pmatrix} : E_0 \times E_3 \to E_1 \times E_2$$

is a (D, D)-isogeny from $E_0 \times E_3$ to $E_1 \times E_2$, and the kernel of Φ is $\{([B]P, \theta(P)) \mid P \in E_0[D]\}$.

From the above theorem, one can compute the (D, D)-isogeny Φ with kernel $\{([B]P, \theta(P)) \mid P \in E_0[D]\}$, and evaluate the isogenies ψ, φ by embedding and projection. This plays an essential role in SQIsignHD and the SQIsign2D family. The algorithm for computing φ, is denoted by **KaniCod**.

KaniCod$(A, B, E_0, E_3, P, Q, \theta(P), \theta(Q); S_1; S_2)$: Given integers A, B with $A + B = D$, finite subsets $S_1 \subseteq E_0$ and $S_2 \subseteq E_3$, the points $\{P, Q\}$ such that $\langle P, Q \rangle = E_0[D]$ and the evaluation of the (AB)-isogeny $\theta : E_0 \to E_3$ on $\{P, Q\}$, outputs the codomain E_1, the evaluation of ψ on S_1 and the evaluation of $\widehat{\varphi'}$ on S_2.

2.3 SQIsign2D-East

The SQIsign2D variants are attractive due to their compact signatures and efficient implementations. Here we review SQIsign2D-East, which is considered one of the fastest variants within the SQIsign2D family. Notably, it outperforms SQIsign2D-West and SQIPrime in signing efficiency, and the verification of SQIsign2D-East is faster than that of PRISM-sig. The other reason why we take SQIsign2D-East as an instance is that some of the security proofs of our new signature share similarities with those of the SQIsign2D-East.

SQIsign2D-East is a Σ-signature scheme, which is derived via the Fiat-Shamir transform [19]. We briefly recall the underlying identification protocol, as illustrated in Figure 3. For more technical details we refer to [28].

$$\begin{tikzcd}
E_0 \arrow[r, "\psi"] \arrow[d, "\tau"'] & E_1 \arrow[d, "\varphi"] \\
E_A \arrow[r, "\sigma"] \arrow[d, "\varphi_{\mathrm{aux}}"'] & E_2 \arrow[d, dashed] \\
E_{\mathrm{aux}} \arrow[r, dashed] & \bullet
\end{tikzcd}$$

Fig. 3: A sketch of the SQIsign2D-East identification protocol.

Setup: Given a security parameter λ, let $p = 2^{a+b}f - 1$ be a 2λ-bit prime, where f is a small cofactor and $0 \leq a - b \leq 2$, $a \approx b \approx \lambda$. Let $E_0 : y^2 = x^3 + x$ defined over $\mathbb{F}_p$ with known endomorphism ring $\mathrm{End}(E_0) \cong \mathcal{O}_0$.

Key Generation: The prover first takes a random prime $N_\tau < p^{\frac{1}{4}}$ such that $\left(\frac{3}{N_\tau}\right) = -1$, where $\left(\frac{\cdot}{\cdot}\right)$ is the Legendre symbol, and then samples a uniform random N_τ-isogeny $\tau : E_0 \to E_A$.

Commitment: The prover first chooses a prime $N_\psi < 2^{a+b} \approx p$, and then samples an N_ψ-isogeny $\psi : E_0 \to E_1$ uniformly at random. After that, the prover transmits the commitment curve E_1 to the verifier.

Challenge: The verifier chooses $K_{\mathrm{cha}} \in E_1[2^b]$ as the kernel generator of the challenge isogeny $\varphi : E_1 \to E_2$, and then sends K_{cha} to the prover.

Response: Given K_{cha}, the prover constructs the challenge isogeny $\varphi : E_1 \to E_2$. From the knowledge of τ, ψ and φ, the prover selects a uniform random response isogeny $\sigma : E_A \to E_2$ such that $q = \deg(\sigma)$ is $(2^a, 2^b)_3$-nice (as defined in Definition 1). After that, the prover samples an auxiliary path $\varphi_{\mathrm{aux}} : E_A \to E_{\mathrm{aux}}$ with degree $2^a - q$ uniformly at random. Finally, the prover transmits an efficient representation of the composition $\sigma \circ \hat{\varphi}_{\mathrm{aux}}$ to the verifier.

Verify: By applying Theorem 1, the verifier accepts if σ is an isogeny from E_A to E_2 with degree $(2^a, 2^b)_3$-nice. Otherwise, the verifier rejects.

Definition 1. *A positive integer q is $(2^a, 2^b)_3$-nice if*

(1) q is odd;
(2) q is smaller than 2^a;
(3) $q(2^a - q) < 2^{a+b}$;
(4) $M(q) := q(2^a - q)(2^{a+b} - q(2^a - q))$ is divisible by 3.

In the original version of SQIsign2D-East, the degree of the response isogeny is required to be $(2^a, 2^b, N_\tau)$-nice, i.e.,

(1) q is odd;
(2) q is smaller than 2^a;
(3) $q(2^a - q) < 2^{a+b}$;
(4) $\left(\frac{M(q)}{N_\tau}\right) = \left(\frac{-1}{N_\tau}\right)$, where $M(q) := q(2^a - q)(2^{a+b} - q(2^a - q))$.

However, this restriction leaks a Legendre symbol modulo N_τ. In [9], Castryck et al. proposed a key-recovery attack on the original version of SQIsign2D-East that halves the security level. To mitigate this attack, the modified protocol includes the following requirements:

- Require 3 to be a non-quadratic residue modulo N_τ;
- Ensure that the degree of the response isogeny is $(2^a, 2^b)_3$-nice.

The prover may fail to sample a response isogeny of $(2^a, 2^b)_3$-nice degree. An effective way to reduce the failure probability is to apply the "gcd-trick" [9, Section 4.1]. Additionally, the modification requires that $q/\gcd(q, f)$ is $(2^a, 2^b)_3$-nice.

3 New Algorithm

In the SQIsign2D family, one main issue is to randomly generate an isogeny whose degree is non-smooth. In this section we propose two new algorithms, which are the main building blocks of SQIsign2D^2. Given an endomorphism ring $\mathrm{End}(E_0)$ and an integer $d < p^{1/4}$, the first algorithm, named **ImRanIso**, generates a d-isogeny starting from E_0 efficiently. From the knowledge of $\tau : E_0 \to E$, we use **GenImRanIso** to generate a random d-isogeny starting from E.

Unlike other SQIsign2D variants, we assume that the initial curve $E_0 : y^2 = x^3 + x$ is defined over $\mathbb{F}_p$, where $p = C \cdot D - 1$ with $D = 2^{e_2}$, $\gcd(C, D) = 1$ and $C \approx D \approx \sqrt{p}$. For efficiency, we set $C = \ell^{e_\ell}$, where ℓ is a small odd prime. The endomorphism ring of E_0 is isomorphic to a maximal quaternion order $\mathcal{O}_0$.

3.1 Generating a random isogeny starting from E_0 for key generation

The first efficient algorithm to generate a non-smooth isogeny ι starting from E_0, named **RandIsogImg**, was introduced by Nakagawa and Onuki [26]. The main idea is to compute an endomorphism of E_0 first, and then decompose it into two isogenies ρ_1 and ρ_2 by computing a two-dimensional isogeny, where the sum of $\deg(\rho_1)$ and $\deg(\rho_2)$ is $2^e \approx p$ with $e \in \mathbb{N}$. This algorithm is further extended and generalized, becoming a fundamental component of the SQIsign2D family. In particular, it is applied to generate the secret key in SQIsign2D-East.

Very recently, Basso et al. [6] proposed a new algorithm (Algorithm 3 in [6]) to efficiently generate a random non-smooth isogeny starting from E_0. The algorithm (we call it **RanIso** in our paper) requires that the characteristic has the form $p = f \cdot C \cdot D - 1$, where f is a small cofactor, $D = 2^{e_2}$ and C is smooth coprime to 2.

In this subsection, we present an improved version of **RanIso**, abbreviated as **ImRanIso**, which computes a non-smooth isogeny from E_0 under our parameter setting in key generation. Here we set $D' = 2^{\bullet}$ and $D' \approx \sqrt{D} \approx p^{1/4}$.

Since the degree of secret isogeny is approximately $p^{1/4}$, computing the secret isogeny through (D, D)-isogeny is inefficient. Different from **RanIso**, the improved algorithm **ImRanIso** adapts a CD'-isogeny instead of a C-isogeny. A sketch of **ImRanIso** is illustrated in Figure 4.

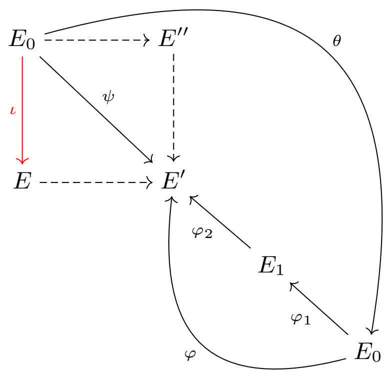

Fig. 4: A sketch of Algorithm 1. The isogeny $\varphi = \varphi_2 \circ \varphi_1$, where φ_1 (resp. φ_2) has degree D' (resp. C).

ImRanIso first generates an endomorphism $\theta \in \mathrm{End}(E_0)$ whose degree $\deg(\theta) = d(D/D' - d)CD' > p$. Since the integers C, D' are smooth and $E_0[CD'] \subset E_0(\mathbb{F}_{p^2})$, we can efficiently compute and evaluate the isogeny $\varphi : E_0 \to E'$ of degree CD', which corresponds to the ideal $I_\varphi = \mathcal{O}_0\langle\overline{\theta}, CD'\rangle$. It follows from $\varphi \circ \theta = [CD']\psi$ that

$$\psi([D']P_0) = [1/C] \circ \varphi \circ \theta(P_0); \quad \psi([D']Q_0) = [1/C] \circ \varphi \circ \theta(Q_0).$$

where $\{P_0, Q_0\}$ is a basis of $E_0[D]$. Since $\langle [D']P_0, [D']Q_0\rangle = E_0[D/D']$ and $\deg(\psi) = d(D/D' - d)$ is coprime to 2, we can compute $\Phi : E_0 \times E' \to E \times E''$ to obtain the target d-isogeny ι efficiently.

When the integer d is relatively small, **RandIsogImg** needs to set $e \approx \log_2(p)$ to confirm the degree of the endomorphism is large enough. In contrast, **ImRanIso** adapts the CD'-isogeny, and significantly decreases the degree of the two-dimensional isogeny.

Algorithm 1 $\textbf{ImRanIso}_{\mathcal{O}_0}(d, C, D, D', S)$

Require: An integer d coprime to C, D, a supersingular elliptic curve E_0 with known endomorphism ring $\mathcal{O}_0$, and a finite set $S \subset E_0$;

Ensure: The image curve E of a random d-isogeny ι starting from E_0, a finite set $\iota(S) \in E$, and the ideal I_ι corresponding to ι.

1: Select $\{P_0, Q_0\}$ such that $\langle P_0, Q_0\rangle = E_0[D]$;
2: $\theta \leftarrow \textbf{FullRepresentInteger}_{\mathcal{O}_0}(d(D/D' - d)CD')$;
3: $I_\varphi \leftarrow \mathcal{O}_0(\overline{\theta}, CD')$;
4: Compute $\varphi : E_0 \to E'$ with kernel $E[I_\varphi]$;
5: $(E; \iota(S); \emptyset) \leftarrow \textbf{KaniCod}(d, D/D' - d, E_0, E', [D']P_0, [D']Q_0, [1/C] \circ \varphi \circ \theta(P_0), [1/C] \circ \varphi \circ \theta(Q_0); S; \emptyset)$;
6: $I_\iota \leftarrow \mathcal{O}_0(\theta, d)$;
7: **return** $E, \iota(S), I_\iota$.

Remark 1. It should be noted that if θ generated in **ImRanIso** is divisible by 2 and ℓ, the ideal I_φ does not correspond to a cyclic isogeny. To circumvent this issue, one divide θ by 2 and ℓ until obtaining an endomorphism θ' such that $2, \ell$ does not divide θ'.

If $\deg(\theta') < d(D/D' - d)$, the algorithm goes back to Step 2 to generate a new endomorphism. If $\deg(\theta') = d(D/D' - d)\tilde{C}$ with $\tilde{C} \mid CD'$, we compute the $\tilde{C}$-isogeny $\varphi : E_0 \to E'$ with kernel $E[I_\varphi]$, where $I_\varphi = \mathcal{O}_0\langle\overline{\theta}', \tilde{C}\rangle$. This yields the isogeny $[1/\tilde{C}] \circ \varphi \circ \theta' : E_0 \to E'$ of degree $d(D/D' - d)$, and the d-isogeny $\iota : E_0 \to E$ can be obtained by decomposing the $(D/D', D/D')$-isogeny from $E_0 \times E'$. This countermeasure further improves the performance, since the chain length of ℓ-isogenies is reduced.

3.2 Generating a random auxiliary path

To achieve a fast verification in the SQIsign2D family, the prover computes an auxiliary path of degree $d \approx \sqrt{p}$ as a part of the conversation. The main idea of the auxiliary path generation in SQisign2D-East is to adapt **EichlerModConstraint** and **FullStrongApproximation** to generate an endomorphism $\theta \in \mathrm{End}(E)$, and then decompose θ to obtain the required auxiliary isogeny of degree $d \approx \sqrt{p}$, where E is the codomain of an N_τ-isogeny τ starting from the initial curve E_0 with known endomorphism ring. To ensure the solution of **FullStrongApproximation** satisfies the condition that $\mathrm{Nrd}(\theta) > pN_\tau^3 \approx p^{\frac{7}{4}}$, the prover sets $\mathrm{Nrd}(\theta) = d'(2^e - d')$, where $d' = d(2^a - d)$, $a \approx \log(p)/2$ and $e \approx \log(p)$. This allows the prover to proceed with a two-step isogeny evaluation process: Construct a $(2^e, 2^e)$-isogeny to evaluate the d'-isogeny, and then decompose the d'-isogeny to obtain the required auxiliary isogeny by performing a $(2^a, 2^a)$-isogeny computation.

In the following we present a generalized version of **ImRanIso**, abbreviated as **GenImRanIso**, which can compute a non-smooth isogeny from E under our parameter setting. The main procedure is summarized in Algorithm 2.

Algorithm 2 $\mathbf{GenImRanIso}_{\tau, I_\tau}(d, C, C', D, S)$

Require: An N-isogeny $\tau : E_0 \to E$ with $\mathrm{End}(E_0) \cong \mathcal{O}_0$ and $\gcd(N, CD) = 1$, an ideal I_τ which corresponds to τ, an integer $d \approx \sqrt{p}$ coprime to CD, an integer $C'|C$, and a finite set $S \subset E$;

Ensure: The image curve E_ι of a random d-isogeny ι starting from E, and a finite set $\iota(S) \in E_\iota$.

1: Select $\{P, Q\}$ such that $\langle P, Q\rangle = E[D]$;
2: $(C_0 : D_0) \leftarrow \mathbf{EichlerModConstraint}(I_\tau, 1, 1)$;
3: $\alpha \leftarrow \mathbf{FullStrongApproximation}_{d(D-d)CC'}(N, C_0, D_0)$;
4: $I_{\varphi_1} \leftarrow [I_\tau]_*\mathcal{O}_0\langle \alpha, C'\rangle$, $I_{\varphi_2} \leftarrow [I_\tau]_*\mathcal{O}_0\langle \bar{\alpha}, C\rangle$;
5: Compute $\varphi_1 : E \to E_1$ with kernel $E[I_{\varphi_1}] = \langle K_1\rangle$, $S_1 = \varphi_1(S)$;
6: Select $K \in E$ such that $\langle K_1, K\rangle = E[C']$;
7: Compute $\varphi_2 : E \to E_2$ with kernel $E[I_{\varphi_2}]$;
8: $(E_A; \iota'(S_1) \cup \iota' \circ \varphi_1(K); \emptyset) \leftarrow \mathbf{KaniCod}(d, D-d, E_1, E_2, \varphi_1(P), \varphi_1(Q), [1/C] \circ \varphi_2 \circ \alpha(P), [1/C] \circ \varphi_2 \circ \alpha(Q); S_1 \cup \{\varphi_1(K)\}; \emptyset)$;
9: Compute $[\iota']_*\hat{\varphi}_1 : E' \to E_\iota$ with kernel $\langle \iota' \circ \varphi_1(K)\rangle$;
10: **return** $E_\iota, [1/C] \circ [\iota]_*\hat{\varphi}_1 \circ \iota'(S_1)$.

The algorithm first generates the endomorphism $\alpha \in \mathfrak{O} = \mathbb{Z} + I_\tau$ by using **EichlerModConstraint** and **FullStrongApproximation**, satisfying that $\deg(\alpha) = d(D-d)CC' > pN_\tau^3 \approx p^{\frac{7}{4}}$ with $C'|C$. Since the integer C is smooth and $E[C] \subset E_0(\mathbb{F}_{p^2})$, the C'-isogeny $\varphi_1 : E \to E_1$ and the C-isogeny $\varphi_2 : E \to E_2$ can be constructed and evaluated by Vélu's formula. In this case, we are able to evaluate the isogeny from E_1 to E_2 of degree $d(D-d)$, and hence one can compute $\Phi : E_1 \times E_2 \to E' \times E''$ to obtain a d-isogeny $\iota' : E_1 \to E'$. Finally, pullback the isogeny ι' through φ_1, and obtain the auxiliary isogeny $\iota = [\varphi_1]^*\iota'$ from E of degree d. A sketch of **GenImRanIso** is illustrated in Figure 5.

Remark 2. The ideals $I_{\varphi_1}, I_{\varphi_2}$ do not correspond to cyclic isogenies when α is divisible by ℓ. Similar to the countermeasure mentioned in Remark 1, we

$$
\begin{tikzcd}
E \arrow[dr, "\varphi_1"] \arrow[dd, red, "\iota"'] \arrow[ddddrrr, bend left, "\alpha"] & & & \\
& E_1 \arrow[r, dashed] \arrow[dd, "\iota'"'] \arrow[ddr] & E'' \arrow[dd, dashed] & \\
E_\iota & & & \\
& E' \arrow[ul, "{[\iota']_*\hat{\varphi}_1}"] \arrow[r, dashed] & E_2 & \\
& & & E \arrow[ul, "\varphi_2"]
\end{tikzcd}
$$

Fig. 5: A sketch of Algorithm 2.

divide α by ℓ until α is not divisible by ℓ. Denote this newly obtained cyclic endomorphism as α'. If the degree of α' is less than $d(D-d)$, the algorithm terminates unsuccessfully and we go back to Step 3 in Algorithm 2. Otherwise, suppose $\deg(\alpha') = d(D-d)\tilde{C}$, where $\tilde{C} \mid CC'$. Then there are two cases as follows:

1. If $\tilde{C} \leq C$, we compute the $\tilde{C}$-isogeny $\varphi_2 : E \to E_2$ with kernel $E[I_{\varphi_2}]$, where $I_{\varphi_2} = \mathcal{O}_0\langle \bar{\alpha'}, \tilde{C}\rangle$. Then the isogeny $[1/\tilde{C}] \circ \varphi_2 \circ \alpha' : E \to E_2$ has degree $d(D-d)$. Subsequently, we obtain the d-isogeny $\iota : E \to E_\iota$ by computing the (D, D)-isogeny from $E \times E_2$.
2. If $\tilde{C} > C$, we compute the C-isogeny $\varphi_2 : E \to E_2$ with kernel $E[I_{\varphi_2}]$ and the $(\tilde{C}/C)$-isogeny $\varphi_1 : E \to E_1$, with kernel $E[I_{\varphi_1}]$, where $I_{\varphi_2} = \mathcal{O}_0\langle \bar{\alpha'}, C\rangle, I_{\varphi_1} = \mathcal{O}_0\langle \alpha', \tilde{C}/C\rangle$. This allows us to construct the isogeny of degree $d(D-d)$ from E_1 to E_2, following the procedures outlined in Algorithm 2.

The main improvement in efficiency compared to the previous work [28] is that our algorithm **GenImRanIso** avoids the $(2^e, 2^e)$-isogeny computation by leveraging isogenies in dimension one. To generate an endomorphism α that satisfies the norm condition $\mathrm{Nrd}(\alpha) > pN_\tau^3$ for **FullStrongApproximation**, the previous work relies on two-dimensional isogenies. In contrast, we take full advantage of the accessible torsion group $E[C]$ to efficiently construct the isogenies φ_1 and φ_2 in dimension one, leading to a significant speedup in the non-smooth isogeny generation process.

3.3 Relaxing the condition on d

In applications (especially for our scheme), we hope that we can generate a d-isogeny from an supersingular curve with $\gcd(d, C) \neq 1$, i.e., d can be divisible by ℓ. Suppose that $d = d'\ell^b$ with $\gcd(d', \ell) = 1$. We first compute an isogeny ι' of degree d' as in **GenImRanIso** and pullback the isogeny $\iota' : E_1 \to E'$ to obtain $\iota_1 : E \to E_{\iota_1}$. Here we propose two methods to obtain the d-isogeny. The first method is to supplement a ℓ^b-isogeny starting from E_{ι_1}. This can be achieved by randomly selecting a ℓ^b-isogeny ι_2. Note that $\deg(\iota_2)$ is smooth so it can be generated efficiently. The second method chooses the final ℓ^b steps in $[\iota']_*(\hat{\varphi}_1)$ to be $\hat{\iota}_2$, and let $\iota = \iota_2 \circ \iota_1$.

In the following, we consider how to modify **GenImRanIso** to achieve a faster implementation in the second method. To supplement a random ℓ^b-isogeny, we compute and evaluate the isogeny φ_3 with kernel $\langle [\ell^b]\iota' \circ \varphi_1(K) \rangle$ instead of going through the entire path $[\iota']_*\hat{\varphi}_1$. As shown in Figure 6, $\iota = \iota_2 \circ \iota_1$ is a d-isogeny starting from E, and we can evaluate ι by $\iota = [1/\deg(\varphi_3)]\varphi_3 \circ \iota' \circ \varphi_1$. Obviously, the second method is more efficient compared to the first one.

Remark 3. In the second method, the kernel of the selected auxiliary isogeny ι is $\ker(\alpha) \cap E[d]$. Essentially, regardless of whether d is divisible by ℓ, the isogeny ι is the d-isogeny of the initial part of α, i.e., $\ker(\varphi_{\mathrm{aux}}) = \ker(\alpha) \cap E[d]$. Heuristically, we expect that φ_{aux} to be chosen uniformly at random once α is chosen uniformly at random.

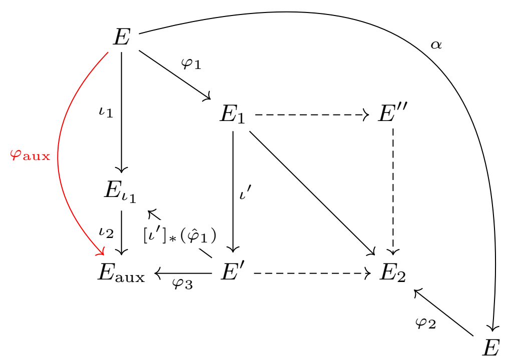

Fig. 6: Auxiliary isogeny generation (relaxing d).

4 SQIsign2D^2

Based on the new algorithms proposed in Section 3, in this section we introduce our newly developed signature scheme called SQIsign2D^2. First, we describe the detailed processes of the SQIsign2D^2 identification protocol. Next, we put forward CompactSQIsign2D^2, which features a smaller signature size compared to the original SQIsign2D^2. Finally, the response ideal sampling is briefly discussed in Section 4.3.

4.1 Identification protocol

We first present the SQIsign2D^2 identification protocol. Using the Fiat–Shamir transform [19], it is straightforward to convert the identification protocol into a corresponding signature scheme. Therefore, we omit the description of the SQIsign2D^2 digital signature.

Setup: Given a security parameter λ, let $p = C \cdot D - 1$ be a 2λ-bit prime where $C = 3^{e_3}$, $D = 2^{e_2}$, and $C \approx D \approx \sqrt{p}$. Define $D' = 2^{\lfloor e_2/2 \rfloor}$. Let $E_0 : y^2 = x^3 + x$ be a supersingular elliptic curve defined over $\mathbb{F}_p$ with known endomorphism ring $\mathrm{End}(E_0) \cong \mathcal{O}_0$. Finally, let $\{P_C, Q_C\}$ $\{P_D, Q_D\}$ be the canonical bases of $E[C]$ and $E[D]$, respectively.

Key Generation: Select a prime $N_\tau < p^{\frac{1}{4}}$ uniformly at random such that $\left(\frac{3}{N_\tau}\right) = -1$. Then use **ImRanIso** to generate an N_τ-isogeny $\tau : E_0 \to E_A$ and the corresponding ideal I_τ. Besides, the prover evaluates τ at the canonical basis of $E[D]$.

Algorithm 3 Key Generation

Require: A supersingular curve E_0 with known endomorphism ring $\mathrm{End}(E_0) \cong \mathcal{O}_0$ and a torsion basis $\{P_D, Q_D\}$ of $E_0[D]$;
Ensure: The public key E_A and the secret key $(I_\tau, N_\tau, \tau(P_D), \tau(Q_D))$.
1: Select a random prime $N_\tau < p^{\frac{1}{4}}$ such that $\left(\frac{3}{N_\tau}\right) = -1$;
2: $E_A, \{\tau(P_D), \tau(Q_D)\}, I_\tau \leftarrow \mathbf{ImRanIso}_{\mathcal{O}_0}(N_\tau, C, D, \{P_D, Q_D\})$;
3: **return** $\mathrm{pk} = (E_A), \mathrm{sk} = (N_\tau, I_\tau, \tau(P_D), \tau(Q_D))$.

Similar to the case in the original SQIsign2D-East identification protocol, the limitation that $\left(\frac{3}{N_\tau}\right) = -1$ in our protocol is to resist the attack as proposed in [9].

It is natural to ask why key generation does not compute an endomorphism of degree divisible by C^2 to minimize the chain length of $(2,2)$-isogeny computations. Indeed, to compute an auxiliary path starting from the public key E_A by Algorithm 2, the prover should evaluate τ at the torsion group $E[C]$. This enables the prover to translate the ideals I_{φ_1} and I_{φ_2} into the corresponding isogenies φ_1 and φ_2 efficiently in the signing process, as executed at Step 4 and Step 8 in Algorithm 2. When selecting an endomorphism whose degree divisible by C^2 instead of C, it is inefficient to evaluate τ at the torsion group $E[C]$, resulting in slower performance.

Commitment: The commitment phase is similar to the key generation phase. Instead of sampling an isogeny of degree $< p^{\frac{1}{4}}$, we sample an isogeny ψ such that $N_\psi = \deg(\psi) < D \approx \sqrt{p}$ and $\gcd(N_\psi, CD) = 1$. The main procedure is shown in Algorithm 4.

Algorithm 4 Commitment

Require: A supersingular curve E_0 with known endomorphism ring $\mathcal{O}_0$ and a torsion basis $\{P_D, Q_D\}$ of $E_0[D]$;
Ensure: The commitment curve E_1, the isogeny $\psi : E_0 \to E_1$ and $\psi(P_D), \psi(Q_D)$.

1: Select a random integer $N_\psi < D$ with $\gcd(N_\psi, CD) = 1$;
2: $E_1, \{\psi(P_D), \psi(Q_D)\}, I_\psi \leftarrow \mathbf{RanIso}_{\mathcal{O}_0}(N_\psi, C, D, \{P_D, Q_D\})$;
3: **return** $E_1, (N_\psi, I_\psi, \psi(P_D), \psi(Q_D))$.

Since the number of N_ψ-isogenies starting from E_0 is about N_ψ and $N_\psi < D$, we expect that the output space of **RanIso** is of size $O(p)$. On the other hand, there are approximately $p/12$ isomorphism classes in the supersingular isogeny graph. Therefore, we give the following assumption:

Assumption 1 *The commitment curve E_1 computed by **RanIso**$(N_\psi, -)$ with $N_\psi \approx \sqrt{p}$ is computationally indistinguishable from an elliptic curve chosen uniformly at random in the supersingular isogeny graph.*

To reinforce the plausibility of Assumption 1 under our parameter setting, an alternative approach is to enlarge the degree of the commitment isogeny. In Section 5.3, we propose several countermeasures to address this issue.

Challenge: Given the commitment curve E_1, the verifier just needs to choose a random integer $c \in \mathbb{Z}/C\mathbb{Z}$ and then compute $P_{\text{cha}} + [c]Q_{\text{cha}}$ as the challenge, where $\{P_{\text{cha}}, Q_{\text{cha}}\}$ is the canonical basis of $E_1[C]$. Algorithm 5 describes this process.

Algorithm 5 Challenge

Require: The commitment curve E_1.
Ensure: $K_{\text{cha}} \in E_1[C]$.

1: Compute the canonical basis $\{P_{\text{cha}}, Q_{\text{cha}}\}$ of $E_1[C]$;
2: Select a random integer $c \in \mathbb{Z}/C\mathbb{Z}$;
3: $K_{\text{cha}} \leftarrow P_{\text{cha}} + [c]Q_{\text{cha}}$;
4: **return** K_{cha}.

Response: The response phase can be divided into two parts. One part is the response isogeny generation, while the other is the auxiliary path generation from E_A. Before introducing the details of the response process, we give the definition of *D-adequate*.

Definition 2. *An integer q is D-adequate if q is odd, $q < D$ and $3 \nmid q$.*

The response isogeny generation is analogous to that of SQIsign2D-East. Firstly, compute the ideal I_φ with respect to the kernel $\langle K_{\text{cha}} \rangle$. After computing the ideal $J = \overline{I}_\tau I_\psi I_\varphi$ which corresponds to $\varphi \circ \psi \circ \hat{\tau}$, we sample an ideal $\alpha \in J$

uniformly at random such that $q = \frac{\mathrm{Nrd}(\alpha)}{\mathrm{Nrd}(J)}$ is D-adequate. Then $I_\sigma = J\frac{\overline{\alpha}}{\mathrm{Nrd}(J)}$ is the response ideal which is equivalent to J. By evaluating $\hat{\alpha}, \hat{\tau}, \psi, \varphi$, we obtain an efficient representation $(q, P_A, Q_A, \sigma(P_A), \sigma(Q_A))$ of the q-isogeny σ, where $\{P_A, Q_A\}$ is the canonical basis of $E_A[D]$.

The main difference of the response isogeny generation between the SQIsign2D-East identification protocol and ours is that we do not require that q is $(2^a, 2^b)_3$-nice. Instead, we limit q to be D-adequate. It should be noted that we no longer require $3 \nmid D - q$ as explained in subsection 3.3.

Compared with generating an efficient representation of σ, the auxiliary isogeny computation from E_A is a more expensive and complicated procedure. Firstly, we check whether

$$\left(\frac{d(D-d)}{N_\tau}\right) = \left(\frac{-1}{N_\tau}\right),$$

i.e., $\left(\frac{d(D-d)C^2}{N_\tau}\right) = \left(\frac{-1}{N_\tau}\right)$. If this condition holds, we generate an endomorphism $\theta \in \mathrm{End}(E_A)$ of norm $d(D-d)C^2$ and obtain the auxiliary d-isogeny φ_{aux} with the help of **GenImRanIso**. Otherwise, we compute the endomorphism of E_A of degree $d(D-d)C^2/3$ instead to obtain the auxiliary isogeny.

In the SQIsign2D-East identification protocol, the prover computes an additional 3-isogeny when the specific Legendre symbol condition does not hold [9]. This additional step increases the computational costs (including kernel generation and isogeny computations), even though it is not the main efficiency bottleneck. Conversely, our handling does not increase the computational costs. Notably, when the Legendre symbol condition is not satisfied, our method exhibits slightly superior performance as the degree of φ_1 in **GenImRanIso** is reduced.

To decrease the response size, the prover computes the matrix M such that $(P_{\mathrm{aux}}, Q_{\mathrm{aux}}) = (R_{\mathrm{aux}}, S_{\mathrm{aux}})M$, where $\{P_{\mathrm{aux}}, Q_{\mathrm{aux}}\}$ is the canonical basis of $E_{\mathrm{aux}}[D]$, $R_{\mathrm{aux}} = \varphi_{\mathrm{aux}}(P_A)$ and $S_{\mathrm{aux}} = \varphi_{\mathrm{aux}}(Q_A)$. From $(\sigma \circ \hat{\varphi}_{\mathrm{aux}}(P_{\mathrm{aux}}), \sigma \circ \hat{\varphi}_{\mathrm{aux}}(Q_{\mathrm{aux}})) = d(\sigma(P_A), \sigma(Q_A))M$ and $D = q + d$, we have

$$\begin{aligned}
(U_2, V_2) &= -(\sigma(P_A), \sigma(Q_A))M \\
&= \left[\frac{1}{q}\right][-q](\sigma(P_A), \sigma(Q_A))M \\
&= \left[\frac{1}{q}\right][d](\sigma(P_A), \sigma(Q_A))M \\
&= \left(\left[\frac{1}{q}\right] \circ \sigma \circ \hat{\varphi}_{\mathrm{aux}}(P_{\mathrm{aux}}), \left[\frac{1}{q}\right] \circ \sigma \circ \hat{\varphi}_{\mathrm{aux}}(Q_{\mathrm{aux}})\right).
\end{aligned}$$

The response is $(E_{\mathrm{aux}}, U_2, V_2)$. To summarize, we present the response algorithm in Algorithm 6.

Algorithm 6 Response

Require: The secret key sk, the secret information $(N_\psi, I_\psi, \psi(P_D), \psi(Q_D))$ generated in the commitment phase and the challenge K_{cha};
Ensure: the curve E_{aux} and $\{U_2, V_2\} \in E_2[D]$.
1: Compute $\varphi : E_1 \to E_2$ with kernel $\langle K_{\text{cha}} \rangle$;
2: $I_\varphi \leftarrow$ **IsogenyToIdeal**(φ, ψ, I_ψ);
3: $J \leftarrow \overline{I_\tau} I_\psi I_\varphi$, $I_\sigma = J \frac{\bar{\alpha}}{\mathrm{Nrd}(J)} \leftarrow$ **RandomEquivalentIdeal**$_D(J)$, $q \leftarrow \mathrm{Nrd}(J)$;
4: If q is not D-adequate, go back to Step 3;
5: Let P_A, Q_A be the canonical basis of $E_A[D]$;
6: Compute $\sigma(P_A)$, $\sigma(Q_A)$;
7: $d \leftarrow D - q$;
8: **if** $\left(\frac{d(D-d)}{N_\tau}\right) = \left(\frac{-1}{N_\tau}\right)$ **then**
9: $\quad E_{\text{aux}}, \{R_{\text{aux}}, S_{\text{aux}}\} \leftarrow$ **GenImRanIso**$_{\tau, I_\tau}(d, C, C, D, \{P_A, Q_A\})$;
10: **else**
11: $\quad E_{\text{aux}}, \{R_{\text{aux}}, S_{\text{aux}}\} \leftarrow$ **GenImRanIso**$_{\tau, I_\tau}(d, C, C/3, D, \{P_A, Q_A\})$;
12: **end if**
13: Let $\{P_{\text{aux}}, Q_{\text{aux}}\}$ be the canonical basis of $E_{\text{aux}}[D]$ and compute the matrix M such that $(P_{\text{aux}}, Q_{\text{aux}}) = (R_{\text{aux}}, S_{\text{aux}})M$;
14: Compute $(U_2, V_2) = -(\sigma(P_A), \sigma(Q_A))M$;
15: **return** $E_{\text{aux}}, \{U_2, V_2\}$.

Verify: From the subgroup

$$\begin{aligned} K &= \langle (P_{\text{aux}}, U_2), (Q_{\text{aux}}, V_2) \rangle \\ &= \left\langle \left(P_{\text{aux}}, \left[\frac{1}{q}\right] \sigma \circ \hat{\varphi}_{\text{aux}}(P_{\text{aux}}) \right), \left(Q_{\text{aux}}, \left[\frac{1}{q}\right] \sigma \circ \hat{\varphi}_{\text{aux}}(Q_{\text{aux}}) \right) \right\rangle \\ &= \langle ([q]P_{\text{aux}}, \sigma \circ \hat{\varphi}_{\text{aux}}(P_{\text{aux}})), ([q]Q_{\text{aux}}, \sigma \circ \hat{\varphi}_{\text{aux}}(Q_{\text{aux}}) \rangle, \end{aligned}$$

the verifier computes the (D, D)-isogeny Φ from $E_{\text{aux}} \times E_2$. The verifier accepts if the image of Φ is $E_A \times E_3$ or $E_3 \times E_A$ for an elliptic curve E_3 and the degree of $\sigma : E_A \to E_2$ is D-adequate. Otherwise, the verifier rejects.

Algorithm 7 Verify

Require: The public key pk $= (E_A)$, the commitment curve E_1, the challenge K_{cha} and the response $(E_{\text{aux}}, \{U_2, V_2\})$;
Ensure: true or false.
1: Compute the canonical basis $\{P_{\text{aux}}, Q_{\text{aux}}\}$ of $E_{\text{aux}}[D]$;
2: Compute the (D, D)-isogeny $\Phi : E_{\text{aux}} \times E_2 \to A$ with kernel $K = \langle (P_{\text{aux}}, U_2), (Q_{\text{aux}}, V_2) \rangle$;
3: **if** $A \cong E_A \times E_3$ or $A \cong E_3 \times E_A$ **then**
4: $\quad$ **if** the degree of $\hat{\sigma} : E_2 \to E_A$ decomposed from Φ is D-adequate **then**
5: $\quad\quad$ **return** true.
6: $\quad$ **end if**
7: **end if**
8: **return** false.

4.2 Compactness

Via the Fiat-Shamir transform, the signature in SQIsign2D^2 is of the form $(j(E_1), j(E_{\text{aux}}), U_2, V_2)$.

Indeed, the points $\{U_2, V_2\}$ can be further compressed. The main idea is to use the canonical basis of $E_2[D]$ to linearly represent $\{U_2, V_2\}$. Rather than storing their coordinates, we store the associated scalars, reducing the size to approximately 3λ bits. This technique has also been employed in public-key compression of SIDH [2,13].In total, the signature size is approximately 11λ bits.

Similar to SQIsign2D-East, the signature in SQIsign2D^2 can be further compressed: Instead of transmitting data related to E_{aux} and E_2, the prover sends the information associated with E_A and E_3. Correspondingly, the verifier reconstructs the (D, D)-isogeny from $E_A \times E_3$ to $E_{\text{aux}} \times E_2$. Since E_A is the public key, this eliminates the need for the prover to transmit the data related to E_A. Instead, the prover needs to give the description of the dual of the challenge isogeny, as the verifier cannot independently generate the challenge isogeny without access to the commitment curve E_1.

Overall, the compressed signature is of the form $(j(E_3), U_3, V_3, P_2, t, bin)$. Clearly, the size of $j(E_3)$ is 4λ bits, while the reduced size of $\{U_3, V_3\}$ is 3λ bits. The point $P_2 \in E_2[C]$ can be represented by an element in $\mathbb{Z}/C\mathbb{Z}$, the integer $t \in \mathbb{Z}/C\mathbb{Z}$ is used for the fast verification and *bin* is a bit. Therefore, the total size of the signature is around 9λ bits.

We refer to the compact version of SQIsign2D^2 as CompactSQIsign2D^2. The response and verification algorithms in CompactSQIsign2D^2 are described in Algorithms 8 and 9.

Algorithm 8 CompactResponse

Require: The secret key sk, the secret information $(N_\psi, I_\psi, \psi(P_D), \psi(Q_D))$ generated in the commitment phase and the message m;

Ensure: The compressed signature (E_3, U, V, P_2, t, bin).

Let K_1 be the kernel generator of φ, which is hashed from the message m and the commitment curve E_1;
Let P_2 be a generator of $\ker(\hat{\varphi})$;
Deterministically compute $Q_2 \in E_2[C]$ such that $\langle P_2, Q_2 \rangle = E_2[C]$;
Find $t \in \mathbb{Z}/C\mathbb{Z}$ and $K_1 = [t]\hat{\varphi}(Q_2)$;
Compute $(\sigma(P_A), \sigma(Q_A))$, $(E_{\text{aux}}, U_2, V_2)$, q and d as in Algorithm 6;
$(E_3; \emptyset; \{U, V\}) \leftarrow \mathbf{KaniCod}(q, d, E_{\text{aux}}, E_2, P_{\text{aux}}, Q_{\text{aux}}, [q]U_2, [q]V_2; \emptyset; \{[\frac{1}{d}]\sigma(P_A), [\frac{1}{d}]\sigma(Q_A))\}$;
Let M, M' be the Montgomery coefficient of E_A and E_3, respectively;
if $M \leq M'$ **then**
    $bin \leftarrow 0$;
else
    $bin \leftarrow 1$;
end if
return E_3, U, V, P_2, t, bin.

Algorithm 9 CompactVerify

Require: The public key $pk = (E_A)$, the message m and the compressed signature (E_3, U, V, P_2, t, bin);
Ensure: true or false.

Compute the canonical basis $\{P_A, Q_A\}$ of $E_A[D]$;
Compute the (D, D)-isogeny $\Phi : E_A \times E_3 \to A$ with kernel $\langle (P_A, U), (Q_A, V) \rangle$;
if $A \not\cong E' \times E''$ for elliptic curves E', E'' **then**
  return false.
end if
Let M', M'' be the Montgomery coefficient of E', E'';
if $M' > M''$ **then**
  $(M', M'') \leftarrow (M'', M')$;
end if
if $bin = 0$ **then**
  $E_2 \leftarrow E'$;
else
  $E_2 \leftarrow E''$;
end if
if the degree of $\sigma : E_A \to E_2$ decomposed from Φ is not D-adequate **then**
  return false
end if
Deterministically compute $Q_2 \in E_2[C]$ such that $\langle P_2, Q_2 \rangle = E_2[C]$;
Compute the C-isogeny $\hat{\varphi} : E_2 \to E_1$ with kernel $\langle P_2 \rangle$ and $L = \hat{\varphi}(Q_2)$;
Let K_1 be the kernel generator of φ, which is hashed from the message m and the commitment curve E_1;
if $K_1 = [t]L$ **then**
  return true;
else
  return false;
end if

4.3 Response ideal sampling

In SQIsign2D^2, the degree q of the response isogeny is D-adequate, i.e., q is odd, $q < D$ and $3 \nmid q$. The probability that $q \bmod 2 \equiv 1$ is $1/2$, while the probability that $3 \nmid q$ is $2/3$. Therefore, the probability that finding such an integer q that satisfies both conditions is expected to be $1/3$.

The Gaussian heuristic illustrates that in a lattice $\Lambda \subseteq \mathbb{R}^4$, the number of $\alpha \in \Lambda$ with norm less than R is approximately $\frac{\pi^2 R^4}{2\mathrm{Vol}(\Lambda)}$. When applied to $\Lambda = J$ and $R = \sqrt{D\mathrm{Nrd}(J)}$, there are around $\frac{2\pi^2 D^2}{p} \approx 2\pi^2 D C^{-1}$ elements in J with norm less than $\|\alpha\| < R$. Since $\mathcal{O}_R(J)^\times = \{\pm 1\}$, the number of the response isogenies of degree less than D is approximately $\pi^2 D C^{-1}$. Hence, the failure probability of finding such q is

$$\Pr\left[\text{none of } q \text{ are } D\text{-adequate}\right] = \left(1 - \frac{1}{3}\right)^{\pi^2 D C^{-1}} = \left(\frac{2}{3}\right)^{\pi^2 D C^{-1}}.$$

To further decrease the failure probability, one may set $p = f \cdot D \cdot C - 1$, where f is a small cofactor coprime to CD, and adapt the "gcd-trick" [9, Section 4.1] in the response phase. However, according to our experiments of SQIsign2D^2, we expect that the failure probability is small enough for practice.

5 Security

In this section we propose a formal security analysis of the SQIsign2D^2 identification protocol. The correctness is straightforward, hence our analysis focuses on demonstrating its special soundness and zero-knowledge properties.

Same as other SQIsign2D variants, the zero-knowledge property of SQIsign2D^2 relies on the fundamental assumption that the commitment curve E_1 is computationally indistinguishable from an elliptic curve chosen uniformly at random in the supersingular isogeny graph. To strengthen the plausibility of this assumption in SQIsign2D^2, in Section 5.3 we present several alternative countermeasures to address this critical requirement.

5.1 Special soundness

The special soundness proof follows a structure analogous to those of SQIsignHD and SQIsign2D-East. The hard problem underlying the special soundness proof is known as Supersingular Endomorphism Problem:

Problem 1 (Supersingular Endomorphism Problem). Given a supersingular elliptic curve E over $\mathbb{F}_{p^2}$ with p prime, find a non-trivial endomorphism of E that can be efficiently evaluated.

From [30], the extraction of any non-scalar endomorphism $\mathrm{End}(E_A)$ enables the complete reconstruction of $\mathrm{End}(E_A)$. This allows for the efficient recovery of the secret ideal I_τ and its corresponding isogeny τ in polynomial time. Therefore, the proof reduces to demonstrating the extraction of a non-scalar endomorphism $\alpha \in \mathrm{End}(E_A)$ from two valid conversations with the same commitment and different challenges.

Theorem 2. *The SQIsign2D^2 identification protocol has the special soundness property. That is, given two valid conversations with the same commitment and different challenges, one can extract a non-scalar endomorphism $\alpha \in \mathrm{End}(E_A)$ that can be efficiently evaluated.*

Proof. Assume that the two valid conversations are $(E_1, K_{cha}, E_{\mathrm{aux}}, U_2, V_2)$ and $(E_1, K'_{cha}, E'_{\mathrm{aux}}, U'_2, V'_2)$ with $\langle K_{cha} \rangle \neq \langle K'_{cha} \rangle$, respectively. From K_{cha} and K'_{cha} one can reveal the challenge isogenies $\varphi : E_1 \to E_2$ and $\varphi' : E_1 \to E'_2$, respectively. Then the response isogenies σ and σ' are recovered with respect to the knowledge of $(E_{\mathrm{aux}}, P_{\mathrm{aux}}, Q_{\mathrm{aux}}, E_2, U_2, V_2)$ and $(E'_{\mathrm{aux}}, P'_{\mathrm{aux}}, Q'_{\mathrm{aux}}, E'_2, U'_2, V'_2)$, where $\{P_{\mathrm{aux}}, Q_{\mathrm{aux}}\}$ and $\{P'_{\mathrm{aux}}, Q'_{\mathrm{aux}}\}$ are the canonical bases of $E_{\mathrm{aux}}[D]$ and $E'_{\mathrm{aux}}[D]$, respectively. Therefore, one can extract an endomorphism $\alpha = \widehat{\sigma'} \circ \varphi' \circ \hat{\varphi} \circ \sigma$, as illustrated in Figure 7.

$$\begin{tikzcd}
& E_1 \arrow[dr, "\varphi'"] & \\
E_2 \arrow[ur, "\hat{\varphi}"] & E_0 \arrow[u, "\psi"'] \arrow[d, "\tau"] & E_2' \arrow[dl, "\widehat{\sigma'}"] \\
& E_A \arrow[ul, "\sigma"] &
\end{tikzcd}$$

Fig. 7: A sketch of the special soundness proof.

It remains to prove that the endomorphism α is non-scalar. Assume that $\alpha = [n]$ for some integer n. Then $\alpha(P) = \infty$ for all $P \in E[C]$. It follows from $\gcd(q, C) = 1$, $\gcd(q', C) = 1$ that $\varphi' \circ \hat{\varphi} = [C]$, i.e., $\ker(\varphi) = \ker(\varphi')$. This leads to a contradiction. Hence, we conclude that α is a non-scalar endomorphism of E_A, which ends the proof. ■

5.2 Zero knowledge

The zero-knowledge proof of the SQIsign2D^2 identification protocol parallels that of the SQIsign2D-East identification protocol. In the proof, we also define two random oracles, to simulate the response isogeny and the auxiliary isogeny, respectively.

Definition 3. *Given an integer D, a Random Uniform Adequate Degree Isogeny Oracle (**RUADIO**) is an oracle taking as input a supersingular elliptic curve E and returning the tuple $(\sigma(P), \sigma(Q))$, where $\langle P, Q \rangle = E[D]$, $\sigma : E \to E'$ is a random isogeny and $\deg(\sigma) = q$ is D-adequate. Besides, the random oracle satisfies the following properties:*

- *The distribution of E' is computationally indistinguishable from that of an elliptic curve chosen uniformly at random in the supersingular isogeny graph;*
- *The conditional distribution of σ given E' is uniform among isogenies from E to E' whose degrees are D-adequate.*

Definition 4. *Given an integer D, a Fixed Degree Isogeny Oracle (**FIDIO**) is an oracle taking as input a supersingular elliptic curve E and an integer N and returning the tuple $(\varphi_{\mathrm{aux}}(P), \varphi_{\mathrm{aux}}(Q))$, where $\{P, Q\}$ is the canonical basis of $E[D]$ and $\varphi_{\mathrm{aux}} : E \to E'$ is a uniformly random N-isogeny.*

Compared with the SQIsign2D-East identification protocol, we use the random oracle **RUADIO** to simulate the response isogeny σ, which has a different requirement on $\deg(\sigma)$: The SQIsign2D-East identification protocol requires $\deg(\sigma)$ to be $(2^a, 2^b)_3$-nice, while ours demands that $\deg(\sigma)$ to be D-adequate. As for the auxiliary isogeny simulation, we employ the same random oracle

FIDIO. Similar to the SQIsign2D-East identification protocol, we assume that the following problem is hard:

Problem 1 *Let D be the integer defined in the parameter setting and E_A be the public curve. Define the distribution of the reduced norm of the response ideals I_σ on $\mathbb{Z}$ by $\mathcal{Q}$. Suppose that $\mathcal{D}_\mathcal{U}$ and $\mathcal{D}_\mathcal{R}$ represent the uniform distribution $\mathcal{U}_{\boldsymbol{Iso}(E_A,q)} = \{\varphi : E_A \to * \mid \deg(\varphi) = D - q\}$ and the output distribution of Algorithm 2, respectively. Let $S = \{\varphi_{\text{aux}} : E_A \to * \mid \deg(\varphi_{\text{aux}}) = D - q\}$ be a set of size $M > \log(N_\tau)$, where either*

1. *S is sampled by first sampling $q \sim \mathcal{Q}$, then sampling φ_{aux} from $\mathcal{D}_\mathcal{U}$; or*
2. *S is sampled by first sampling $q \sim \mathcal{Q}$, then sampling φ_{aux} from $\mathcal{D}_\mathcal{R}$.*

The problem is, given E_A, D, S, to distinguish between the two cases with a polynomial number of queries to $\mathcal{Q}$, ***FIDIO*** *and $\mathcal{D}_\mathcal{R}$.*

As discussed in [28, Remark 5], a natural approach to addressing Problem 1 is to determine the endomorphism by reverse engineering the algorithms. This task is equivalent to solving Supersingular Endomorphism Problem, as defined in Problem 1. Consequently, we conjecture that Problem 1 is computationally hard. A rigorous analysis of the hardness of Problem 1 is left as future work.

Theorem 3. *Suppose that the commitment curve E_1 is computationally indistinguishable from an elliptic curve chosen uniformly at random in the supersingular isogeny graph, and Problem 1 is computationally hard. Then, the SQIsign2D^2 identification protocol is special honest-verifier zero-knowledge (SHVZK) in the* ***RUADIO*** *and* ***FIDIO*** *models. That is, there exists a simulator $\mathcal{S}$ with access to* ***RUADIO*** *and* ***FIDIO****, such that the distribution of the accepting conversations generated by $\mathcal{S}$ is computationally indistinguishable from those of honest executions of the SQIsign2D^2 identification protocol.*

Proof. We proceed similarly as the zero-knowledge proof of SQIsign2D-East. The simulator $\mathcal{S}$ operates as follows: The simulator first adapts the **RUADIO** model to generate an efficient representation $(E_A, P_A, Q_A, E_2', \sigma'(P_A), \sigma'(Q_A))$ of a q'-isogeny $\sigma' : E_A \to E_2'$, where $\{P_A, Q_A\}$ is the canonical basis of $E_A[D]$ and q' is D-adequate. Subsequently, the simulator $\mathcal{S}$ uniformly samples a C-isogeny $\widehat{\varphi'} : E_2' \to E_1'$. Finally, the simulator constructs the $(D - q')$-isogeny $\varphi'_{\text{aux}} : E_A \to E'_{\text{aux}}$ with the help of **FIDIO**. The resulting simulated transcript takes the form $(E_1', \varphi', E'_{\text{aux}}, U_2', V_2')$, where U_2', V_2' are computed from φ'_{aux} and σ'.

Assume that the real transcript is $(E_1, \varphi, E_{\text{aux}}, U_2, V_2)$. In the following, we prove that the two transcripts are computationally indistinguishable.

From the first property of **RUADIO**, E_2' is uniformly distributed in the supersingular isogeny graph. Since the isogeny $\widehat{\varphi'} : E_2' \to E_1'$ is chosen uniformly at random, the codomain E_1' of $\widehat{\varphi'}$ is also uniformly random. Hence, E_1 and E_1' are computationally indistinguishable. Furthermore, as φ, φ' are sampled from the same way, their distributions are the same.

The second property of **RUADIO** ensures that the response isogeny σ' is uniformly distributed among all isogenies of D-adequate degree from E_A to E_2'. Similarly, the response isogeny σ in the real transcript has the same distribution.

Thanks to the hardness of Problem 1, the auxiliary isogeny φ_{aux} in the real transcript is computationally indistinguishable from a random isogeny φ'_{aux} of degree $D-q$ starting from E_A.

Therefore, it remains to show that $(E_{\text{aux}}, U_2, V_2)$ and $(E'_{\text{aux}}, U'_2, V'_2)$ are computationally indistinguishable. Given the computational indistinguishability of $(\sigma, \varphi_{\text{aux}})$ and $(\sigma', \varphi'_{\text{aux}})$, it follows that the response $(E_{\text{aux}}, U_2, V_2)$ in the real identification protocol is computationally indistinguishable from $(E'_{\text{aux}}, U'_2, V'_2)$ in the simulated transcript. This completes the proof. ■

5.3 Commitment sampling

The zero-knowledge property critically depends on Assumption 1, i.e., the commitment curve E_1 is computationally indistinguishable from an elliptic curve chosen uniformly at random in the supersingular isogeny graph.

During the commitment phase of SQIsign2D^2, we construct the commitment isogeny of degree N_ψ by using **ImRanIso**. Given our parameter constraint $D = 2^{e_2}$ with $D \,\|\, p+1$, to evaluate the commitment isogeny efficiently via (D,D)-isogeny computations, we let $N_\psi < D \approx \sqrt{p}$. In the following, we introduce three methods to enlarge the degree of the commitment isogeny, making Assumption 1 more robust.

Double path: The first method is based on the algorithm **FastDoublePath**, which is utilized in the key generation and commitment phases in SQIsignHD [14, Section 3.3].

Here we briefly review the algorithm **FastDoublePath**. First, compute an endomorphism γ of E_0 with degree $C'^2D'^2$, where $C' \mid C$ and $D' \mid D$. Then there exist two isogenies ρ_1 and ρ_2 from E to E' with kernel

$$\begin{aligned}\ker(\rho_1) &= \ker(\gamma) \cap E_0[C'D'],\\ \ker(\rho_2) &= \ker(\bar{\gamma}) \cap E_0[C'D'].\end{aligned}$$

Consider the following diagram:
where $\rho_1 = \widehat{\theta'_1} \circ \theta_1$, $\rho_2 = \hat{\theta}_2 \circ \theta'_2$, $\deg(\theta_1) = \deg(\theta_2) = C'$, $\deg(\theta'_1) = \deg(\theta'_2) = D'$.

From the above diagram, the isogeny $\psi_1 = ([\theta'_1]_*\theta_2) \circ \theta_1$ is C'^2-isogeny, while the isogeny $\psi_2 = ([\theta_2]_*\theta'_1) \circ \theta'_2$ is D'^2-isogeny. Both are isogenies from the initial curve E_0 to the commitment curve E_1. In the challenge phase, we use ψ_2 to efficiently pullback the challenge isogeny as $\gcd(C, D') = 1$. On the other hand, we use ψ_1 to evaluate the response isogeny σ on $E_A[D]$ in the response phase since $\gcd(D, C') = 1$.

In this case, the degree of the commitment isogeny is approximately p. Therefore, it is reasonable to assume that the commitment curve E_1 is computationally indistinguishable in the supersingular graph. As is well known, SQIsignHD is attractive for its fast signing within the SQIsign family. Therefore, we expect that

$$\begin{tikzcd}
 & E' \arrow[d, "{[\theta_2]_*\theta_1'}"] & \\
E_0 \arrow[ur, "\theta_2'"] \arrow[dr, "\theta_1"'] & E_1 & E''' \arrow[ul, "\theta_2"'] \arrow[dl, "\theta_1'"] \\
 & E'' \arrow[u, "{[\theta_1']_*\theta_2}"'] &
\end{tikzcd}$$

Fig. 8: Commitment generation using the technique in SQIsignHD.

this approach to generating the commitment isogeny will not compromise the efficiency of $\mathrm{SQIsign2D}^2$.

3-isogeny adaption: This method aims to apply a random C'-isogeny to extend the commitment isogeny, where $C'|C$.

To be precise, after computing the N_{ψ_1}-isogeny $\psi_1 : E_0 \to E_1'$ using **RanIso** with $N_{\psi_1} \approx \sqrt{p}$, the prover selects a random C'-isogeny ψ_2 from E_1' to E_1. The commitment curve is then set as E_1, with the commitment isogeny defined as $\psi = \psi_2 \circ \psi_1$ and the associated ideal as I_ψ.

A critical challenge arises in translating the composition of the commitment isogeny and the challenge isogeny to the associated ideal in the response phase, due to $\gcd(\deg(\psi), \deg(\varphi)) \neq 1$. We analyze this through the following cases:

- $\ker(\varphi) \cap \ker(\hat{\psi}_2) = \{\infty\}$, where ∞ is the infinity point of E_1: From the knowledge of $\hat{\psi}(\ker(\varphi))$, the prover is able to directly compute the ideal $I_{[\psi]^*\varphi}$ corresponding to $[\psi]^*\varphi$. Hence, the ideal corresponding to $\varphi \circ \psi$ is $I_\psi \cap I_{[\psi]^*\varphi}$.
- $\ker(\varphi) \cap \ker(\hat{\psi}_2) \neq \{\infty\}$: Assume that $\langle K_{cha} \rangle \cap \ker(\hat{\psi}_2) = \langle K_3 \rangle$, where $\#K_3 = \mathrm{ord}(K_3)|C'$. In this case, the challenge isogeny φ can be decomposed as $\varphi = \varphi'' \circ \varphi'$, where $\varphi' : E_1 \to E_1''$ has kernel $\langle K_3 \rangle$. Similarly, one can decompose $\psi_2 = \psi_2'' \circ \psi_2'$, where $\psi_2'' : E_1'' \to E_1$ is the dual of φ'. Clearly, the prover is able to compute the ideals corresponding to $[\psi_1]^*(\psi_2')$ and $[\psi_2' \circ \psi_1]^*(\varphi'')$. Therefore, the composition of the commitment isogeny and the challenge isogeny is $[\mathrm{ord}(K_3)] \left(I_{\psi_1} \cap I_{[\psi_1]^*(\psi_2')} \cap I_{[\psi_2' \circ \psi_1]^*(\varphi'')} \right)$.

As a result, the degree of the commitment isogeny is $N_\psi C'$. When $C' \approx C$, the degree of the commitment isogeny is approximately p.

$(3,3)$-isogeny adaption: Note that $p = CD - 1$, where $C = 3^{e_3}$ and $D = 2^{e_2}$. Therefore, one can compute the commitment isogeny by (CD, CD)-isogenies.

To be precise, the prover begins by selecting a random integer $N_\psi < CD$, and then computes an endomorphism θ of E_0 with reduced norm $N_\psi(CD - N_\psi)$.

$$\begin{tikzcd}
E_0 \arrow[r, "\psi_1"] \arrow[d, "{[\psi_2'\circ\psi_1]^*(\varphi'')}"'] & E_1' \arrow[r, "\psi_2'"] & E_1'' \arrow[r, bend left, "\psi_2''"] \arrow[d, "\varphi''"] & E_1 \arrow[l, bend left, "\varphi'"] \\
E \arrow[rr, dashed] & & E_2
\end{tikzcd}$$

Fig. 9: A sketch of the second case.

Subsequently, the prover computes the (CD, CD)-isogeny from $E_0 \times E_0$ with kernel $\langle([N_\psi]P_0, \theta(P_0)), ([N_\psi]Q_0, \theta(Q_0))\rangle$, where $\{P_0, Q_0\}$ is the canonical basis of $E_0[CD]$. By decomposition, the N_ψ-isogeny $\psi : E_0 \to E_1$ can be obtained. Since C and D are smooth, the evaluation of the (CD, CD)-isogeny is computationally feasible. Note that the degree of the commitment isogeny $N_\psi < CD = p + 1$. Heuristically, the commitment curve E_1 is close to a random elliptic curve in the supersingular isogeny graph.

Currently, the computation of $(3, 3)$-isogenies is no as efficient as that of the $(2, 2)$-isogenies [12,15]. With further optimizations in $(3, 3)$-isogeny computations, we believe that this countermeasure can be made efficient in practice.

6 Implementation

In this section, we implement SQIsign2D^2 and give efficiency comparisons between SQIsign2D^2 and other SQIsign2D variants.

Section 6.1 provides the parameter settings and the public-key/signature sizes of SQIsign2D^2 at different security levels. A theoretical comparison of isogeny operation counts between our protocols and other SQIsign2D variants is proposed in Section 6.2, while Section 6.3 presents benchmarking results for SQIsign2D^2 against SQIsign2D-East.

6.1 Parameter setting

Parameter setting is straightforward in SQIsign2D^2: For the security parameter λ, we just need to sample a 2λ-bit prime $p = 2^{e_2}3^{e_3} - 1$ with $2^{e_2} \approx 3^{e_3}$. It is easy to be found by performing an exhaustive search.

The signature of SQIsign2D^2 takes 11λ bits. As discussed in Section 4.2, the size of the signature can be further reduced to 9λ bits. Table 1 presents the used primes and the corresponding public-key/signature sizes for different security levels.

6.2 Cost estimates

The computational costs of isogeny-based signature schemes, including all the SQIsign2D variants, are dominated by isogeny computations. Table 2 reports the required isogeny computations of different degrees.

Table 1: Parameter settings, public-key sizes and (compressed) signature sizes (expressed in bytes) for different security levels.

Security	Prime	Public-key size	Signature size	
			Uncom.	Com.
NIST-I	$p = 2^{131} \cdot 3^{78} - 1$	64	182	154
NIST-III	$p = 2^{194} \cdot 3^{121} - 1$	98	274	228
NIST-V	$p = 2^{263} \cdot 3^{156} - 1$	128	359	299

From Table 2, it is easy to see that SQIsign2D^2 reduces two-dimensional isogeny computations compared to existing schemes in key generation. Besides, we expect that SQIsign2D^2 would be more efficient in signing than other existing isogeny-based signatures.

Regarding the signing phase, SQIsign2D^2 achieves the shortest chain length of $(2,2)$-isogeny among all the schemes. Even though SQIsign2D^2 needs to compute a number of 3-isogenies, we anticipate that this does not bring significant computational overhead. Compared to PRISM-sig, SQIsign2D^2 saves considerable two-dimensional isogenies. Besides, PRISM-sig suffers from its slow LLL implementation [3, Section 5.4]. As a result, SQIsign2D^2 remains highly competitive in terms of computational efficiency compared to PRISM-sig.

Finally, SQIsign2D^2 achieves rapid verification performance, matching the efficiency of SQIsign2D-West and SQIsign2D-East while significantly outperforming PRISM-sig.

6.3 Experimental results

Based on the SQIsign2D-East implementation[6], we provide a proof-of-concept implementation of SQIsign2D^2 in Julia. We compile and benchmark our code on Intel(R) Core(TM) i9-12900K 3.20 GHz with TurboBoost and hyperthreading features disabled. The efficiency comparison is illustrated in Table 3. Our code is available at

`https://github.com/Kaizhan-Lin/SQIsign2DSquare`.

As we can see in Table 3, SQIsign2D^2 significantly reduces the key generation and signing times compared to SQIsign2D-East. At the NIST-I level, key generation achieves an acceleration factor of 2.63, while signing offers a $\times 2.15$ speedup.

The compact versions of SQIsign2D^2 and SQIsign2D-East show increased computational costs compared to their non-compact counterparts. Nevertheless, CompactSQIsign2D^2 retains significant performance advantages. For example,

[6] `https://github.com/hiroshi-onuki/SQIsign2D-East.jl`

Table 2: Cost Estimates for SQIsign2D variants and SQIsign2D^2 using NIST-I parameters. The data in parentheses varies slightly depending on the specific situations.

Signature	Phase	Isogeny Computation			
		2	3	5	(2,2)
SQIsign2D-West [4]	KeyGen	-	-	-	496
	Sign	(248)	-	-	992
	Verify	(248)	-	-	(126)
SQIsign2D-East [28]	KeyGen	-	-	-	253
	Sign	127	(2)	(1)	641
	Verify	127	(2)	(1)	129
PRISM-sig [3]	KeyGen	-	-	-	496
	Sign	-	-	-	496
	Verify	-	-	-	248
SQIsign2D^2 (This work)	KeyGen	65	78	-	66
	Sign	-	(390)	-	262
	Verify	-	78	-	131

CompactSQIsign2D^2 achieves an acceleration factor of 1.77 for signing at the NIST-I level.

The verification procedure of SQIsign2D^2 remains comparable to that of SQIsign2D-East. SQIsign2D-East may involve the small-degree isogeny computations in dimension one in verification. On the other hand, SQIsign2D^2 requires the verifier to additionally reveal the degree q of the response isogeny by pairings to check q is D-adequate.

Indeed, the performance of SQIsign2D^2 can be further improved through optimizations proposed in the literature. For example, one can optimize the pairing computations via biextensions [32]. Besides, the discrete logarithm computations can be accelerated using the tricks proposed in [23]. We leave the optimized implementation of SQIsign2D^2 as future work.

7 Conclusion

In this paper, we presented a fast approach for generating non-smooth isogenies starting from arbitrary curves that are connected to E_0. Leveraging the accessible isogenies in dimension one, we introduced SQIsign2D^2, a new variant of the SQIsign2D family. SQIsign2D^2 demonstrates superior performance in both key generation and signing phases compared to other existing SQIsign2D schemes.

While SQIsign2D^2 advances the state-of-the-art, further optimizations of its computational efficiency remain critical. Especially, CompactSQIsign2D^2 involves additional two-dimensional isogeny computations in the signature compression process. The development of new techniques to eliminate this computational overhead is left as future work. As discussed in Section 6.3, it is also interesting to further explore how to efficiently generate the commitment isogeny of degree approximately equal to p.

Table 3: Efficiency Comparison between SQIsign2D-East and SQIsign2D^2 for different security levels. The compact version of SQIsign2D^2 is named CompactSQIsign2D^2. The experimental results are obtained by averaging over 100 experiments and expressed in milliseconds. The last column provides the acceleration factor.

Security	Procedure	SQIsign2D-East	SQIsign2D^2	A.F.
NIST-I	KeyGen	560	213	2.63
	Sign	1263	587	2.15
	Verify	296	247	1.20
NIST-III	Keygen	924	371	2.49
	Sign	2675	1265	2.11
	Verify	474	557	0.85
NIST-V	KeyGen	1523	486	3.13
	Sign	4318	1973	2.19
	Verify	771	855	0.90

Security	Procedure	CompactSQIsign2D-East	CompactSQIsign2D^2	A.F.
NIST-I	KeyGen	617	224	2.75
	Sign	1693	959	1.77
	Verify	304	254	1.20
NIST-III	Keygen	999	364	2.74
	Sign	3052	1702	1.79
	Verify	567	613	0.92
NIST-V	KeyGen	1561	693	2.25
	Sign	4928	2477	1.99
	Verify	779	833	0.94

References

1. Azarderakhsh, R., Campagna, M., Costello, C., De Feo, L., Hess, B., Hutchinson, A., Jalali, A., Jao, D., Karabina, K., Koziel, B., LaMacchia, B., Longa, P., Naehrig, M., Pereira, G., Renes, J., Soukharev, V., Urbanik, D.: Supersingular Isogeny Key Encapsulation (2020), http://sike.org
2. Azarderakhsh, R., Jao, D., Kalach, K., Koziel, B., Leonardi, C.: Key Compression for Isogeny-Based Cryptosystems. In: Proceedings of the 3rd ACM International Workshop on ASIA Public-Key Cryptography. pp. 1–10 (2016)
3. Basso, A., Borin, G., Castryck, W., Santos, M.C.R., Invernizzi, R., Leroux, A., Maino, L., Vercauteren, F., Wesolowski, B.: PRISM: Simple And Compact Identification and Signatures From Large Prime Degree Isogenies. Cryptology ePrint Archive, Paper 2025/135 (2025), https://eprint.iacr.org/2025/135
4. Basso, A., Dartois, P., Feo, L.D., Leroux, A., Maino, L., Pope, G., Robert, D., Wesolowski, B.: SQIsign2D–West. In: Chung, K.M., Sasaki, Y. (eds.) Advances in Cryptology – ASIACRYPT 2024. pp. 339–370. Springer Nature Singapore, Singapore (2025)
5. Basso, A., Fouotsa, T.B.: New SIDH Countermeasures for a More Efficient Key Exchange. In: Guo, J., Steinfeld, R. (eds.) Advances in Cryptology – ASIACRYPT 2023. pp. 208–233. Springer Nature Singapore, Singapore (2023)
6. Basso, A., Maino, L.: Poké: A compact and efficient pke from higher-dimensional isogenies. In: Fehr, S., Fouque, P.A. (eds.) Advances in Cryptology – EUROCRYPT 2025. pp. 94–123. Springer Nature Switzerland, Cham (2025)
7. Basso, A., Maino, L., Pope, G.: FESTA: Fast Encryption from Supersingular Torsion Attacks. In: Guo, J., Steinfeld, R. (eds.) Advances in Cryptology – ASIACRYPT 2023. pp. 98–126. Springer Nature Singapore, Singapore (2023)
8. Bernstein, D.J., de Feo, L., Leroux, A., Smith, B.: Faster computation of isogenies of large prime degree. In: Galbraith, S. (ed.) ANTS-XIV - 14th Algorithmic Number Theory Symposium. Proceedings of the Fourteenth Algorithmic Number Theory Symposium (ANTS-XIV), vol. 4, pp. 39–55. Mathematical Sciences Publishers, Auckland, New Zealand (Jun 2020). https://doi.org/10.2140/obs.2020.4.39, https://hal.inria.fr/hal-02514201
9. Castryck, W., Chen, M., Invernizzi, R., Lorenzon, G., Vercauteren, F.: Breaking and Repairing SQIsign2D-East. Cryptology ePrint Archive, Paper 2024/1453 (2024), https://eprint.iacr.org/2024/1453
10. Castryck, W., Decru, T.: An Efficient Key Recovery Attack on SIDH. In: Advances in Cryptology–EUROCRYPT 2023: 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23-27, 2023, Proceedings, Part V. pp. 423–447. Springer (2023)
11. Chavez-Saab, J., Santos, M.C.R., Feo, L.D., Eriksen, J.K., Hess, B., Kohel, D., Leroux, A., Longa, P., Meyer, M., Panny, L., Patranabis, S., Petit, C., Henríquez, F.R., Schaeffler, S., Wesolowski, B.: SQIsign (2023), manuscript available at http://sqisign.org
12. Corte-Real Santos, M., Costello, C., Smith, B.: Efficient (3, 3)-isogenies on fast Kummer surfaces. Research in Number Theory **11**(1), 25 (Jan 2025)
13. Costello, C., Jao, D., Longa, P., Naehrig, M., Renes, J., Urbanik, D.: Efficient Compression of SIDH Public Keys. In: Coron, J.S., Nielsen, J.B. (eds.) Advances in Cryptology – EUROCRYPT 2017. pp. 679–706. Springer International Publishing, Cham (2017)

14. Dartois, P., Leroux, A., Robert, D., Wesolowski, B.: SQIsignHD: New Dimensions in Cryptography. In: Joye, M., Leander, G. (eds.) Advances in Cryptology – EUROCRYPT 2024. pp. 3–32. Springer Nature Switzerland, Cham (2024)
15. Dartois, P., Maino, L., Pope, G., Robert, D.: An Algorithmic Approach to (2, 2)-Isogenies in the Theta Model and Applications to Isogeny-Based Cryptography. In: Chung, K.M., Sasaki, Y. (eds.) Advances in Cryptology – ASIACRYPT 2024. pp. 304–338. Springer Nature Singapore, Singapore (2025)
16. De Feo, L., Kohel, D., Leroux, A., Petit, C., Wesolowski, B.: SQISign: Compact Post-quantum Signatures from Quaternions and Isogenies. In: Moriai, S., Wang, H. (eds.) Advances in Cryptology – ASIACRYPT 2020. pp. 64–93. Springer International Publishing, Cham (2020)
17. De Feo, L., Leroux, A., Longa, P., Wesolowski, B.: New Algorithms for the Deuring Correspondence: Towards Practical and Secure SQISign Signatures. In: Hazay, C., Stam, M. (eds.) Advances in Cryptology – EUROCRYPT 2023. pp. 659–690. Springer Nature Switzerland, Cham (2023)
18. Duparc, M., Fouotsa, T.B.: SQIPrime: A Dimension 2 Variant of SQISignHD with Non-smooth Challenge Isogenies. In: Chung, K.M., Sasaki, Y. (eds.) Advances in Cryptology – ASIACRYPT 2024. pp. 396–429. Springer Nature Singapore, Singapore (2025)
19. Fiat, A., Shamir, A.: How To Prove Yourself: Practical Solutions to Identification and Signature Problems. In: Odlyzko, A.M. (ed.) Advances in Cryptology — CRYPTO' 86. pp. 186–194. Springer Berlin Heidelberg, Berlin, Heidelberg (1987)
20. Fouotsa, T.B., Moriya, T., Petit, C.: M-SIDH and MD-SIDH: Countering SIDH Attacks by Masking Information. In: Hazay, C., Stam, M. (eds.) Advances in Cryptology – EUROCRYPT 2023. pp. 282–309. Springer Nature Switzerland, Cham (2023)
21. Jao, D., De Feo, L.: Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies. In: Yang, B.Y. (ed.) Post-Quantum Cryptography. pp. 19–34. Springer Berlin Heidelberg, Berlin, Heidelberg (2011)
22. Kani, E.: The number of curves of genus two with elliptic differentials. Journal für die reine und angewandte Mathematik **1997**(485), 93–122 (1997)
23. Lin, K., Wang, W., Xu, Z., Zhao, C.A.: A Faster Software Implementation of SQIsign. IEEE Transactions on Information Theory **70**(9), 6679–6689 (2024)
24. Maino, L., Martindale, C., Panny, L., Pope, G., Wesolowski, B.: A direct key recovery attack on SIDH. In: Advances in Cryptology–EUROCRYPT 2023: 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23-27, 2023, Proceedings, Part V. pp. 448–471. Springer (2023)
25. Mumford, D.: Abelian Varieties, Tata Institute of Fundamental Research Studies in Mathematics, vol. 5. Tata Institute of Fundamental Research, Bombay (2012), reprint of the 1974 edition published by Oxford University Press
26. Nakagawa, K., Onuki, H.: QFESTA: Efficient Algorithms and Parameters for FESTA Using Quaternion Algebras. In: Reyzin, L., Stebila, D. (eds.) Advances in Cryptology – CRYPTO 2024. pp. 75–106. Springer Nature Switzerland, Cham (2024)
27. Nakagawa, K., Onuki, H.: SQIsign2DPush: Faster Signature Scheme Using 2-Dimensional Isogenies. Cryptology ePrint Archive, Paper 2025/897 (2025), `https://eprint.iacr.org/2025/897`
28. Nakagawa, K., Onuki, H., Castryck, W., Chen, M., Invernizzi, R., Lorenzon, G., Vercauteren, F.: SQIsign2D-East: A New Signature Scheme Using 2-Dimensional

Isogenies. In: Chung, K.M., Sasaki, Y. (eds.) Advances in Cryptology – ASIACRYPT 2024. pp. 272–303. Springer Nature Singapore, Singapore (2025)
29. Onuki, H., Nakagawa, K.: Ideal-to-Isogeny Algorithm Using 2-Dimensional Isogenies and Its Application to SQIsign. In: Chung, K.M., Sasaki, Y. (eds.) Advances in Cryptology – ASIACRYPT 2024. pp. 243–271. Springer Nature Singapore, Singapore (2025)
30. Page, A., Wesolowski, B.: The Supersingular Endomorphism Ring and One Endomorphism Problems are Equivalent. In: Joye, M., Leander, G. (eds.) Advances in Cryptology – EUROCRYPT 2024. pp. 388–417. Springer Nature Switzerland, Cham (2024)
31. Robert, D.: Breaking SIDH in polynomial time. In: Advances in Cryptology–EUROCRYPT 2023: 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23-27, 2023, Proceedings, Part V. pp. 472–503. Springer (2023)
32. Robert, D.: Fast pairings via biextensions and cubical arithmetic. Cryptology ePrint Archive, Paper 2024/517 (2024), https://eprint.iacr.org/2024/517
33. Silverman, J.H.: The Arithmetic of Elliptic Curves, 2nd Edition. Graduate Texts in Mathematics. Springer (2009)
34. Vélu, J.: Isogénies entre courbes elliptiques. C. R. Acad. Sci., Paris, Sér. A **273**, 238–241 (1971)
35. Voight, J.: Quaternion algebras. Springer Graduate Texts in Mathematics series. (2021)