WaterSQI and PRISMO: Quaternion Signatures for Supersingular Isogeny Group Actions

Tako Boris Fouotsa*

Department of Computer Science, University of Manchester, M13 9PL, UK
takoboris.fouotsa@manchester.ac.uk

Abstract. Isogeny group action based signatures are obtained from a sigma protocol with high soundness error, say $\frac{1}{2}$ for its most basic variant. One needs to independently repeat the sigma protocol $O(\lambda)$ times to reduce the soundness error to negligible (with λ being the security parameter). These repetitions come with a considerable efficiency and size overhead. On the other hand, quaternion isogeny-based signatures such as SQIsign and PRISM are directly obtained from a sigma protocol with a negligible soundness error. The secret key in SQIsign and PRISM is a random supersingular isogeny, and both schemes are insecure when the secret isogeny arises from the supersingular isogeny group action setting. In this paper, we propose WaterSQI and PRISMO, variants of SQIsign and PRISM respectively, suited for secret isogenies that arise from the supersingular isogeny group action setting. They use a sigma protocol whose soundness error is negligible without requiring parallel repetitions. They are hence more compact and $O(\lambda)$ times more efficient compared to Generalised CSI-FiSh (the generalisation of CSI-FiSh to large parameters using generic isogeny group action evaluation algorithms such as Clapotis/KLaPoTi/PEGASIS). For example, for our proof of concept implementation with a 2000 bits prime in Sagemath, PRISMO, when compared to Generalised CSI-FiSh with the same public key size, is about 80x faster for signing and 1457x faster for verification, while also being 29x more compact (signature size). Moreover, we prove that WaterSQI is a quantum proof of knowledge of the full endomorphism ring.

Keywords: Post-quantum cryptography · Generalised CSI-FiSh · SQIsign · SQI-FiSh · WaterSQI · PRISM · PRISMO

Note. This a major revision of [38,39]. The WaterSQI signature scheme was revisited and a new soundness proof was provided. In this new version, the primality requirement on the degree of the response isogeny is lifted. This leads to a more efficient signature scheme. The claim that WaterSQI is a proof of knowledge of the endomorphism ring was updated to "WaterSQI is a quantum proof of knowledge of the endomorphism ring", as there was a misinterpretation of prior works related to this claim in earlier versions.

* Part of this work was done while the author was affiliated with EPFL Lausanne, Switzerland.

1 Introduction

Peter Shor's quantum algorithm [61] theoretically breaks classical public key cryptography. In the recent years, new cryptographic protocols that are believed to be resistant to quantum adversaries have been proposed. The security of these protocols relies on new hard problems from lattices, codes, multivariate polynomials, isogenies, and many more. The most interesting point about isogeny based schemes is that they are very compact in general. One of their main disadvantage is that they are relatively slow. Designing more efficient variants of isogeny based protocols is an active research direction.

The isogeny-based cryptography zoo has several flagship schemes such as CSIDH [17] and CSI-Fish [9], SQISign [32,1], SIDH/SIKE [45,31,44], and many others. In 2022, SIDH was broken in polynomial time by the so-called SIDH attacks [16,48,60]. These attacks heavily exploit the torsion point information available in SIDH. This means that they do not extend to any other isogeny based scheme in which torsion point information is not provided. This is the case for schemes such as CSIDH and its derivatives, SQISign and its newest variants [6,28,36,53,54,23,64], and PRISM [4].

Supersingular isogeny group actions have become very popular in the last decade as they allow to design compact and efficient post-quantum protocols by instantiating schemes built from generic cryptographic group actions. Moreover, the rich properties of supersingular elliptic curves and isogenies (such as quadratic twists) enable some advanced construction techniques which are not possible with a generic generic cryptographic group action. For key exchange, we have CSIDH (Commutative Supersingular Isogeny Diffie-Hellman) [17]. Since its introduction in 2018, it has gained a lot of interest as it is the most compact and practically efficient post-quantum Non-Interactive Key Exchange. For digital signatures, we mainly have SeaSign [30] and CSI-Fish [9]. These two digital signatures are designed using the generic graph isomorphism identification protocol (or GMW [41]) instantiated with the supersingular isogeny group action. For this reason, they rely on a sigma protocol in which the cardinality of the challenge space has polynomial size: the cardinality of the challenge space is 2 for the most basic variant. This implies that for a given security parameter λ, one needs $O(\lambda)$ parallel repetitions in order to reduce the soundness error to negligible. This causes a great efficiency and signature size overhead. Moreover, CSI-FiSh [9], the most efficient one, makes use of the class group structure to evaluate the action of random ideals. The best classical algorithm for computing the class group structure has sub-exponential cost [42]. A record class group computation was done for a 512 bits prime, which was then used to instantiate CSI-FiSh. Several works [8,10,58] have argued that a 512 bits prime does not provide enough quantum security, and the use of several thousand bits primes is recommended [19]. Instantiating CSI-FiSh for those primes with thousands bits is out of reach. Building on OSIDH [22] (a generalisation of CSIDH), it has been proposed (SCALLOP [29], SCALLOP-HD [20], PEARL-SCALLOP [3]) to use isogeny group actions for which the class group and its structure are known or easy to compute by construction, but these techniques also come with some non

negligible efficiency overhead. Recently, Clapoti [56] and its more efficient variants KLaPoTi [57] and PEGASIS [26], polynomial time algorithms for evaluating ideals action on elliptic curves have been introduced. These class group evaluations algorithms can be used to instantiate a CSI-FiSh style signature, which we will call Generalised CSI-FiSh, with large primes without needing to compute the class group. The fact that Generalised CSI-FiSh also makes $O(\lambda)$ parallel repetition of the generic graph isomorphism identification protocol implies that there is some non negligible efficiency and signature size overhead.

As isogeny based signatures, besides CSI-FiSh and Seasign, we also have SQIsign [1,32] and PRISM [4]. SQIsign is a digital signature scheme whose design is inspired by the GPS [40] signature. Its security relies on the problem of computing a non trivial endomorphism of a random supersingular elliptic curve. More precisely, the SQISign signature scheme is obtained by applying the Fiat-Shamir transform to a sigma protocol for the relation

$$\mathcal{R} = \{(E, w), E/\mathbb{F}_{p^2} \text{ supersingular}, w \in \mathrm{End}(E) \setminus \mathbb{Z}\}.$$

In this identification protocol, a starting supersingular curve E_0 with known endomorphism ring $\mathcal{O}_0$ is fixed, the secret is an isogeny $\tau : E_0 \to E_A$. Note that the knowledge of τ is equivalent to the knowledge of $\mathrm{End}(E_A)$ which contains all the witnesses for E_A with respect to the relation $\mathcal{R}$. The commitment is a curve E_1 obtained by computing a random isogeny $\psi : E_0 \to E_1$. The challenge is a random isogeny $\varphi : E_A \to E_2$. The response consists of a random isogeny $\sigma : E_1 \to E_2$. Figure 1 illustrates this identification protocol.

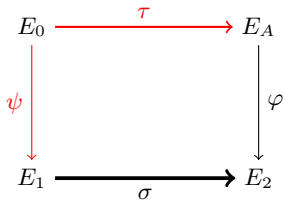

Fig. 1. The SQISign identification protocol.

PRISM [4] is a hash-and-sign type isogeny-based signature whose security relies on the problem of computing large prime degree isogenies from a supersingular elliptic curve E of unknown endomorphism ring. In the underlying identification protocol, the challenge is a large prime q and the response is an isogeny $\sigma : E \to E'$ of degree q. The problem of computing large prime degree isogenies from E is known to be hard, but the signer/prover can achieve this task efficiently using the secret which is the endomorphism ring of E.

One important fact about SQIsign and PRISM, in comparison to (Generalised) CSI-FiSh, is that the challenge space is of exponential size. This means that when Generalised CSI-FiSh on one hand, and SQIsign and PRISM on the

other hand are instantiated with primes p of similar size, SQIsign and PRISM are $O(\lambda)$ times faster and more compact compared to the Generalised CSI-FiSh. This leads us to the following question.

Can one instantiate SQIsign and PRISM with the secret isogeny $\tau : E_0 \to E_A$ arising from the supersingular isogeny group action?

From now on, we will be working with the action of the class group $\mathsf{cl}(\mathbb{Z}[\pi])$ (where π is the Frobenius endomorphism) on the set of supersingular elliptic curves defined over $\mathbb{F}_p$. All the results in this paper can be generalised (modulo minor technical adjustments) to any other (primitive) orientation on supersingular elliptic curves.

Paper contribution. In this paper we answer the question above in the affirmative by describing WaterSQI and PRISMO, variants of SQIsign and PRISM respectively, in which the secret keys are $\mathbb{F}_p$-rational isogenies.

Let us note that directly choosing the secret key in SQIsign as an $\mathbb{F}_p$-rational isogeny is not secure. This is because the hard relation in SQIsign asks to compute a non scalar endomorphism on the public key E_A and when the secret isogeny is $\mathbb{F}_p$-rational, E_A is defined over $\mathbb{F}_p$ and $\pi \in \mathrm{End}(E_A) \setminus \mathbb{Z}$ would be a witness for the relation $\mathcal{R}$. For this reason, WaterSQI uses the relation

$$\mathcal{R}_p = \{(E, w), E/\mathbb{F}_p \text{ supersingular}, w \in \mathrm{End}(E) \setminus \mathrm{End}_{\mathbb{F}_p}(E)\}$$

where $\mathrm{End}_{\mathbb{F}_p}(E)$ is the subring of $\mathrm{End}(E)$ containing all the endomorphisms of E defined over $\mathbb{F}_p$. The most difficult task is to come up with a design for which one can prove that the underlying sigma protocol is sound and honest verifier zero knowledge.

At a high level, in WaterSQI, the commitment isogeny $\psi : E_0 \to E_1$ is a random supersingular isogeny with E_1 not defined over $\mathbb{F}_p$. The challenge isogeny $\varphi : E_A \to E_2$ is an isogeny such that none of the subgroups of its kernel is fixed by the Frobenius. The response $\sigma : E_1 \to E_2$ is an isogeny of degree $d < \sqrt{p}$. Since we do not require d to be co-prime with the degree of the challenge isogeny, similarly to what is done in SQIsign [1,6], we increase the length of the challenge isogeny and allow the response isogeny to backtrack the challenge isogeny up to some extend. Under these restrictions, we prove that the resulting sigma protocol for the relation $\mathcal{R}_p$ is sound and honest verifier zero knowledge. We further propose a fast variant FastWaterSQI where the security assumptions rely on well understood heuristics. Moreover, as a direct application of the result of Chen and Petit [21], we show that WaterSQI is a quantum proof of knowledge of the full endomorphism ring of the curve E, as [21] provides a quantum algorithm that can be used to recover $\mathrm{End}(E)$ from $\mathbb{Z}[w, \pi]$ where $w \in \mathrm{End}(E) \setminus \mathrm{End}_{\mathbb{F}_p}(E)$ is the extracted witness. As a consequence, WaterSQI is a more efficient quantum proof of knowledge of an ideal $\mathfrak{a}$ such that $\mathfrak{a}E_0 = E$, subject to the endomorphism ring of E_0 being public. Since generating supersingular elliptic curves with unknown endomorphism ring is an open problem [11,50], then it is often the case that $\mathrm{End}(E_0)$ is public, except when E_0 was generated by another participant or a

third party. For instance, in a CSIDH based El-Gamal type encryption scheme, when a quantum proof of knowledge is admissible, WaterSQI is the better tool the sender could use to prove that they honestly generated the first component $E_1 = \mathfrak{b}E_0$ of the ciphertext $(E_1, \mathsf{m} \oplus H(j(\mathfrak{b}E_A)))$ where E_A is the public key of the receiver. This could for example be the case for the threshold isogeny group action encryption scheme Kea in PQarrots [2], if the protocol were to relax its security regime to accept a quantum proof of knowledge rather than a more expensive classical one such as Generalised CSI-FiSh or SQI-FiSh (discussed below).

In PRISM, if one uses a public key E which is defined over $\mathbb{F}_p$, then when the challenge q is a split prime in $\mathfrak{O} \simeq \mathbb{Z}[\pi]$, one can efficiently evaluate the two $\mathbb{F}_p$-rational q-isogenies using PEGASIS [26]. This implies that PRISM is not secure when the secret isogeny arises from the group action setting. In PRISMO, we restrict the challenge space to primes q which are inert in the orienting order $\mathfrak{O} \simeq \mathbb{Z}[\pi]$. This implies that the knowledge of the orientation is not helpful to an attacker trying to evaluate q-isogenies.

On our way, we also describe Generalised CSI-FiSh and SQI-FiSh. As highlighted earlier, instantiating CSI-FiSh with larger parameters that offer enough quantum security is out of reach. Generalised CSI-FiSh is the generalisation of CSI-FiSh to larger parameters where higher dimensional isogeny group action algorithms, such as PEGASIS, are used to evaluate the action of ideals.

Generalised CSI-FiSh is very close to a black box isogeny group actions signature, while the starting curve E_0 used in its instantiation is not a generic oriented supersingular elliptic curve. In fact, the endomorphism ring of E_0 is known. Since $\mathrm{End}(E_0)$ is known, one can replace all instances of the generic class group evaluation algorithm in key generation and signing by the (quaternion) ideal to isogeny algorithm Qlapoti. This change allows faster key generation and signing. We name this variant SQI-FiSh.

We propose a theoretical comparison of the designed signature schemes. PRISMO is the most compact and has the most efficient verification while Fast-WaterSQI has the most efficient signing algorithm. Table 5 provides a general comparison between the schemes, while Table 1 specialises Table 5 to the case where p is the 2031 bits prime $p_{2000} = 3 \cdot 17 \cdot 2^{2026} - 1$ and provides the runtimes of our Sagemath proof of concept implementation of PRISMO and Generalised CSI-FiSh (where qt-PEGASIS [27] is used).

Related work. A recent analysis [52] shows that the identification scheme PRISM-id may not meet the expected security guaranties. This analysis does not affect the PRISM signature. In a similar way, it also does not affect our PRISMO variant of the PRISM signature.
A more efficient variant qt-PEGASIS [27] of PEGASIS have recently appeared online. We have updated our proof of concept implementation of Generalised CSI-FiSh and the runtimes in Table 1 and Table 4.

Outline. In Section 2, we discuss isogeny representations, the Deuring correspondence, SQIsign and isogeny group action signatures. Moreover, we describe

Protocol			$p_{2000} = 3 \cdot 17 \cdot 2^{2026} - 1$				
				Type of isogeny			
	$\|\mathsf{pk}\|$	$\|\mathsf{sig}\|$		2	(2,2)	(2,2,2,2)	**Runtime**
PRISMO	256	608	KeyGen	-	2 026	-	11.087 s
			Sign	-	2 026	-	8.123 s
			Verify	-	256	-	0.442 s
FastWaterSQI	256	1 040	KeyGen	-	2 026	-	-
			Sign	640	1 038	-	-
			Verify	128	1 038	-	-
WaterSQI	256	1 040	KeyGen	-	2 026	-	-
			Sign	128	4 052	-	-
			Verify	128	1 038	-	-
Generalised CSI-FiSh $(2, 71, 15)$	256	18 040	KeyGen*	-	-	2 026	9.17 s
			Sign*	-	-	143 846	10.84 m
			Verify*	-	-	143 846	10.73 m
Generalised CSI-FiSh $(2^4, 23, 14)$	3 810	5 854	KeyGen*	-	-	30 390	2.29 m
			Sign*	-	-	46 598	3.52 m
			Verify*	-	-	46 598	3.48 m
SQI-FiSh $(2, 71, 15)$	254	18 040	KeyGen	-	2 026	-	-
			Sign	-	143 846	-	-
			Verify*	-	-	143 846	-
SQI-FiSh $(2^4, 23, 14)$	3 810	5 854	KeyGen	-	30 390	-	-
			Sign	-	46 598	-	-
			Verify*	-	-	46 598	-

Table 1. Key sizes (in bytes) and number of isogenies computed of each degree when the schemes are instantiated with the prime p_{2000}. The $*$ indicates that the estimate does not include a small and variable number of small degree isogenies that occur in the algorithm. The last column provides runtimes for our proof of concept implementation in Sagemath.

Generalised CSI-FiSh and SQI-FiSh, and detail techniques that will be used to generate the challenge isogeny in WaterSQI. In Section 3 and Section 4 we describe WaterSQI and FastWaterSQI respectively. In Section 5 we describe PRISMO, and in Section 6 we instantiate and compare the designed protocols: Generalised CSI-FiSh, SQI-FiSh, WaterSQI, FastWaterSQI and PRISMO.

2 Preliminaries

In this section, we briefly discuss isogeny representations, the Deuring correspondence, SQIsign and isogeny group action signatures. We also describe Generalised

CSI-FiSh and SQI-FiSh, and detail techniques that will be used to generate the challenge isogeny in WaterSQI.

2.1 Efficient isogeny representation from Kani's theorem

Informally, a *efficient representation* of a supersingular isogeny $\varphi : E \to E'$ is any string of polynomial size that allows to evaluate the isogeny φ on any point of E which is defined over a relatively small extension of $\mathbb{F}_{p^2}$. The most natural representation of a cyclic isogeny is its kernel generator, but this representation is only efficient when the degree of the isogeny is smooth and the kernel generator is defined over a relatively small extension of $\mathbb{F}_{p^2}$ as one can use the Vélu formulas [62] or the square root Vélu formulas [7] to compute the isogeny. A composition of smooth degree isogenies can be represented by concatenating the representations of its factors. When the degree of the isogeny is not smooth, the kernel representation is not efficient.

As an application of the attacks on SIDH, or of Kani's lemma [46] precisely, Robert [59] described an algorithm that embeds the non-smooth degree isogeny $\varphi : E \to E'$ into a higher dimensional smooth degree isogeny Φ in such a way that from the evaluation of Φ on torsion points, one can retrieve the evaluation of φ on torsion points. We describe the dimension 2 representation, which is the one used in PRISMO and WaterSQI.

Dimension 2 representation. Let $\phi : E_1 \to E_2$ be an isogeny of degree d and let $N > d$ be a smooth integer coprime to d such that $E_1[N]$ is defined over a small extension of $\mathbb{F}_{p^2}$. Let $c = N - a$ and let $\psi : E_1 \to E_3$ be any isogeny of degree c. Then we have the following commutative diagram:

$$\begin{array}{ccc} E_1 & \xrightarrow{\phi} & E_2 \\ \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \psi'} \\ E_3 & \xrightarrow[\phi']{} & E_4 \end{array}$$

The dimension 2 isogeny $\Psi : E_2 \times E_3 \to E_1 \times E_4$ given by $\Phi = \begin{pmatrix} \widehat{\phi} & \widehat{\psi} \\ -\psi' & \phi' \end{pmatrix}$, has kernel $\ker \Phi = \{(\phi(P), \psi(P)), P \in E_1[N]\}$ and degree $N = a + b$. Since Ψ has smooth degree and accessible kernel, it can be evaluated on points $(P, 0) \in E_2 \times E_3$ to obtain $(\widehat{\phi}(P), *)$, allowing to evaluate $\widehat{\phi}$ efficiently. In practice, one chooses N to be a power of two. This representation is used in SQIsign for the response isogeny σ. Note that the representation requires the knowledge of $\phi(E_1[N])$ and $\psi(E_1[N])$, but this is not an issue in SQIsign as the signer knows the endomorphism rings of the curves E_1 and E_2, hence they can generate this data using the Deuring correspondence which we describe in the next section.

2.2 The Deuring correspondence

Let p be a prime. Let $\mathbb{Q}_{p,\infty}$ denote the quaternion algebra ramified at p and ∞. We have $\mathbb{Q}_{p,\infty} = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$ where $i^2 = -q$, $j^2 = -p$, $k = ij = -ji$, with $q \in \mathbb{N}$ being a well chosen integer. Let E be a supersingular curve defined over $\mathbb{F}_{p^2}$, then the endomorphism ring of E is a maximal order in $\mathbb{Q}_{p,\infty}$. For example, when $p \equiv 3 \mod 4$, $q = 1$ and the elliptic curve $E_0 : y^2 = x^3 + x$ is supersingular. The endomorphism ring of E_0 is isomorphic to the maximal order $\mathcal{O}_0 = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}\frac{1+k}{2} + \mathbb{Z}\frac{i+j}{2}$. In this paper, we will be using a prime $p \equiv 3 \mod 4$ and the curve $E_0 : y^2 = x^3 + x$. The actual isomorphism from $\mathcal{O}_0$ to $\text{End}(E_0)$ is given by $i \mapsto \iota$ and $j \mapsto \pi$ where

$$\iota : (x, y) \mapsto (-x, \sqrt{-1}y) \quad \text{and} \quad \pi : (x, y) \mapsto (x^p, y^p).$$

There is a correspondence (Deuring correspondence [35]) between the world of supersingular elliptic curves (up to isomorphism and Galois conjugacy) and isogenies, and the world of maximal (quaternion) orders (up to conjugacy) and ideals. Going from the quaternion world to the geometric world is easy, while going from the geometric world to the quaternion world is hard since it is essentially the endomorphism ring computation problem for supersingular elliptic curves. Hence the correspondence can only be effective when we know the endomorphism rings of the supersingular elliptic curves in play. We briefly mention the two major algorithms which will be useful in the rest of this paper. We refer to [12,51] for further details.

Sampling a random isogeny of given degree from E_0 (KaniDoublePath). Let d be an odd integer, our aim is to generate a random isogeny $\phi : E_0 \to E$ of degree d. The technique described here was introduced in QFESTA [51]. One fixes an integer a such that $d(2^a - d) \gg p$ and the 2^a-torsion is accessible. On samples a random endomorphism $\theta \in \text{End}(E_0)$ of degree $d(2^a - d)$ and one evaluates $\theta(E_0[2^a])$. The endomorphism θ can be factored as $\theta = \psi \circ \phi$ where $\deg \phi = d$ and $\deg \psi = 2^a - d$, which implies that $\deg \phi + \deg \psi = 2^a$ and $\theta(E_0[2^a])$ is a valid representation of both ϕ and ψ. One uses the dimension 2 representation to represent ϕ. Moreover, the ideal representation of ϕ is $\mathcal{O}_0\langle \alpha_\theta, d \rangle$ where α_θ is the quaternion representation of θ.

From $\mathcal{O}_0$ left ideals to isogenies (Qlapoti). Given a left ideal J of $\mathcal{O}_0$, our aim is to compute the isogeny $\phi : E_0 \to E$ corresponding to the ideal J. We use the techniques described Qlapoti [12]. First, one replaces J with an equivalent ideal I of smallest norm n and writes I as $I = \mathcal{O}_0\langle \alpha, n \rangle$. One then solves for $\beta_k = \gamma_k \cdot n + \alpha$ ($k \in \{1, 2\}$) such that $\gamma_k \in \mathbb{Z}[i]$ and $n(\beta_1) + n(\beta_2) = 2^a \cdot n$ with $2^a \approx p$ and the 2^a-torsion being accessible. The elements β_k define ideals $I_k = I\overline{\beta_k}/n$ of norm $d_k = n(\beta_k)/n$ such that $d_1 + d_2 = 2^a$. Let $\phi_k : E_0 \to E$ be the isogeny corresponding to I_k, and let $\theta = \widehat{\phi_2} \circ \phi_1$. Then we can evaluate θ on the 2^a torsion using the knowledge of $\text{End}(E_0)$. Since $\deg \phi_1 + \deg \widehat{\phi_2} = d_1 + d_2 = 2^a$, then $\theta(E_0[2^a])$ is a valid representation of both ϕ_1 and ϕ_2, from which one deduces a representation of $\phi : E_0 \to E$ corresponding to J.

2.3 SQISign

SQISign [32,33] is a digital signature scheme whose design is inspired by the GPS [40] signature. Its security relies on the problem of computing a non trivial endomorphism of a random supersingular elliptic curve. In the identification scheme used in SQISign, a starting curve E_0 with known endomorphism ring $\mathcal{O}_0$ is fixed, the secret is an isogeny $\tau : E_0 \to E_A$. The commitment is a curve E_1 obtained by computing a random isogeny $\psi : E_0 \to E_1$. The challenge is a random isogeny $\varphi : E_A \to E_2$. The response consists of a random isogeny $\sigma : E_1 \to E_2$. Figure 1 illustrates this identification protocol.

The response computation heavily relies the Deuring correspondence [35] that allows the owner of the secret key to recover the endomorphism rings $\mathcal{O}_1$ and $\mathcal{O}_2$ of E_1 and E_2 respectively, and to compute a random isogeny $\sigma : E_1 \to E_2$. Computing the endomorphism rings $\mathcal{O}_1$ and $\mathcal{O}_2$ involves translating isogenies into ideals and computing the right order of these ideals. Sampling a random isogeny $\sigma : E_1 \to E_2$ from $\mathcal{O}_A$ and $\mathcal{O}_2$, involves computing the connecting ideal $I = I(\mathcal{O}_1, \mathcal{O}_2)$, solving for an equivalent ideal $J \sim I$ and translating the ideal J into an isogeny σ. In earlier versions, the response isogeny σ was required to be smooth. This requirement had several side effects such as the use of the computationally expensive KLPT [47] and the use of primes p which are the sum of smooth twins (which are difficult to generate [24,32,33,25,14]). Today, with the new higher dimensional isogeny representation [59] that arose from the SIDH attacks, this requirement has been lifted and further adjustments have been made. Instead of returning a random isogeny $E_1 \to E_2$ of large smooth degree, one returns a random short isogeny $\sigma : E_1 \to E_2$ of generic degree using the dimension 2 isogeny representation. With these changes, SQISign [1] now uses a prime of the form $p = 2^a \cdot f - 1$.

2.4 Supersingular isogeny group actions and Generalised CSI-FiSh

Let $p \equiv 3 \mod 4$ be a prime greater than 3, let E be a supersingular curve defined over $\mathbb{F}_p$, and let π be the Frobenius endomorphism of E. The $\mathbb{F}_p$-endomorphism ring $\mathrm{End}_{\mathbb{F}_p}(E) \simeq \mathfrak{O}$ of E is either $\mathbb{Z}[\pi]$ or $\mathbb{Z}[\frac{1+\pi}{2}]$ [34]. As in the ordinary case, the class group $\mathsf{cl}(\mathfrak{O})$ of $\mathfrak{O}$ acts freely and transitively on the set $\mathcal{E}_p(\mathfrak{O})$ of supersingular elliptic curves defined over $\mathbb{F}_p$ and having $\mathbb{F}_p$-endomorphism ring isomorphic to $\mathfrak{O}$ [17, Theorem 7].

In CSIDH [17], $\mathfrak{O} \simeq \mathbb{Z}[\pi]$ while in CSURF [15] $\mathfrak{O} \simeq \mathbb{Z}[\frac{1+\pi}{2}]$. This can be generalised [55] to OSIDH [22] where $\mathfrak{O}$ is a generic quadratic order and $\mathcal{E}_p(\mathfrak{O})$ is the set of supersingular curves primitively oriented by $\mathfrak{O}$. We will be working with the CSIDH setting but everything can be translated to OSIDH.

The main signature schemes in the isogeny group action setting are SeaSign [30] and CSI-FiSh [9]. SeaSign uses rejection sampling, and is slower compared to CSI-FiSh. CSI-FiSh makes extensive use of the class group structure of the order $\mathfrak{O}$. As explained in the introduction, the prime used in CSI-FiSh does not offer enough quantum security and scaling up CSI-FiSh to larger primes is out of reach

as algorithms for computing the class group structure have sub-exponential complexity. SCALLOP [29] and its variants [20,3] use large suborders $\mathfrak{O}$ of orders $\mathfrak{O}_0$ with computable class group such that the class group structure of $\mathfrak{O}$ can be easily deduced from that of $\mathfrak{O}_0$. Nevertheless, these constructions come with a high efficiency overhead.

In fact, CSI-FiSh, SCALLOP and variants use the class group structure because of the inexistence of polynomial time algorithms for evaluating the action of class group ideals of generic norm back in the days. Today, this has changed completely. Clapoti [56], KLaPoTi [57] and PEGASIS [26] allow us to efficiently evaluate the action of any class group ideal, meaning that for any prime p one can instantiate a graph isomorphism type sigma protocol and turn it into a digital signature. We call this signature Generalised CSI-FiSh.

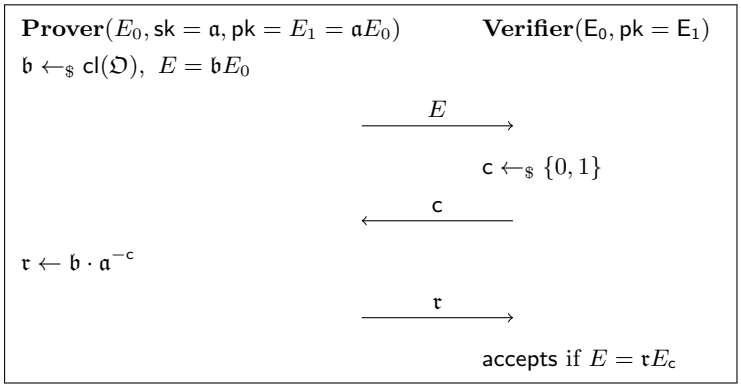

Fig. 2. Graph isomorphism type sigma protocol for isogeny group actions.

Generalised CSI-FiSh. At a high level, the graph isomorphism (or GMW [41]) type sigma protocol for isogeny group action which all existing isogeny group action signature rely on is described in Figure 2. In Generalised CSI-FiSh, the curves $\mathfrak{b}E_0$ and $\mathfrak{r}E_0$ are computed using any polynomial time algorithm for evaluating the action of random class group ideals, the most efficient one is PEGASIS. Since the soundness error of this sigma protocol is $1/2$, one needs λ parallel repetitions of the protocol to bring down the soundness error to $2^{-\lambda}$ and apply the Fiat-Shamir transform to obtain a digital signature scheme.

There are several techniques that can be used to optimise the resulting signature scheme, in such a way that $t \leq \lambda$ repetitions are sufficient to reach the desired security level while being more compact. The first one is to exploit the fact that the sigma protocol is commitment recoverable and return $(\mathfrak{r}_1, \ldots, \mathfrak{r}_t, \mathsf{c}_1, \ldots, \mathsf{c}_t)$ as the signature. The second technique is to use several public keys, say $S-1$, to reduce the soundness error of the basic sigma protocol in Figure 2 to $1/S$. Moreover, one can double the number of public keys for free

by also considering their quadratic twits. This brings down the soundness error to $(2S-1)^{-1}$ for the basic sigma protocol, which leads to a soundness error of $(2S-1)^{-t}$ when there are t parallel repetitions. As explained in [9, Section 6.1], using a (slow) hash function which is a factor of 2^k slower than a standard hash function, one can further improve on the soundness error and bring it down to $2^{-k}(2S-1)^{-t}$, hence reducing the number of repetitions t and the signature size. We refer to [9, Section 5.2] and [13] for further details regarding these optimisation techniques. Choosing the value of (S, t, k) allows some trade-off between signing/verification time, key generation time, public key size and signature size.

SQI-FiSh. The Generalised CSI-FiSh described above works with any starting curve E_0 which is primitively oriented by $\mathfrak{O}$. This means that the knowledge of the endomorphism ring of E_0 is not required. Nevertheless, in practice, the curve E_0 is the supersingular curve $E_0 : y^2 = x^3 + x$ whose endomorphism ring $\mathrm{End}(E_0)$ is known, or just any other curve with known endomorphism ring. In fact, generating supersingular elliptic curves with unknown endomorphism is an open research question [11,50], the only known solution being to rely on a trusted party or to use a secure multiparty [5,49]. It is hence reasonable to assume that the endomorphism ring of the starting curve is available.

In this case, one can replace all instances of the generic class group evaluation algorithm in the key generation and signing algorithms of Generalised CSI-FiSh by the (quaternion) ideal to isogeny algorithm. This change allows a faster key generation and signing as ideal to isogeny (Qlapoti) computes (2,2)-isogenies while PEGASIS computes (2,2,2,2)-isogenies. We name this variant SQI-FiSh. In SQI-FiSh, the key generation generation and the signing algorithms use Qlapoti to compute the public key curve $\mathfrak{a}E_0$ and the commitment curve $\mathfrak{b}E_0$, as $\mathrm{End}(E_0)$ is available. During verification, the verifier uses PEGASIS as usual.

Remark 1. One should note that even though we work on the floor of the $\mathbb{F}_p$ supersingular isogeny graph ($\mathfrak{O} \simeq \mathbb{Z}[\pi]$) in this paper, Generalised CSI-FiSh and SQI-FiSh are most efficient when instantiated on the surface ($\mathfrak{O} \simeq \mathbb{Z}[\frac{1+\pi}{2}]$) as this allows PEGASIS to fully run over $\mathbb{F}_p$. One could climb the volcano, run PEGASIS on the surface and descend with the solution to the floor, but it is just easier to work on the surface.

2.5 Generating isogenies ϕ such that 1_ϕ is not $\mathbb{F}_p$-rational

In our design of WaterSQI, we will need to generate isogenies ϕ that do not "trivially" factor through an $\mathbb{F}_p$-rational isogeny, meaning that no non-trivial subgroup of their kernel is fixed by the Frobenius. When $\phi = \phi_e \circ \cdots \circ \phi_1$ is cyclic and has prime power degree ℓ^e (with $\deg \phi_i = \ell$), this is equivalent to $1_\phi := \phi_1$ not being $\mathbb{F}_p$-rational. In the rest of this paper, if $\phi = \phi_e \circ \cdots \circ \phi_1$ is a cyclic isogeny of prime power degree ℓ^e, we use the notation 1_ϕ for its first component ϕ_1. In this section, we describe how to generate cyclic prime power degree isogenies ϕ such that 1_ϕ is not $\mathbb{F}_p$-rational.

We assume that $\ell \neq p$. When $\ell \neq 2$ is inert in $\mathfrak{O} \simeq \mathbb{Z}[\pi]$, then all ℓ-isogenies are not $\mathbb{F}_p$-rational and for any cyclic ℓ^e-isogeny ϕ, 1_ϕ is not $\mathbb{F}_p$-rational. When $\ell \neq 2$ splits in $\mathfrak{O} \simeq \mathbb{Z}[\pi]$, we have the following lemma.

Lemma 2. *Let E be a supersingular elliptic curve defined over $\mathbb{F}_p$. Let $\ell \neq 2$ be a prime that splits in $\mathfrak{O} \simeq \mathbb{Z}[\pi]$. Let $E[\ell^e] = \langle P, Q\rangle$ with $\pi(P) \in \langle P\rangle$ and $\pi(Q) \in \langle Q\rangle$. Then for any cyclic isogeny $\phi : E \to E/\langle P + [s]Q\rangle$ where $s \in \mathbb{Z}_{\ell^e}^\times$, 1_ϕ is not $\mathbb{F}_p$-rational.*

Proof. Let us assume for a moment that 1_ϕ is $\mathbb{F}_p$-rational. Then $\pi(\ker 1_\phi) = \ker 1_\phi$. Let $E[\ell] = \langle P', Q'\rangle$ where $P' = [\ell^{e-1}]P, Q' = [\ell^{e-1}]Q$, let $\pi(P') = [\alpha]P'$ and $\pi(Q') = [\beta]Q'$. Since ℓ splits in $\mathbb{Z}[\pi]$, then $\alpha \neq \beta$. We have $\pi(\ker 1_\phi) = \pi(P' + [s]Q') = [\alpha]P' + [s\beta]Q'$. Hence there exists u such that $[u](P' + [s]Q') = [\alpha]P' + [s\beta]Q'$, which implies that $u = \alpha$ and $us = s\beta$. Since $s \in \mathbb{Z}_{\ell^e}^\times$, then $\alpha = u = \beta$, which is a contradiction. □

When the degree of the isogeny to be generated is a power of 2, more care is needed. In fact, the $\mathbb{F}_p$ sub-graph has a two level volcano structure and the connectedness of the graph with respect to 2-isogenies depends on $p \mod 8$. We refer to [15,34] for further details regarding these graphs. In our case, $p \equiv 7 \mod 8$. Let 2^e be the largest power of 2 dividing $p + 1$. When E is on the surface, that is $\mathrm{End}_{\mathbb{F}_p}(E) = \mathbb{Z}[\frac{1+\pi}{2}]$, then $E(\mathbb{F}_p)[2^e] \simeq \mathbb{Z}_{2^{e-1}} \oplus \mathbb{Z}_2$ and there are three $\mathbb{F}_p$-rational 2-isogenies of domain E. When E is on the floor, that is $\mathrm{End}_{\mathbb{F}_p}(E) = \mathbb{Z}[\pi]$, then $E(\mathbb{F}_p)[2^e] \simeq \mathbb{Z}_{2^e}$ is cyclic and there is only one $\mathbb{F}_p$-rational 2-isogeny of domain E. The kernel generator of the later isogeny corresponds to $[2^{e-1}]Q$ where Q is any point such that $E(\mathbb{F}_p)[2^e] = \langle Q\rangle$. This implies that any cyclic isogeny $\phi : E \to E/\langle S\rangle$ of degree $2^{e'}$ where S and $[2^{e-e'}]Q$ are linearly independent is such that 1_ϕ is not $\mathbb{F}_p$-rational. To sample points S of order $2^{e'}$ that are linearly independent with $Q' = [2^{e-e'}]Q$, one can complete Q' to any basis (P', Q') of $E[2^{e'}]$, and sample S as $S = P' + [s]Q'$ where $s \in \mathbb{Z}_{2^{e'}}$. We hence deduce the following lemma.

Lemma 3. *Let E be a supersingular elliptic curve defined over $\mathbb{F}_p$ with $p \equiv 7 \mod 8$, such that $\mathrm{End}_{\mathbb{F}_p}(E) = \mathbb{Z}[\pi]$. Let $e \geq 3$ be an integer, let $E[2^e] = \langle P, Q\rangle$ with $E(\mathbb{F}_p)[2] = \langle [2^{e-1}]Q\rangle$. Then for any $s \in \mathbb{Z}_{2^{e'}}$ where $e' \leq e$, the isogeny $\phi : E \to E/\langle [2^{e-e'}](P + [s]Q)\rangle$ is such that 1_ϕ is not $\mathbb{F}_p$-rational.*

3 WaterSQI

We are now ready to describe the WaterSQI sigma protocol. Here we describe a conservative variant (WaterSQI) and in Section 4 we will describe a fast variant (FastWaterSQI). The main difference between the two is the way the commitment and the response are computed. In the conservative case, the (very long) commitment isogeny is generated in such a way that the commitment curve is statistically indistinguishable from a random supersingular curve while in the fast variant the commitment curve is computationally indistinguishable from a

random supersingular curve. This difference in the commitment generation has a huge effect on the response computation, which leads to the FastWaterSQI variant being more efficient.

For a secure design, we impose the following requirements which we motivate in Appendix A.

1. The commitment curve E_1 should not be defined over $\mathbb{F}_p$.
2. The degree of the challenge isogeny φ is 2^e where $a \geq e \geq \lambda$, and φ should not "trivially" factor through an $\mathbb{F}_p$-rational isogeny. The latter means that no non-trivial subgroup of $\ker \varphi$ should be fixed by the Frobenius, which is equivalent to 1_φ not being $\mathbb{F}_p$-rational.
3. The degree d of the response isogeny σ is bounded[1] by $\sqrt{p}$, and the response isogeny is allowed to backtrack the challenge isogeny by n_{bt} steps where $n_{\mathsf{bt}} < e - \lambda$ steps.

At a high level, in WaterSQI, the secret isogeny $\tau : E_0 \to E_A$ is $\mathbb{F}_p$-rational, the commitment isogeny $\psi : E_0 \to E_1$ is a random supersingular isogeny such that E_1 is not defined over $\mathbb{F}_p$. The challenge isogeny is a random non $\mathbb{F}_p$-rational 2^e-isogeny $\varphi : E_A \to E_2$ such that 1_φ is not $\mathbb{F}_p$-rational. The response is a random isogeny $\sigma : E_2 \to E_1$ of degree $d < \sqrt{p}$ such that $2^{e-\lambda+1}$ does not divide $\widehat{\varphi} \circ \sigma$. WaterSQI uses isogenies in dimension 1 and 2 only.

3.1 Public parameters, key generation, commitment and challenge

Public parameters. We use a prime of the form $p = 2^a \cdot f - 1$ where f is a small co-factor. The starting curve is $E_0 : y^2 = x^3 + x$ whose endomorphism ring $\mathrm{End}(E_0)$ is generated by $1, \iota, \frac{\iota+\pi}{2}, \frac{1+\iota\circ\pi}{2}$, and $\mathrm{End}(E_0)$ corresponds to the quaternion maximal order $\mathcal{O}_0$ generated by $1, i, \frac{i+j}{2}, \frac{1+k}{2}$ in $\mathbb{Q}_{p,\infty}$. The quadratic order used for our group action is $\mathfrak{O} \simeq \mathbb{Z}[\pi] \subset \mathrm{End}(E_0)$. Let $r = \lceil \log(\sqrt{p}) \rceil$, and let $e \in [\lambda, a - r]$ be an integer. The public parameters are $\mathsf{pp} = (p, a, r, e, E_0, \mathfrak{O}, \mathrm{End}(E_0) \simeq \mathcal{O}_0)$.

Key generation. The key generation in WaterSQI is very straightforward. In fact, it consists of a single class group evaluation. One samples a random integral ideal $\mathfrak{a}$ of $\mathfrak{O}$ and one uses the Qlapoti algorithm to compute the corresponding isogeny $\tau_\mathfrak{a} : E_0 \to E_A$. One evaluates $\tau_\mathfrak{a}$ on the 2^a torsion group. The public key is $\mathsf{pk} = E_A$ and the secret key is $\mathsf{sk} = (\mathfrak{a}, \tau_\mathfrak{a}(E_0[2^a]))$. This process is summarised in Algorithm 1.

Commitment. The commitment isogeny is a random isogeny $\psi : E_0 \to E_1$ which is generated as in SQIsign, except that one needs to double-check that E_1 is not be defined over $\mathbb{F}_p$. This is done by sampling a random left $\mathcal{O}_0$ ideal

[1] This bound is in fact the square root of the degree of the smallest non integer element in the orienting order (which in our case is $\mathbb{Z}[\pi]$). When considering curves on the surface where the orienting order is $\mathfrak{O} = \mathbb{Z}[\frac{\pi+1}{2}]$, this bound would be $\frac{1}{2}\sqrt{p+1}$.

Algorithm 1 Key generation

Require: $\mathsf{pp} = (p, a, r, e, E_0, \mathfrak{O}, \mathrm{End}(E_0) \simeq \mathcal{O}_0)$
Ensure: $\mathsf{sk} = (\mathfrak{a}, \tau_{\mathfrak{a}}(E_0[2^a]))$, $\mathsf{pk} = E_A$
1: Sample a random prime $\ell \gg |d_{\mathfrak{O}}|$ that splits in $\mathfrak{O}$ ▷ $d_{\mathfrak{O}}$ is the discriminant of $\mathfrak{O}$
2: Compute a square root μ of $-p$ modulo ℓ and set $\mathfrak{a} = (\ell, \pi - \mu)\mathfrak{O}$
3: Translate $\mathfrak{a}$ into an isogeny $\tau_{\mathfrak{a}} : E_0 \to E_A := \mathfrak{a}E_0$ using Qlapoti
4: Evaluate $\tau_{\mathfrak{a}}$ on the 2^a-torsion to obtain $\tau_{\mathfrak{a}}(E_0[2^a])$.
5: **return** $\mathsf{sk} = (\mathfrak{a}, \tau_{\mathfrak{a}}(E_0[2^a]))$, $\mathsf{pk} = E_A$

Algorithm 2 Commitment

Require: $\mathsf{pp} = (p, a, r, e, E_0, \mathfrak{O}, \mathrm{End}(E_0) \simeq \mathcal{O}_0)$
Ensure: $\mathsf{com}_{\mathsf{state}} = (I, \psi(E_0[2^a]))$, $\mathsf{com} = E_1$
1: Sample a random $\mathcal{O}_0$ ideal I of norm d_{com}
2: Translate I into an isogeny $\psi : E_0 \to E_1$ using Qlapoti
3: **if** $j(E_1) \in \mathbb{F}_p$ **then**
4: Go back to Step 1
5: Evaluate ψ on the 2^a-torsion to obtain $\psi(E_0[2^a])$
6: **return** $\mathsf{com}_{\mathsf{state}} = (I, \psi(E_0[2^a]))$, $\mathsf{com} = j(E_1)$

Algorithm 3 Challenge isogeny computation

Require: $\mathsf{pp} = (p, a, r, e, E_0, \mathfrak{O}, \mathrm{End}(E_0) \simeq \mathcal{O}_0)$, $\mathsf{pk} = E_A$, $\mathsf{chal} = c \in \mathbb{Z}/2^\lambda\mathbb{Z}$
Ensure: The challenge isogeny $\varphi : E_A \to E_2$ of degree 2^e
1: Canonically generate $\langle P_A, Q_A \rangle = E_A[2^e]$ such that $E_A(\mathbb{F}_p)[2] = \langle [2^{e-1}]Q_A \rangle$
2: Set $R = P_A + [c]Q_A$
3: Compute the isogeny $\varphi : E_A \to E_2 := E_A/\langle R \rangle$ whose kernel is generated by R
4: **return** $\varphi : E_A \to E_2$

I of large norm d_{com}, and translating I into an isogeny $\psi : E_0 \to E_1$ using the Qlapoti algorithm. If $j(E_1) \in \mathbb{F}_p$ (this happens with negligible probability), one samples a brand new ideal I. Moreover, the action of ψ on the 2^a-torsion is computed and kept secret. This process is summarised in Algorithm 2. Note the commitment is actually $j(E_1)$, but the signer maintains E_1 internally until they are done with the signing process.

Challenge. The challenge is a random scalar c sampled from $\mathbb{Z}/2^\lambda\mathbb{Z}$. The challenge isogeny is an isogeny $\varphi : E_A \to E_2$ of degree 2^e derived from the challenge c, and which is such that 1_φ is not $\mathbb{F}_p$-rational. To sample such an isogeny, one canonically generates a basis (P_A, Q_A) of $E_A[2^e]$ such that $E_A(\mathbb{F}_p)[2] = \langle [2^{e-1}]Q_A \rangle$, and sets $R = P_A + [c]Q_A$ as the generator of $\ker \varphi$. One computes $\varphi : E_A \to E_2$. Following Lemma 3, 1_φ is not $\mathbb{F}_p$-rational, which will be useful when proving soundness. The challenge isogeny computation is summarised in Algorithm 3.

3.2 Response and verification

Algorithm 4 Response

Require: $\mathsf{pp} = (p, a, r, e, E_0, \mathfrak{O}, \mathrm{End}(E_0) \simeq \mathcal{O}_0)$, $\mathsf{sk} = (\mathfrak{a}, \tau_{\mathfrak{a}}(E_0[2^a]))$, $\mathsf{pk} = E_A$, $\mathsf{com}_{\mathsf{state}} = (I, \psi(E_0[2^a]))$, $\mathsf{com} = j(E_1)$, $\mathsf{chal} = c$

Ensure: The response $\mathsf{resp} = (E_\delta, \sigma_{\mathsf{real}} \circ \widehat{\delta}(E_\delta[2^{r-n_{\mathsf{bt}}}]), d_0, n_{\mathsf{nbt}}, n_{\mathsf{bt}})$

//Translating the challenge isogeny into an ideal

Compute the kernel the challenge isogeny $\varphi : E_A \to E_2$ as described in Algorithm 3

Compute $\widehat{\tau_{\mathfrak{a}}}(\ker \varphi)$ and translate it into a left $\mathcal{O}_0$ ideal I

Compute the push-forward $I_\varphi = [\mathfrak{a}]_* I$ of I through $\mathfrak{a}$

//Sampling the ideal of the response isogeny

Compute the ideal $I = \overline{I_\psi}\mathfrak{a}I_\varphi$

Sample a uniformly random ideal $I_\sigma \sim I$ of norm $d = d_0 \cdot 2^n < \sqrt{p}$ with d_0 odd

Compute the largest integer $n_{\mathsf{bt}} \leq n$ such that $I_\varphi \cdot \overline{I_\sigma} \in n_{\mathsf{bt}}\mathcal{O}_A$, and set $n_{\mathsf{nbt}} = n - n_{\mathsf{bt}}$

if $e - n_{\mathsf{bt}} < \lambda$ **then**

  return $\perp$ ▷ The whole signing process is actually restarted

//Evaluating the response isogeny σ

Find $\gamma \in \mathcal{O}_0$ such that $\mathcal{O}_0\gamma = I_\psi I_\sigma \overline{I_\varphi}\overline{\mathfrak{a}}$

Compute $\theta(E_0[2^a])$ where $\theta \in \mathrm{End}(E_0)$ corresponds to $\gamma \in \mathcal{O}_0$.

Recover $\sigma(E_1[2^r]) = [2^{a-e-r}]\sigma(E_1[2^{a-e}]) = \frac{2^{a-e-r}}{d_{\mathsf{com}} \cdot \deg \tau}\varphi \circ \tau \circ \theta \circ \widehat{\psi}(E_1[2^a])$

Write $\sigma = \sigma_{\mathsf{bt}} \circ \sigma_{\mathsf{real}}$, and recover $\sigma_{\mathsf{real}}(E_1[2^{r-n_{\mathsf{bt}}}])$ from $\sigma(E_1[2^r])$.

//Generating the auxiliary isogeny and computing the response

Sample a random $\mathcal{O}_0$ left ideal I_δ of norm $2^{r-n} - d_0$

Compute the ideal $J = I_\psi \cap I_\delta$

Translate J into its corresponding isogeny $\delta \circ \psi : E_0 \to E_\delta$ using Qlapoti

Recover $\delta(E_2[2^{r-n_{\mathsf{bt}}}])$ from $\psi(E_0[2^r])$ and $\delta \circ \psi(E_0[2^r])$

Deduce $\sigma_{\mathsf{real}} \circ \widehat{\delta}(E_\delta[2^{r-n_{\mathsf{bt}}}])$ from $\delta(E_2[2^{r-n_{\mathsf{bt}}}])$ and $\sigma_{\mathsf{real}}(E_1[2^{r-n_{\mathsf{bt}}}])$

return $\mathsf{resp} = (E_\delta, \sigma_{\mathsf{real}} \circ \widehat{\delta}(E_\delta[2^{r-n_{\mathsf{bt}}}]), d_0, n_{\mathsf{nbt}}, n_{\mathsf{bt}})$

Response. The response algorithm follows several steps which are detailed bellow.

1. Compute the ideal I_φ corresponding to the challenge isogeny $\varphi : E_A \to E_2$. This is achieved by mapping $\ker \varphi$ to E_0 through $\widehat{\tau_{\mathfrak{a}}}$, translating $\widehat{\tau_{\mathfrak{a}}}(\ker \varphi)$ into an ideal and computing the pushforward of this ideal through $\mathfrak{a}$ to obtain I_φ.
2. Recover the ideal $I := \overline{I_\psi}\mathfrak{a}I_\varphi$. Sample a uniformly random ideal $I_\sigma \sim I$ of norm $d < \sqrt{p}$ and compute n such that $d = d_0 \cdot 2^n$ with d_0 odd. This means that σ contains a 2^n-isogeny. Determine the largest integer $n_{\mathsf{bt}} \leq n$ such that $\widehat{\sigma}$ backtracks φ by n_{bt} steps, that is $I_\varphi \cdot \overline{I_\sigma} \subseteq n_{\mathsf{bt}}\mathcal{O}_A$. If $e - n_{\mathsf{bt}} < \lambda$ one aborts and restarts the whole signing process with a new commitment isogeny. One then sets $n_{\mathsf{nbt}} = n - n_{\mathsf{bt}}$. The ideal I_σ corresponds to the response isogeny $\sigma : E_1 \to E_2$, which factors as $\sigma = \sigma_{\mathsf{bt}} \circ \sigma_{\mathsf{nbt}} \circ \sigma_{\mathsf{odd}}$ where $\sigma_{\mathsf{odd}} : E_1 \to E_{\mathsf{odd}}$, $\sigma_{\mathsf{nbt}} : E_{\mathsf{odd}} \to E_{\mathsf{nbt}}$ and $\sigma_{\mathsf{bt}} : E_{\mathsf{nbt}} \to E_2$ have degree d_0, $2^{n_{\mathsf{nbt}}}$ and $2^{n_{\mathsf{bt}}}$ respectively. The real response which is returned to the verifier $\sigma_{\mathsf{real}} = \sigma_{\mathsf{nbt}} \circ \sigma_{\mathsf{odd}}$, as the remaining part is contained in the challenge isogeny φ which one can factor as $\varphi = \sigma_{\mathsf{bt}} \circ \varphi_{\mathsf{nbt}}$.

3. Recover the endomorphism $\theta = \widehat{\tau} \circ \widehat{\varphi} \circ \sigma \circ \psi \in \mathrm{End}(E_0)$ from the principal ideal $I_\psi I_\sigma \overline{I_\varphi} \mathfrak{a}$ of $\mathcal{O}_0$. Evaluate $\theta(E_0[2^a])$ and use it to recover $\sigma(E_1[2^{a-e}])$ as $[2^e \cdot d_{\mathsf{com}} \cdot \deg \tau]\sigma = \varphi \circ \tau \circ \theta \circ \widehat{\psi}$ and $\deg \psi \cdot \deg \tau$ is odd. Deduce $\sigma(E_1[2^r])$ (note that $r \leq a - e$), then $\sigma_{\mathsf{real}}(E_1[2^{r-n_{\mathsf{bt}}}])$.
4. Now we need to generate an auxiliary isogeny $\delta : E_1 \to E_\delta$ of degree $2^{r-n} - d_0$ and use it to represent the odd part $\sigma_{\mathsf{odd}} : E_1 \to E_{\mathsf{odd}}$ of our response isogeny in dimension 2. One proceeds as follows. Sample a random $\mathcal{O}_0$ left ideal I_δ of norm $2^{r-n} - d_0$. Translate the ideal $I_\psi \cap I_\delta$ into the isogeny $\delta \circ \psi : E_0 \to E_\delta$ using Qlapoti. Recover $\delta(E_1[2^{r-n_{\mathsf{bt}}}])$ from $\psi(E_0[2^r])$ and $\delta \circ \psi(E_0[2^r])$, and deduce $\widehat{\delta}(E_\delta[2^{r-n_{\mathsf{bt}}}])$.
5. Finally, we compose the evaluations $\widehat{\delta}(E_\delta[2^{r-n_{\mathsf{bt}}}])$ and $\sigma_{\mathsf{real}}(E_1[2^{r-n_{\mathsf{bt}}}])$ to obtain $\sigma_{\mathsf{real}} \circ \widehat{\delta}(E_\delta[2^{r-n_{\mathsf{bt}}}])$. The response is $(E_\delta, \sigma_{\mathsf{real}} \circ \widehat{\delta}(E_\delta[2^{r-n_{\mathsf{bt}}}]), d_0, n_{\mathsf{nbt}}, n_{\mathsf{bt}})$. The response process is summarised in Algorithm 4 and is depicted in Figure 3 which is similar to that of SQIsign [6, Figure 2].

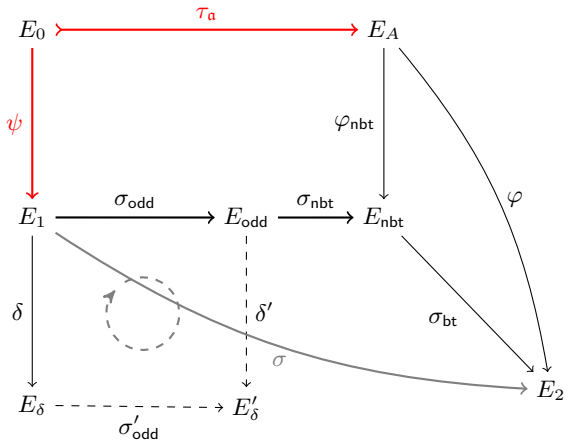

Fig. 3. WaterSQI response diagram

Remark 4 (On the sizes of e). Once the commitment curve E_1 and the challenge curve E_2 are fixed, there exists [28, Lemma 12] an isogeny of degree at most $2\sqrt{2p}/\pi = 0.9003 \cdot \sqrt{p}$ between them. Under the heuristic that the degrees of isogenies between the two curves are distributed like random numbers, the probability that the degree d of a random isogeny $\sigma : E_1 \to E_2$ is divisible by 2^n is roughly 2^{-n}. Moreover, factoring σ as $\sigma = \sigma_{\mathsf{even}} \circ \sigma_{\mathsf{odd}}$ where $\deg(\sigma_{\mathsf{even}}) = 2^n$ and $\deg(\sigma_{\mathsf{odd}}) = d_0$ is odd, the probability that σ_{even} backtracks φ by exactly n_{bt} steps is roughly $\frac{1}{3 \cdot 2^{n_{\mathsf{bt}}-1}} \sim 2^{-n_{\mathsf{bt}}}$. Hence for a given integer n_{bt}, heuristically, when sampling a uniformly random response isogeny σ in Algorithm 4, the probability that d is divisible by $2^{n_{\mathsf{bt}}}$ and σ_{even} backtracks φ by at least n_{bt} steps is

Algorithm 5 Verify

Require: $\mathsf{pp} = (p, a, r, e, E_0, \mathfrak{O}, \mathrm{End}(E_0) \simeq \mathcal{O}_0)$, $\mathsf{pk} = E_A/\mathbb{F}_p$, $\mathsf{com} = j(E_1)$, $\mathsf{chal} = c$, $\mathsf{resp} = (E_\delta, \sigma_{\mathsf{real}} \circ \widehat{\delta}(E_\delta[2^{r-n_{\mathsf{bt}}}]), d_0, n_{\mathsf{nbt}}, n_{\mathsf{bt}})$

Ensure: Accept or Reject

1: Set $n = n_{\mathsf{bt}} + n_{\mathsf{nbt}}$
2: **if** $\frac{\pi+1}{2} \in \mathrm{End}(E_A)$ *or* d_0 is even *or* $e - \lambda < n_{\mathsf{bt}}$ *or* $\sqrt{p} \leq d_0 \cdot 2^n$ **then**
3: **return** Reject
4: Use Algorithm 3 to compute $\varphi_{\mathsf{nbt}} : E_A \to E_{\mathsf{bt}}$ of degree $2^{e-n_{\mathsf{bt}}}$ such that $\varphi = \sigma_{\mathsf{bt}} \circ \varphi_{\mathsf{nbt}}$
5: Recover $P_{\mathsf{nbt}} = \sigma_{\mathsf{real}} \circ \widehat{\delta}(P_\delta)$ and $Q_{\mathsf{nbt}} = \sigma_{\mathsf{real}} \circ \widehat{\delta}(Q_\delta)$
6: **if** $\{P_{\mathsf{nbt}}, Q_{\mathsf{nbt}}\} \not\subset E_{\mathsf{nbt}}$ *or* $\langle [2^{r-n}]P_{\mathsf{nbt}}, [2^{r-n}]Q_{\mathsf{nbt}} \rangle$ is not a cyclic group of order $2^{n_{\mathsf{nbt}}}$ **then**
7: **return** Reject
8: Compute the isogeny of kernel $\langle [2^{r-n}]P_{\mathsf{nbt}}, [2^{r-n}]Q_{\mathsf{nbt}} \rangle$, the dual of $\sigma_{\mathsf{nbt}} : E_{\mathsf{odd}} \to E_{\mathsf{nbt}}$
9: Recover $P_{\mathsf{odd}} = \widehat{\sigma_{\mathsf{nbt}}}(P_{\mathsf{nbt}})$, $Q_{\mathsf{odd}} = \widehat{\sigma_{\mathsf{nbt}}}(Q_{\mathsf{nbt}})$
10: Canonically generate a basis (P'_δ, Q'_δ) of $E_\delta[2^{r-n_{\mathsf{bt}}}]$
11: Compute $(P_\delta, Q_\delta) = ([2^{n_{\mathsf{nbt}}}]P'_\delta, [2^{n_{\mathsf{nbt}}}]Q'_\delta)$
12: Compute the isogeny $\Psi : E_\delta \times E_{\mathsf{nbt}} \to F_1 \times F_2$ of kernel $\langle ([d_0]P_\delta, P_{\mathsf{odd}}), ([d_0]Q_\delta, Q_{\mathsf{odd}}) \rangle$
13: **if** the computation of Ψ fails **or** $F_1 \not\cong E_1$ **then**
14: **return** Reject
15: Compute $(P', -) = \Psi(0, P_{\mathsf{odd}})$ and $(Q', -) = \Psi(0, Q_{\mathsf{odd}})$
16: **if** $e_{2^{r-n}}(P', Q') = e_{2^{r-n}}(P_{\mathsf{odd}}, Q_{\mathsf{odd}})^{d_0}$ **then**
17: **return** Accept
18: **return** Reject

bounded by $2^{-2n_{\mathsf{bt}}}$. Since we allow n_{bt} to be up to $e - \lambda$, then the response algorithm aborts in step 8 with a probability bounded by $2^{-2(e-\lambda)}$, which one can choose to be as small as possible by increasing e. In WaterSQI, we set $e = \frac{3}{2}\lambda$ so that the probability that d is divisible by $2^{e-\lambda} = 2^{\lambda/2}$ and $\widehat{\sigma_{\mathsf{even}}}$ backtracks φ by at least $\lambda/2$ steps is bounded by $2^{-\lambda}$ which is negligible. In the faster variant FastWaterSQI, we set $e = \frac{5}{4}\lambda$, leading to step 8 triggering a restart of the signing process with a probability bounded by $2^{-\lambda/2}$.

Verification. Given the public key $\mathsf{pk} = E_A/\mathbb{F}_p$, the commitment $\mathsf{com} = j(E_1)$, the challenge $\mathsf{chal} = c$ and the response $(E_\delta, \sigma_{\mathsf{real}} \circ \widehat{\delta}(E_\delta[2^{r-n_{\mathsf{bt}}}]), d_0, n_{\mathsf{nbt}}, n_{\mathsf{bt}})$, one first checks that d_0 is odd, $\lambda \leq e - n_{\mathsf{bt}}$ and $d_0 \cdot 2^n < \sqrt{p}$ where $n = n_{\mathsf{nbt}} + n_{\mathsf{bt}}$. One also checks that $\frac{\pi+1}{2} \notin \mathrm{End}(E_A)$, which ensures that the orienting order is $\mathfrak{O} = \mathbb{Z}[\pi]$ and the bound $\sqrt{p}$ on the degree of the response is the right one. One then computes the part $\varphi_{\mathsf{nbt}} : E_A \to E_{\mathsf{nbt}}$ of the challenge isogeny $\varphi : E_A \to E_2$ which is not backtracked by the dual of the response isogeny to recover E_{bt}. Note that $2^\lambda \leq \deg(\varphi_{\mathsf{nbt}})$ as $\lambda \leq e - n_{\mathsf{bt}}$, hence ensuring at least λ bits of entropy in the "real" challenge isogeny φ_{nbt}. Since $\sigma_{\mathsf{real}} \circ \widehat{\delta}$ is an isogeny of degree $(2^{r-n} - d_0) \cdot d_0 \cdot 2^{n_{\mathsf{nbt}}}$, then $\langle [2^{r-n}]P_{\mathsf{bt}}, [2^{r-n}]Q_{\mathsf{bt}} \rangle$ where $P_{\mathsf{nbt}} = \sigma_{\mathsf{real}} \circ \widehat{\delta}(P_\delta)$ and $Q_{\mathsf{nbt}} = \sigma_{\mathsf{real}} \circ \widehat{\delta}(Q_\delta)$ should be a cyclic group of order $2^{n_{\mathsf{nbt}}}$. If this is not the case,

one rejects the signature. One computes the dual $\widehat{\sigma_{\mathsf{nbt}}}$ of $\sigma_{\mathsf{nbt}} : E_{\mathsf{odd}} \to E_{\mathsf{nbt}}$, whose kernel is $\langle [2^{r-n}]P_{\mathsf{nbt}}, [2^{r-n}]Q_{\mathsf{nbt}} \rangle$. One recovers $P_{\mathsf{odd}} = \widehat{\sigma_{\mathsf{nbt}}}(P_{\mathsf{nbt}})$, $Q_{\mathsf{odd}} = \widehat{\sigma_{\mathsf{nbt}}}(Q_{\mathsf{nbt}})$. One canonically generates a basis (P_δ, Q_δ) of $E_\delta[2^{r-n_{\mathsf{bt}}}]$ and compute $(P'_\delta, Q'_\delta) = ([2^{n_{\mathsf{nbt}}}]P_\delta, [2^{n_{\mathsf{nbt}}}]Q_\delta)$. Since $P_{\mathsf{nbt}} = \sigma_{\mathsf{real}} \circ \widehat{\delta}(P_\delta)$, $Q_{\mathsf{nbt}} = \sigma_{\mathsf{real}} \circ \widehat{\delta}(Q_\delta)$ and $\sigma_{\mathsf{real}} = \sigma_{\mathsf{nbt}} \circ \sigma_{\mathsf{odd}}$, then $P_{\mathsf{odd}} = \sigma_{\mathsf{odd}} \circ \widehat{\delta}(P'_\delta)$ and $Q_{\mathsf{odd}} = \sigma_{\mathsf{odd}} \circ \widehat{\delta}(Q'_\delta)$. One computes the dimension 2 isogeny

$$\Psi = \begin{pmatrix} \widehat{\delta} & -\widehat{\sigma_{\mathsf{odd}}} \\ \sigma'_{\mathsf{odd}} & \delta' \end{pmatrix} : E_\delta \times E_{\mathsf{nbt}} \to F_1 \times F_2$$

of kernel $\{([d_0]S, \sigma_{\mathsf{odd}} \circ \widehat{\delta}(S)), S \in E_\delta[2^{r-n}]\}$. By definition, the codomain Ψ should be (isomorphic to) $E_1 \times E_{\delta'}$. If the computation of Ψ fails or F_1 is not isomorphic to E_1 one rejects the response. One then computes $(P', -) = \Psi(0, P_{\mathsf{odd}})$ and $(Q', -) = \Psi(0, \mathsf{odd})$ and checks that $e_{2^{r-n}}(P', Q') = e_{2^{r-n}}(P_{\mathsf{odd}}, Q_{\mathsf{odd}})^{d_0}$. This check confirms that the degree of σ_{odd} is d_0, which implies that the degree of σ is $d = d_0 \cdot 2^n$. The verification process is summarised in Algorithm 5.

3.3 The WaterSQI signature algorithm

We prove that the WaterSQI identification protocol is in fact Σ-protocol by showing that it is 2-special sound and honest-verifier zero knowledge. We then apply the Fiat-Shamir transform to obtain a digital signature scheme which is Existentially UnForgeable under Chosen Message Attacks (EUF-CMA) in the Random Oracle model, under Assumption 10. Note that the WaterSQI Σ-protocol, similarly to the SQIsign2D-West one, is commitment recoverable. In fact the signature contains the challenge and the response. During verification, the verifier recovers the commitment from the signature, and verifies that the commitment, the challenge and the response form a valid transcript.

Soundness. We consider the language

$$\{(E_A, \alpha) \mid \alpha \in \mathrm{End}(E_A) \setminus \mathrm{End}_{\mathbb{F}_p}(E_A),\ E_A/\mathbb{F}_p\}$$

which translates to the One Non-rational Endomorphism problem (Problem 5) for supersingular curves defined over $\mathbb{F}_p$.

Problem 5. Let E be a supersingular elliptic curve defined over $\mathbb{F}_p$. Compute an endomorphism α of E such that $\alpha \in \mathrm{End}(E) \setminus \mathrm{End}_{\mathbb{F}_p}(E)$.

In order to prove 2-special soundness with respect to the language above, we need to design an extractor which extracts a non $\mathbb{F}_p$-rational endomorphism of E_A from two valid transcripts with the same commitment but different challenges.

Proposition 6. *Given two valid WaterSQI transcripts sharing the same commitment but with different challenges, one can efficiently extract an efficient representation of a non $\mathbb{F}_p$-rational endomorphism $\alpha \in \mathrm{End}(E_A) \setminus \mathrm{End}_{\mathbb{F}_p}(E_A)$.*

Proof. Let E_1 be the common commitment curve (up to isomorphism) in both transcripts, and let (φ, resp) and $(\varphi', \mathsf{resp}')$ be the challenge and response of the two transcripts, with $\ker\varphi \neq \ker\varphi'$. Let $\sigma : E_1 \to E_2$ of degree $d = d_0 \cdot 2^{n_{\mathsf{nbt}}+n_{\mathsf{bt}}} < \sqrt{p}$ and $\sigma' : E_1 \to E_2'$ of degree $d' = d_0' \cdot 2^{n'_{\mathsf{nbt}}+n'_{\mathsf{bt}}} < \sqrt{p}$ be the two corresponding response isogenies where $\varphi : E_A \to E_2$ and $\varphi' : E_A \to E_2'$ have degree 2^e, and $c, c' \in \mathbb{Z}/2^\lambda\mathbb{Z}$ are the (scalar) challenges used to generate φ and φ'. From Figure 3, these two responses allow us to derive a representation of the endomorphism $\alpha_0 = \widehat{\varphi'_{\mathsf{nbt}}} \circ \sigma'_{\mathsf{nbt}} \circ \sigma'_{\mathsf{odd}} \circ \widehat{\sigma_{\mathsf{odd}}} \circ \widehat{\sigma_{\mathsf{nbt}}} \circ \varphi_{\mathsf{nbt}} \in \mathrm{End}(E_A)$ where the parts of the responses that backtrack the respective challenges have been removed. Let $\alpha \in \mathrm{End}(E_A)$ be the cyclic component of α_0. We will split the proof into two cases: $\sigma'_{\mathsf{odd}} \circ \widehat{\sigma_{\mathsf{odd}}} \in \mathbb{Z}$ and $\sigma'_{\mathsf{odd}} \circ \widehat{\sigma_{\mathsf{odd}}} \notin \mathbb{Z}$.

Case 1 : $\sigma'_{\mathsf{odd}} \circ \widehat{\sigma_{\mathsf{odd}}} \in \mathbb{Z}$. If $\sigma'_{\mathsf{odd}} \circ \widehat{\sigma_{\mathsf{odd}}} \in \mathbb{Z}$, then since σ_{odd} and σ'_{odd} are cyclic, we must have $\sigma' \circ \widehat{\sigma} = [d_0]$ and $d_0 = d_0'$. This implies that $\alpha \in \mathrm{End}(E_A)$ is in fact the cyclic component of $\alpha_0 = [d_0]\widehat{\varphi'_{\mathsf{nbt}}} \circ \sigma'_{\mathsf{nbt}} \circ \widehat{\sigma_{\mathsf{nbt}}} \circ \varphi_{\mathsf{nbt}}$. We claim that $\widehat{\varphi'_{\mathsf{nbt}}} \circ \sigma'_{\mathsf{nbt}} \circ \widehat{\sigma_{\mathsf{nbt}}} \circ \varphi_{\mathsf{nbt}} \notin \mathbb{Z}$. In fact, if it were a scalar, then since $\widehat{\sigma_{\mathsf{nbt}}} \circ \varphi_{\mathsf{nbt}}$ and $\widehat{\sigma'_{\mathsf{nbt}}} \circ \varphi'_{\mathsf{nbt}}$ are cyclic isogenies of degree $2^{e-n_{\mathsf{bt}}+n_{\mathsf{nbt}}}$ and $2^{e-n'_{\mathsf{bt}}+n'_{\mathsf{nbt}}}$ respectively, we would have that $e-n_{\mathsf{bt}}+n_{\mathsf{nbt}} = e-n'_{\mathsf{bt}}+n'_{\mathsf{nbt}}$ and $\ker(\widehat{\sigma_{\mathsf{nbt}}} \circ \varphi_{\mathsf{nbt}}) = \ker(\widehat{\sigma'_{\mathsf{nbt}}} \circ \varphi'_{\mathsf{nbt}})$. Since $\lambda \leq e - n_{\mathsf{bt}} \leq e - n_{\mathsf{bt}} + n_{\mathsf{nbt}}$, then

$$\begin{aligned}\ker(\varphi) \cap E_A[2^\lambda] &= \ker(\widehat{\sigma_{\mathsf{nbt}}} \circ \varphi_{\mathsf{nbt}}) \cap E_A[2^\lambda] \\ &= \ker(\widehat{\sigma'_{\mathsf{nbt}}} \circ \varphi'_{\mathsf{nbt}}) \cap E_A[2^\lambda] \\ &= \ker(\varphi') \cap E_A[2^\lambda].\end{aligned}$$

Let $\langle P_A, Q_A\rangle = E_A[2^e]$ as in Algorithm 3. Then $\langle 2^{e-\lambda}P_A, 2^{e-\lambda}Q_A\rangle = E_A[2^\lambda]$ and

$$\begin{aligned}\langle [2^{e-\lambda}]P_A + [c][2^{e-\lambda}]Q_A)\rangle &= \ker(\varphi) \cap E_A[2^\lambda] \\ &= \ker(\varphi') \cap E_A[2^\lambda] \\ &= \langle [2^{e-\lambda}]P_A + [c'][2^{e-\lambda}]Q_A)\rangle,\end{aligned}$$

implying that $c = c'$ and $\ker\varphi = \ker\varphi'$, which is a contradiction.

Hence $\widehat{\varphi'_{\mathsf{nbt}}} \circ \sigma'_{\mathsf{nbt}} \circ \widehat{\sigma_{\mathsf{nbt}}} \circ \varphi_{\mathsf{nbt}} \notin \mathbb{Z}$. It follows that $\alpha \notin \mathbb{Z}$, its degree is 2^b for some integer $b > 0$, and $\alpha_0 = [2^{e'}d_0]\alpha$ where $e' = \frac{2e-n_{\mathsf{bt}}+n_{\mathsf{nbt}}-n'_{\mathsf{bt}}+n'_{\mathsf{nbt}}-b}{2}$. WLOG, let us assume that $e - n'_{\mathsf{bt}} + n'_{\mathsf{nbt}} \leq e - n_{\mathsf{bt}} + n_{\mathsf{nbt}}$. Then $e' < e - n_{\mathsf{bt}} + n_{\mathsf{nbt}}$. Let $\ker(\widehat{\sigma_{\mathsf{nbt}}} \circ \varphi_{\mathsf{nbt}}) = \langle S\rangle$. Then $\alpha_0(S) = 0$, implying that $[2^{e'}]\alpha(S) = 0$ (because d_0 is odd), that is $[2^{e'}]S \in \ker\alpha$. Since S has order $2^{e-n_{\mathsf{bt}}+n_{\mathsf{nbt}}}$ and $b' = e - n_{\mathsf{bt}} + n_{\mathsf{nbt}} - e' > 0$, then $[2^{e'}]S \in E_A[2^{b'}] \cap \ker\alpha$. Since $\ker\alpha$ is a cyclic group whose order is a power of 2, then it admits a unique subgroup of order $2^{b'}$, which is in fact $\langle [2^{e'}]S\rangle$. Hence

$$\ker 1_\alpha = [2^{b'-1}]\langle [2^{e'}]S\rangle = \langle [2^{e-n_{\mathsf{bt}}+n_{\mathsf{nbt}}-1}]S\rangle = \ker 1_{\widehat{\sigma_{\mathsf{nbt}}}\circ\varphi_{\mathsf{nbt}}} = \ker 1_\varphi. \quad (1)$$

Since 1_φ is not $\mathbb{F}_p$-rational, then 1_α is not $\mathbb{F}_p$-rational as well, which implies that α is not $\mathbb{F}_p$-rational. Hence $\alpha \in \mathrm{End}(E_A) \setminus \mathrm{End}_{\mathbb{F}_p}(E_A)$.

Case 2 : $\sigma'_{\mathsf{odd}} \circ \widehat{\sigma_{\mathsf{odd}}} \notin \mathbb{Z}$. Now let us assume that $\sigma'_{\mathsf{odd}} \circ \widehat{\sigma_{\mathsf{odd}}} \notin \mathbb{Z}$. Consider the commutative diagram in Figure 4 and rewrite $\alpha_0 = \sigma'^*_{\mathsf{odd}} \circ \widehat{\sigma^*_{\mathsf{odd}}} \circ \widehat{\varphi'^*_{\mathsf{nbt}}} \circ \sigma'^*_{\mathsf{nbt}} \circ \widehat{\sigma_{\mathsf{nbt}}} \circ \varphi_{\mathsf{nbt}} \in \mathrm{End}(E_A)$.

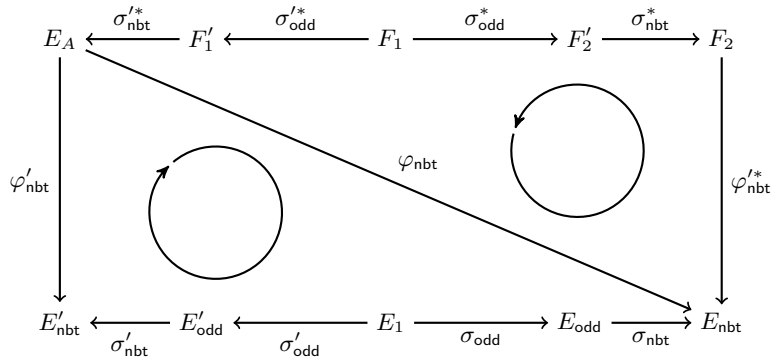

Fig. 4. Commutative diagram for the extractor, the sides of the rectangle are parallel isogenies.

If $\widehat{\varphi'^*_{\mathsf{nbt}}} \circ \sigma'^*_{\mathsf{nbt}} \circ \widehat{\sigma_{\mathsf{nbt}}} \circ \varphi_{\mathsf{nbt}} \notin \mathbb{Z}$, then since $\sigma'^*_{\mathsf{odd}} \circ \widehat{\sigma^*_{\mathsf{odd}}}$ has odd degree, the degree of α is divisible by 2. This leads us to the same setting as earlier in Equation 1, where the first step of the power 2 isogeny that appears in α is not $\mathbb{F}_p$-rational, implying that α is not $\mathbb{F}_p$-rational.

If $\widehat{\varphi'^*_{\mathsf{nbt}}} \circ \sigma'^*_{\mathsf{nbt}} \circ \widehat{\sigma_{\mathsf{nbt}}} \circ \varphi_{\mathsf{nbt}} \in \mathbb{Z}$, then the degree of α divides $d_0 d'_0 = \deg(\sigma'^*_{\mathsf{odd}} \circ \widehat{\sigma^*_{\mathsf{odd}}})$ which in turn divides dd' and $dd' < p$. We claim that α is not $\mathbb{F}_p$-rational. In fact, if α were $\mathbb{F}_p$-rational, then since the orienting order is $\mathfrak{O} = \mathbb{Z}[\pi]$, we would have that $\alpha = u + v\pi$ and $u^2 + v^2 p = \deg(\alpha) < p$, implying that $v = 0$ and $\alpha = [u] \in \mathbb{Z}$. Since α is cyclic, then $\alpha = [\pm 1]$, implying that $\alpha_0 = [\pm d_0 d'_0 2^{e - \frac{n_{\mathsf{bt}} + n'_{\mathsf{bt}} - n_{\mathsf{nbt}} - n'_{\mathsf{nbt}}}{2}}]$. Since σ_{odd} and $\widehat{\sigma'_{\mathsf{odd}}}$ are cyclic isogenies of odd degree d_0 and d'_0 respectively, then $d_0 = d'_0$ and $\sigma'_{\mathsf{odd}} \circ \widehat{\sigma_{\mathsf{odd}}} = [d_0] \in \mathbb{Z}$. This contradicts our starting point in Case 2 where we assume that $\sigma'_{\mathsf{odd}} \circ \widehat{\sigma_{\mathsf{odd}}} \notin \mathbb{Z}$. □

Zero-knowledge. As in all dimension two variants [6,54,36] of SQIsign, each valid signature reveals two random non-smooth degree isogenies $\sigma : E_1 \to E_2$ and $\delta : E_1 \to E_\delta$. Computing isogenies of non-smooth degree is hard in general. In order to prove the zero-knowledge property of our scheme, we need to equip the adversary with oracles that he can query to get such random isogenies. Since these are random isogenies, which every one could generate if their degree were smooth, then it is believed that the access to these oracles does weaken the One Non-rational Endomorphism problem.

Definition 7. *The* Random Uniform Bounded Degree Isogeny Oracle *(RUBDIO) is an oracle that takes as input a supersingular curve E and returns an efficient representation of an isogeny $\sigma : E \to E'$ of degree $d < \sqrt{p}$ such that:*

- *E' is uniformly distributed in the supersingular isogeny graph.*
- *If $j(E') \in \mathbb{F}_p$ one resamples E'.*
- *The conditional distribution of σ given E' is uniform among isogenies $\sigma : E \to E'$ of degree $d < \sqrt{p}$.*

Definition 8. *The* Random Auxiliary Isogeny Oracle *(RAIO) is an oracle that takes as input a supersingular curve E, an odd integer $d_0 < \sqrt{p}$ and an integer $r' \geq \lceil \log(d_0) \rceil$, and returns an efficient representation of a random isogeny $\delta : E \to E'$ of odd degree $2^{r'} - d_0$.*

Proposition 9. *Let $p \approx 2^{2\mu\lambda}$ (where λ is the security parameter) be the prime used in WaterSQI. If $d_{\mathsf{com}} \geq 2^{2(\mu+1)\lambda}$, then there exists an efficient simulator which when given access to a RUBDIO and a RAIO, outputs random transcripts which are statistically indistinguishable from honest transcripts in WaterSQI.*

Proof. Given an honestly generated challenge $\varphi : E_A \to E_2$, the simulator calls RUBDIO on E_2 and gets an efficient representation of a random isogeny $\widehat{\sigma} : E_2 \to E_1$ of degree $d < \sqrt{p}$. It writes d as $d = d_0 \cdot 2^n$. Let n_{bt} be the number of steps of which $\widehat{\sigma}$ backtracks φ. If $e - \lambda < n_{\mathsf{bt}}$, the simulator issues new calls to RUBDIO with the same curve E_2 until it gets an output $\widehat{\sigma} : E_2 \to E_1$ for which $n_{\mathsf{bt}} \leq e - \lambda$. It factors $\sigma : E_1 \to E_2$ as $\sigma = \sigma_{\mathsf{bt}} \circ \sigma_{\mathsf{real}}$ where $\sigma_{\mathsf{real}} : E_1 \to E_{\mathsf{nbt}}$ and $\sigma_{\mathsf{bt}} : E_{\mathsf{nbt}} \to E_2$ have degree $d_0 \cdot 2^{n-n_{\mathsf{bt}}}$ and $2^{n_{\mathsf{bt}}}$ respectively. It then calls RAIO on E_1 and gets an efficient representation of a random isogeny $\delta : E_1 \to E_\delta$ of degree $2^{r-n} - d_0$. It computes $\sigma_{\mathsf{real}} \circ \widehat{\delta}(E_\delta[2^{r-n_{\mathsf{bt}}}])$ and returns $(E_\delta, \sigma_{\mathsf{real}} \circ \widehat{\delta}(E_\delta[2^{r-n_{\mathsf{bt}}}]), d_0, n - n_{\mathsf{bt}}, n_{\mathsf{bt}})$ as the transcript.

The degree of the commitment isogeny is $d_{\mathsf{com}} \geq 2^{2(\mu+1)\lambda}$. Applying [28, Proposition 29] with $\epsilon = 1/\mu$, it follows that an honestly generated commitment curve E_1 in WaterSQI is at statistical distance $O(p^{-\epsilon/2}) = O(2^{-\lambda})$ from a uniformly random supersingular curve. Notice that with respect to the definition of RUBDIO, the simulator rejecting the output of RUBDIO when $e - \lambda < n_{\mathsf{bt}}$ and issuing a new call, is the same as the signer triggering a restart of the signing process in step 8 of the response algorithm. Therefore, the transcript returned by the simulator is statistically indistinguishable from a transcript obtained by running WaterSQI. □

Now that we have proven 2-special soundness and honest-verifier zero knowledge, applying the Fiat-Shamir transform gives us a signature algorithm which is EUF-CMA under Assumption 10.

Assumption 10 *The One Non-rational Endomorphism problem (Problem 5) remains hard in the RUBDIO and RAIO model.*

4 FastWaterSQI: a faster variant of WaterSQI

As discussed at the beginning of Section 3, we also propose a faster variant where the commitment isogeny and the response computation are more efficient, at the cost of having a computational zero-knowledge property for our sigma protocol. In FastWaterSQI, the commitment isogeny is now sampled as an isogeny of degree $2^{2\lambda}$. This allows the computation of the commitment isogeny to be fully in dimension 1. When generating the auxiliary isogeny $\delta : E_1 \to E_\delta$, we first generate a random isogeny $\delta_0 : E_0 \to E_{\delta_0}$ of the same degree $2^{r-n} - d_0$, then we compute its push-forward through the commitment isogeny ψ to obtain $\delta = [\psi]_* \delta_0$. The remainder of the scheme is unchanged.

Algorithm 6 Fast commitment isogeny computation

Require: $\mathsf{pp} = (p, a, r, e, E_0, \mathfrak{O}, \mathrm{End}(E_0) \simeq \mathcal{O}_0)$
Ensure: $\mathsf{com}_{\mathsf{state}} = (I_\psi, u)$, $\mathsf{com} = E_1$
1: Generate a canonical basis (P_0, Q_0) of $E_0[2^{2\lambda}]$ such that $E_0(\mathbb{F}_p)[2] = \langle [2^{2\lambda-1}]Q_0 \rangle$
2: Sample u at random from $\mathbb{Z}/2^{2\lambda}\mathbb{Z}$
3: Set $R = P_0 + [u]Q_0$
4: Compute the isogeny $\varphi : E_0 \to E_1 := E_0/\langle R \rangle$ whose kernel is generated by R
5: **if** $j(E_1) \in \mathbb{F}_p$ **then**
6: Go back to Step 2
7: Compute the left $\mathcal{O}_0$ ideal I_ψ corresponding to the isogeny ψ
8: **return** $\mathsf{com}_{\mathsf{state}} = (I_\psi, u)$, $\mathsf{com} = j(E_1)$

4.1 Public parameters, key generation, commitment and challenge

The public parameters $\mathsf{pp} = (p, a, r, e, E_0, \mathfrak{O}, \mathrm{End}(E_0) \simeq \mathcal{O}_0)$ where $p = 2^a \cdot f - 1$ are similar to those of WaterSQI, except that $e = \frac{5}{4}\lambda$. The key generation algorithm and the challenge algorithm are also identical to that of WaterSQI (see Section 3). We now describe the commitment algorithm.

Commitment. The commitment isogeny is now a random isogeny $\psi : E_0 \to E_1$ of degree $2^{2\lambda}$ which is generated in a similar way as the challenge isogeny. That is one generates a deterministic basis (P_0, Q_0) of $E_0[2^{2\lambda}]$ such that $E_0(\mathbb{F}_p)[2] = \langle [2^{2\lambda-1}]Q_0 \rangle$, one samples u at random from $\mathbb{Z}/2^{2\lambda}\mathbb{Z}$ and sets $R = P_0 + [u]Q_0$. One computes $\psi : E_0 \to E_1$ of kernel $\langle R \rangle$. If $j(E_1) \in \mathbb{F}_p$, one samples a new u and recomputes ψ. One then translates ψ into its corresponding ideal I_ψ. This fast commitment process is summarised in Algorithm 6.

4.2 Response and verification in FastWaterSQI

The verification in FastWaterSQI is identical to that of WaterSQI. We hence only describe the response computation.

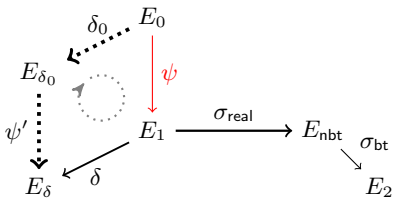

Fig. 5. Fast aux. isogeny computation.

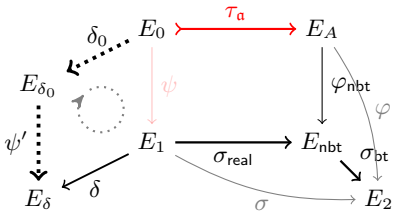

Fig. 6. Fast response computation.

Response. The response algorithm follows several steps.

Algorithm 7 Fast response

Require: $\mathsf{pp} = (p, a, r, e, E_0, \mathfrak{O}, \mathrm{End}(E_0) \simeq \mathcal{O}_0)$, $\mathsf{sk} = (\mathfrak{a}, \tau_{\mathfrak{a}}(E_0[2^a]))$, $\mathsf{pk} = E_A$, $\mathsf{com}_{\mathsf{state}} = (I_\psi, u)$, $\mathsf{com} = j(E_1)$, $\mathsf{chal} = c$

Ensure: The response $\mathsf{resp} = (E_\delta, \sigma_{\mathsf{real}} \circ \widehat{\delta}(E_\delta[2^{r-n_{\mathsf{bt}}}]), d_0, n_{\mathsf{nbt}}, n_{\mathsf{bt}})$

//Translating the challenge isogeny into an ideal

Compute the kernel the challenge isogeny $\varphi : E_A \to E_2$ as described in Algorithm 3

Compute $\widehat{\tau_{\mathfrak{a}}}(\ker \varphi)$ and translate it into a left $\mathcal{O}_0$ ideal I

Compute the push-forward $I_\varphi = [\mathfrak{a}]_* I$ of I through $\mathfrak{a}$

//Sampling the ideal of the response isogeny

Compute the ideal $I = \overline{I_\psi}\mathfrak{a}I_\varphi$

Sample a uniformly random ideal $I_\sigma \sim I$ of norm $d = d_0 \cdot 2^n < \sqrt{p}$ with d_0 odd

Compute the largest integer $n_{\mathsf{bt}} \leq n$ such that $I_\varphi \cdot \overline{I_\sigma} \in n_{\mathsf{bt}}\mathcal{O}_A$, and set $n_{\mathsf{nbt}} = n - n_{\mathsf{bt}}$

if $e - n_{\mathsf{bt}} < \lambda$ **then**

  return $\perp$ ▷ The whole signing process is actually restarted

//Generating the auxiliary isogeny and computing the response

Sample a random isogeny $\delta_0 : E_0 \to E_{\delta_0}$ of degree $2^{r-n} - d_0$ using KaniDoublePath

Recover I_{δ_0}

Compute $\delta_0(E_0[2^a])$ and retrieve $\delta_0(\ker(\psi))$

Compute $\psi' = [\delta_0]_*\psi : E_{\delta_0} \to E_\delta = E_{\delta_0}/\delta_0(\ker(\psi))$ and recover $\psi'(E_{\delta_0}[2^a])$

Compute the push-forward $I_\delta := [I_\psi]_* I_{\delta_0}$ of I_{δ_0} through I_ψ

//Evaluating $\sigma \circ \widehat{\delta}$ on $E_\delta[2^{r-n_{\mathsf{bt}}}]$

Find $\gamma \in \mathcal{O}_0$ such that $\mathcal{O}_0\gamma = I_{\delta_0} I_{\psi'} I_\delta I_\sigma \overline{I_\varphi}\overline{\mathfrak{a}} = (2^{r-n} - d_0) I_\psi I_\sigma \overline{I_\varphi}\overline{\mathfrak{a}}$

Compute $\theta(E_0[2^a])$ where $\theta \in \mathrm{End}(E_0)$ corresponds to $\gamma \in \mathcal{O}_0$.

Recover $\sigma \circ \widehat{\delta}(E_\delta[2^r]) = [2^{a-3\lambda-r}]\sigma \circ \widehat{\delta}(E_\delta[2^{a-3\lambda}]) = \frac{2^{a-3\lambda-r}}{\deg \delta_0 \cdot \deg \tau} \varphi \circ \tau \circ \theta \circ \widehat{\delta_0} \circ \widehat{\psi'}(E_\delta[2^a])$

Deduce $\sigma_{\mathsf{real}} \circ \widehat{\delta}(E_\delta[2^{r-n_{\mathsf{bt}}}])$ from $\sigma \circ \widehat{\delta}(E_\delta[2^r])$

return $\mathsf{resp} = (E_\delta, \sigma_{\mathsf{real}} \circ \widehat{\delta}(E_\delta[2^{r-n_{\mathsf{bt}}}]), d_0, n_{\mathsf{nbt}}, n_{\mathsf{bt}})$

1. Compute the ideal I_φ corresponding to the challenge isogeny $\varphi : E_A \to E_2$, sample the ideal I_σ of norm $d = d_0 \cdot 2^n$ and compute n_{bt}, n_{nbt} as described in WaterSQI (section 3.2). Contrarily to WaterSQI where we evaluate σ and the auxiliary isogeny δ separately. In FastWaterSQI, we generate the auxiliary isogeny, evaluate $\sigma \circ \widehat{\delta}(E_\delta[2^r])$ directly and deduce $\sigma_{\mathsf{real}} \circ \widehat{\delta}(E_\delta[2^{r-n_{\mathsf{bt}}}])$.
2. To generate a random auxiliary isogeny $\delta : E_1 \to E_\delta$ of degree $2^{r-n} - d_0$, one proceeds as follows. Use KaniDoublePath to sample a random isogeny $\delta_0 : E_0 \to E_{\delta_0}$ of degree $2^{r-n} - d_0$ together with its ideal I_{δ_0}. Compute the pushforward $\psi' = [\delta_0]_*\psi : E_{\delta_0} \to E_\delta$ of ψ through δ_0 which has kernel $\delta_0(\ker \psi)$, together with its ideal $I_{\psi'} = [I_{\delta_0}]_* I_\psi$. Let $\delta = [\psi]_*\delta_0 : E_1 \to E_\delta$ be the pushforward of δ_0 through ψ. Compute the ideal $I_\delta = [\psi]_* I_{\delta_0}$.
3. Now we want to evaluate $\sigma \circ \widehat{\delta}(E_\delta[2^r])$. We first recover the endomorphism $\theta = \widehat{\tau} \circ \widehat{\varphi} \circ \sigma \circ \widehat{\delta} \circ \psi' \circ \delta_0 = [2^{r-n} - d_0]\widehat{\tau} \circ \widehat{\varphi} \circ \sigma \circ \psi \in \mathrm{End}(E_0)$ from the principal ideal $I_{\delta_0} I_{\psi'} I_\delta I_\sigma \overline{I_\varphi}\overline{\mathfrak{a}} = (2^{r-n} - d_0) I_\psi I_\sigma \overline{I_\varphi}\overline{\mathfrak{a}}$ of $\mathcal{O}_0$. Evaluate $\theta(E_0[2^a])$. Rely on the fact that $[2^{3\lambda} \cdot \deg \delta_0 \cdot \deg \tau]\sigma \circ \widehat{\delta} = [\deg \varphi \cdot \deg \psi' \cdot \deg \delta_0 \cdot \deg \tau]\sigma \circ \widehat{\delta} = \varphi \circ \tau \circ \theta \circ \widehat{\delta_0} \circ \widehat{\psi'}$ and $\deg \delta_0 \cdot \deg \tau$ is odd to recover $\sigma \circ \widehat{\delta}(E_\delta[2^{a-3\lambda}]) = \frac{1}{\deg \delta_0 \cdot \deg \tau} \varphi \circ \tau \circ \theta \circ \widehat{\delta_0} \circ \widehat{\psi'}(E_\delta[2^a])$. Recover $\sigma \circ \widehat{\delta}(E_\delta[2^r])$

and deduce $\sigma_{\mathsf{real}} \circ \widehat{\delta}(E_\delta[2^{r-n_{\mathsf{bt}}}])$ where σ_{real} is, as in WaterSQI, the part of σ_{real} left after one has removed the part of $\widehat{\sigma}$ that backtracks φ. Here, r must satisfy $r \leq a - 3\lambda$, which is not that much restrictive as we will be using primes of several thousand bits.

The response is $(E_\delta, \sigma_{\mathsf{real}} \circ \widehat{\delta}(E_\delta[2^{r-n_{\mathsf{bt}}}]), d_0, n_{\mathsf{nbt}}, n_{\mathsf{bt}})$. The auxiliary isogeny computation and the response computation are illustrated in Figure 5 and Figure 6 respectively, and the fast response algorithm is summarised in Algorithm 7.

4.3 The FastWaterSQI signature algorithm

As usual, we prove that the FastWaterSQI identification scheme is a Σ-protocol by showing that it is 2-special sound and honest-verifier zero knowledge, before applying[2] the Fiat-Shamir transform to obtain a digital signature scheme which is EUF-CMA in the Random Oracle model.

In fact, transcripts of WaterSQI and FastWaterSQI are quite similar, the only differences being the distribution of the commitment curve E_1 and the upper bound $e-\lambda$ on the number of steps by which the dual of the response isogeny is allowed to backtrack the challenge isogeny. As a consequence, the soundness proof for FastWaterSQI is identical to that of WaterSQI. Only the zero-knowledge property if affected. In fact, we will obtain the zero-knowledge property under the assumption that the commitment curve is computationally indistinguishable from a random supersingular curve and that the auxiliary isogeny generated using KaniDoublePath and pushforwards is computationally indistinguishable from a random isogeny of the same degree.

Assumption 11 *The commitment curve E_1 obtained by sampling a random $2^{2\lambda}$-isogeny such that 1_ϕ is not $\mathbb{F}_p$-rational is computationally indistinguishable from a supersingular elliptic curve sampled uniformly at random.*

Assumption 12 *Let $\psi : E_0 \to E_1$ be a random $2^{2\lambda}$-isogeny and let $d_0 < 2^{r'}$ be an integer. An isogeny $\delta : E_1 \to E_\delta$ of degree $2^{r'} - d_0$ generated by sampling a random isogeny $\delta_0 : E_0 \to E_{\delta_0}$ using KaniDoublePath and computing its pushforward through ψ is computationally indistinguishable from a random isogeny of the same degree.*

Proposition 13. *Under Assumption 11 and Assumption 12, there exists an efficient simulator which when given access to a RUBDIO and a RAIO, outputs random transcripts which are computationally indistinguishable from honest transcripts in FastWaterSQI.*

Proof. The simulator is the same as in WaterSQI (see the proof of Proposition 9). Let $(E_\delta, \sigma_{\mathsf{real}} \circ \widehat{\delta}(E_\delta[2^{r-n_{\mathsf{bt}}}]), d_0, n - n_{\mathsf{bt}}, n_{\mathsf{bt}})$ be its output.

[2] Similarly to WaterSQI, FastWaterSQI is commitment recoverable. Hence the discussion at the beginning of Section 3.3 applies to FastWaterSQI as well.

From Assumption 11, an honestly generated commitment curve E_1 in FastWaterSQI is computationally indistinguishable from a uniformly random supersingular curve. From Assumption 12, the auxiliary isogenies returned by RAIO is computationally indistinguishable from the ones in honest transcripts of FastWaterSQI. Therefore, the transcript returned by the simulator is computationally indistinguishable from a transcript obtained by running FastWaterSQI. □

Finally, applying the Fiat-Shamir transform gives us a signature algorithm which is EUF-CMA under Assumption 10, Assumption 11 and Assumption 12.

4.4 WaterSQI as a quantum proof of knowledge of the endomorphism ring

The WaterSQI sigma protocol proves the knowledge of an endomorphism $\alpha \in \mathrm{End}(E) \setminus \mathrm{End}_{\mathbb{F}_p}(E)$ where E is a supersingular elliptic curve defined over $\mathbb{F}_p$. What about proving the knowledge of an ideal $\mathfrak{a}$ such that $\mathfrak{a}E_0 = E$, as it is the case for (Generalised) CSI-FiSh? Well, WaterSQI also does that, but in the quantum regime. In fact, since $\mathrm{End}(E_0)$ is known, then proving the knowledge of an ideal $\mathfrak{a}$ such that $\mathfrak{a}E_0 = E$ is equivalent to proving the knowledge of $\mathrm{End}(E)$ [18,63].

Proposition 14. *Given two valid WaterSQI transcripts sharing the same commitment but with different challenges, there exist a quantum polynomial time algorithm to recover* $\mathrm{End}(E_A)$.

Proof. First, one runs the WaterSQI extractor (Prop. 6) to obtain an endomorphism $\alpha \in \mathrm{End}(E_A) \setminus \mathrm{End}_{\mathbb{F}_p}(E_A)$, which leads to the subring $\mathbb{Z}[\alpha, \pi] \subset \mathrm{End}(E_A)$ of rank 4. One then applies Chen and Petit's quantum algorithm [21] to recover $\mathrm{End}(E_A)$ from $\mathbb{Z}[\alpha, \pi]$.

Remark 15. In [37], Eisenträger and Scullard propose a classical algorithm for recovering $\mathrm{End}(E_A)$ from $\mathbb{Z}[\alpha, \pi]$, when the factorisation of the discriminant of $\mathbb{Z}[\alpha, \pi]$ is known. In our case, we have that

$$\mathrm{disc}(\mathbb{Z}[\alpha, \pi]) = 16 \cdot \mathrm{Vol}(\mathbb{Z}[\alpha, \pi]) \leq 16 \cdot \sqrt{\deg \pi \deg \alpha \deg \pi \circ \alpha} = p^2 \cdot 2^{2e+4},$$

meaning that the number to be factored, $[\mathrm{End}(E_A) : \mathbb{Z}[\alpha, \pi]] \approx \sqrt{\mathrm{disc}(\mathbb{Z}[\alpha, \pi])}/p$, has at most $e + 2 = \frac{3}{2}\lambda + 2$ bits (or $e + 2 = \frac{5}{4}\lambda + 2$ bits for FastWaterSQI). It can hence be factored by current consumer computers. Nevertheless, the cost of the algorithm is dominated by the largest prime $q \neq p$ dividing $[\mathrm{End}(E_A) : \mathbb{Z}[\alpha, \pi]]$, preventing this method from being classically efficient.

5 PRISMO: PRISM for Oriented supersingular curves

In this section, we briefly recall PRISM and describe PRISMO, the variant of PRISM that work with the public key E being defined over $\mathbb{F}_p$ (or being an oriented supersingular curve in general).

5.1 The PRISM signature

Let u be an integer and let Primes_u be the set of primes q such that $2^{u-1} < q < 2^u$. In PRISM, the signer's public key is a random supersingular curve $\mathsf{pk} = E$ defined over $\mathbb{F}_{p^2}$ and his secret key is an isogeny $\tau : E_0 \to E$. The PRISM identification scheme uses of two main algorithms:

- $\sigma \leftarrow \mathsf{GenIsogeny}(E, \phi, q)$ which takes a supersingular curve E, an isogeny $\phi : E_0 \to E$ and a prime q as inputs, and returns a representation of an isogeny $\varphi : E \to E'$ of degree $q(2^u - q)$ which is uniformly distributed among isogenies of degree $q(2^u - q)$ from E. It makes a call to Qlapoti internally.
- $\mathsf{accept/reject} \leftarrow \mathsf{VerIsogeny}(\sigma, E, q)$ which takes a representation of an isogeny $\sigma : E \to E'$ and returns accept if its degree is $q(2^u - q)$, reject if not.

In the PRISM identification scheme, the prover gets a challenge $q \in \mathsf{Primes}_u$ from the verifier, runs $\mathsf{GenIsogeny}(E, \phi, q)$ to obtain the response $\sigma : E \to E'$ which they send to the verifier. The verifier then runs $\mathsf{VerIsogeny}(\sigma, E, q)$ and either accepts or rejects. Using a collision resistance hash function $\mathsf{H}_{\mathsf{Prime}} : \{0,1\}^* \to \mathsf{Primes}_u$, one can transform the PRISM identification scheme into a hash-and-sign type digital signature as shown in Figure 7. Since each PRISM signature provides a $q(2^u - q)$-isogeny which is hard to generate in practice, in the security analysis of PRISM, an oracle generating such isogenies is provided to the adversary. This oracle is called SPEDIO. The signature scheme is then proven [4, Prop. 2] to be EUF-CMA secure under the assumption that $\mathsf{H}_{\mathsf{Prime}}$ is a collision resistant hash function and Problem 17 is hard.

Definition 16. *A special degree isogeny oracle (SPEDIO) is an oracle which takes as inputs a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$ and a prime $q \in \mathsf{Primes}_u$, and returns a uniformly random cyclic isogeny of degree $q(2^u - q)$ from E.*

Problem 17. Given a random supersingular elliptic curve E and a SPEDIO, output an isogeny of degree $q'(2^u - q')$ with $q' \in \mathsf{Primes}_u$ different from all degrees q formerly queried to SPEDIO.

Proposition 18 ([4, Prop. 2]). *If $\mathsf{H}_{\mathsf{Prime}}$ is a collision-resistant cryptographic hash function and Problem 17 is hard, then PRISM is EUF-CMA secure.*

5.2 The PRISMO signature

PRISM is not secure when the public key E is defined over $\mathbb{F}_p$ (or oriented in general) as it is easy to forge valid signatures. In fact, given E defined over $\mathbb{F}_p$, one proceeds as follows to forge a valid signature.

1. *Sieve for the message to be forged.* Here we randomly sample messages m till we get one for which $q = \mathsf{H}_{\mathsf{Prime}}(E||\mathsf{m})$ and the non-smooth factors of $2^u - a$ are split primes in $\mathfrak{O} \simeq \mathbb{Z}[\pi]$. This requires $O(\log p)$ evaluations of $\mathsf{H}_{\mathsf{Prime}}$ and Legendre symbol computations. For each evaluation, one needs to factor $2^u - q$. This is done by factoring out its smooth part and checking if the remaining factor is a prime.

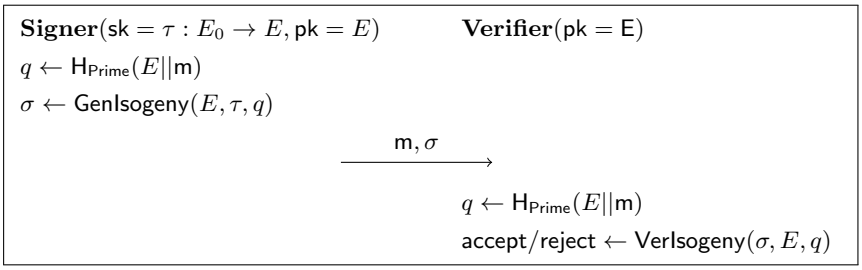

Fig. 7. PRISM signature scheme.

2. *Generate the quadratic ideal.* Once we have found a message m such that $q = \mathsf{H}_{\mathsf{Prime}}(E||\mathsf{m})$ and the non-smooth factors of $2^u - q$ are split primes in $\mathfrak{O} \simeq \mathbb{Z}[\pi]$, we write $2^u - q$ as $2^u - q = st$ where s is the smooth part of $2^u - q$, this implies that t is made of split primes. Let $v = tq$. We generate an ideal $\mathfrak{b} = \mathfrak{O}\langle\sqrt{-p} - w, v\rangle$ of $\mathfrak{O} \simeq \mathbb{Z}[\pi]$ of norm v by computing a square root w of $-p \mod v$. Since we know the prime factorisation of v this is efficient as one computes square roots modulo these primes and use the Chinese Remainder Theorem to recover w.
3. *Forge the signature.* Use PEGASIS [26] to compute the v-isogeny $\sigma_1 : E \to E_1$ corresponding to $\mathfrak{b}$. Generate a random isogeny $\sigma_2 : E_1 \to E'$ of degree s. Return $(\mathsf{m}, \sigma = \sigma_2 \circ \sigma_1)$ as the forged signature. Note that (m, σ) is a valid signature as the degree of $\sigma : E \to E'$ is $sv = stq = q(2^u - q)$ and $q = \mathsf{H}_{\mathsf{Prime}}(E||\mathsf{m})$. Computing $\sigma_1 : E \to E_1$ is efficient as one uses PEGASIS, and generating $\sigma_2 : E_1 \to E'$ is efficient as well as its degree s is smooth.

The main ingredient in the attack above is the PEGASIS algorithm which is used to evaluate non-smooth degree $\mathbb{F}_p$-rational (oriented) isogenies. This algorithm is useless when it comes to evaluating non $\mathbb{F}_p$-rational (non oriented) isogenies. To thwart the attack, it suffices to require that the q-isogeny part of the response isogeny σ of degree $q(2^u - q)$ is not $\mathbb{F}_p$-rational. A straightforward way to insure this is to ask for q to be a prime inert in $\mathfrak{O} \simeq \mathbb{Z}[\pi]$. The cost of this change is almost negligible as it only affects the run time of the hash function $\mathsf{H}_{\mathsf{Prime}}$ which is two times slower as about $1/2$ of primes are inert in $\mathfrak{O} \simeq \mathbb{Z}[\pi]$, and the verification algorithm where one further checks that q is inert in $\mathfrak{O} \simeq \mathbb{Z}[\pi]$ by computing one Legendre symbol. In Appendix B, we describe an alternative design choice where the hash function is left as it is, but the verifier actually checks that the q-isogeny part of the response isogeny σ is not $\mathbb{F}_p$-rational. Here we go for an inert challenge degree q.

In the PRISMO identification scheme, the public key $\mathsf{pk} = E$ is a curve defined over $\mathbb{F}_p$, and the secret key is an $\mathbb{F}_p$-rational isogeny $\tau_{\mathfrak{a}} : E_0 \to E$. The challenge is a large prime q which is inert in $\mathfrak{O} \simeq \mathbb{Z}[\pi]$. The response is a $q(2^u - q)$-isogeny $\sigma : E \to E'$. During the verification, one verifies that $\sigma : E \to E'$ is an isogeny of degree $q(2^u - q)$ and that q is inert in $\mathfrak{O} \simeq \mathbb{Z}[\pi]$. The PRISMO identification scheme hence makes use of the following two algorithms:

- $\sigma \leftarrow \mathsf{GenIsogeny}_{\mathsf{O}}(E, \phi, q)$ which takes a supersingular curve E defined over $\mathbb{F}_p$, an isogeny $\phi : E_0 \to E$ and a large prime q inert in $\mathfrak{O} \simeq \mathbb{Z}[\pi]$ as inputs, and returns a representation of an isogeny $\varphi : E \to E'$ of degree $q(2^u - q)$ which is uniformly distributed among isogenies of degree $q(2^u - q)$ from E. It makes a call to Qlapoti internally.
- $\mathsf{accept/reject} \leftarrow \mathsf{VerIsogeny}_{\mathsf{O}}(\sigma, E, q)$ which takes a representation of an isogeny $\sigma : E \to E'$ and returns accept if its degree is $q(2^u - q)$ and q inert in $\mathfrak{O} \simeq \mathbb{Z}[\pi]$; reject if not.

With the $\mathsf{GenIsogeny}_{\mathsf{O}}$ and $\mathsf{VerIsogeny}_{\mathsf{O}}$ algorithms defined above, one obtains the PRISMO identification scheme in a similar way as in PRISM. To turn it into a signature scheme, we need a hash function $\mathsf{H}_{\mathsf{InertPrime}} : \{0,1\}^* \to \mathsf{InertPrimes}_u$, where $\mathsf{InertPrimes}_u$ is the set of primes q such that $2^{u-1} < q < 2^u$ and q is inert $\mathfrak{O} \simeq \mathbb{Z}[\pi]$. It is designed in a similar way as $\mathsf{H}_{\mathsf{Prime}} : \{0,1\}^* \to \mathsf{Primes}_u$ which is obtained from any other generic hash function $\mathsf{H}_{u-2} : \{0,1\}^* \to \{0,1\}^{u-2}$ as follows: given a message m and a public key E, $\mathsf{H}_{\mathsf{Prime}}(E||\mathsf{m})$ is obtained by repeatedly computing $2^{u-1} + 2\mathsf{H}_{u-2}(E||\mathsf{m}||\mathsf{counter}) + 1$ for increasing values of counter until the output is a prime number. For $\mathsf{H}_{\mathsf{InertPrime}}$, we iterate until we get a prime which is inert in $\mathfrak{O} \simeq \mathbb{Z}[\pi]$. We expect the number of iterations to double as about $1/2$ of primes are inert in $\mathfrak{O} \simeq \mathbb{Z}[\pi]$.

With $\mathsf{H}_{\mathsf{InertPrime}}$, we transform the PRISMO identification scheme into the PRISMO signature as described in Figure 8.

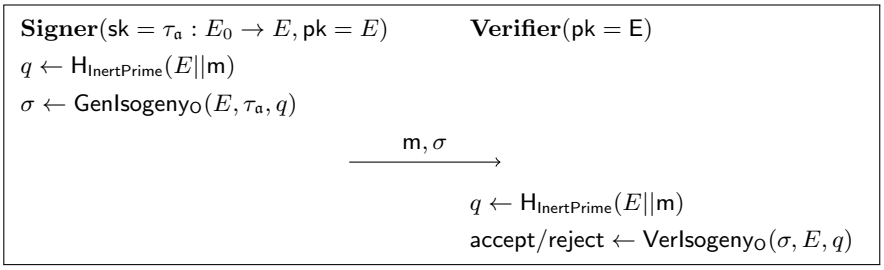

Fig. 8. PRISMO signature scheme.

5.3 Security

The security arguments for PRISMO are similar to those provided for PRISM, with the only exceptions being that one needs to use a prime characteristic p offering enough quantum security as we are in the supersingular isogeny group actions setting, and one needs to restrict the SPEDIO oracle and the hard problem underlying the security of the scheme to inert degrees q. We provide the new $\mathrm{SPEDIO}_{\mathsf{O}}$ oracle in Definition 19 and the new hard problem in Problem 20. We then state in Proposition 21 that PRISMO is EUF-CMA secure under the

assumption that $\mathsf{H}_{\mathsf{InertPrime}}$ is a collision resistance hash function and Problem 20 is hard. We omit the proof of as it can be obtained from that of Proposition 18 (see [4, Prop. 2]) where one replaces SPEDIO by SPEDIO$_{\mathsf{O}}$ and Problem 17 by Problem 20.

Definition 19. *SPEDIO$_{\mathsf{O}}$ is an oracle which takes as input a supersingular elliptic curve E defined over $\mathbb{F}_p$ and a prime $q \in \mathsf{InertPrimes}_u$, and returns a uniformly random cyclic isogeny φ of degree $q(2^u - q)$ from E.*

Problem 20. Given a random supersingular elliptic curve E defined over $\mathbb{F}_p$ and a SPEDIO$_{\mathsf{O}}$, output an isogeny φ of degree $q'(2^u - q')$ with $q' \in \mathsf{InertPrimes}_u$ different from all degrees q formerly queried to SPEDIO$_{\mathsf{O}}$ ($u = 2\lambda$).

Proposition 21. *If $\mathsf{H}_{\mathsf{InertPrime}}$ is a collision-resistant cryptographic hash function and Problem 20 is hard, then PRISMO is EUF-CMA secure.*

We believe that Problem 20 in PRISMO is as hard as Problem 17 in PRISM because as the prime q is inert in $\mathfrak{O} \simeq \mathbb{Z}[\pi]$, the sub-ring $\mathbb{Z}[\pi]$ of $\mathrm{End}(E)$ is not useful at all when trying to evaluate a q-isogeny when q has not been queried to SPEDIO$_{\mathsf{O}}$. Meaning that even if one were able to compute a $(2^u$-$q)$-isogeny, the degree q one would be infeasible to compute as the best known algorithm would run in time $O(q^2)$ [4, §4.4].

Remark 22. In Problem 20, since we have one non-trivial endomorphism $\pi \in \mathrm{End}(E)$, given one $q(2^u - q)$-isogeny $\varphi : E \to E'$ returned by SPEDIO$_{\mathsf{O}}$, one can efficiently compute a representation of the isogeny[3] $\varphi^{(p)} : E \to E'^{(p)}$. But, since the degree of $\varphi^{(p)}$ is also $q(2^u - q)$, $\varphi^{(p)}$ is not a solution to Problem 20. Nevertheless, this means that PRISMO is not strongly unforgeable under chosen message attacks, as given a message/signature pair (m, σ), $(\mathsf{m}, \sigma^{(p)})$ is also a valid signature for m and $\sigma \neq \sigma^{(p)}$.

6 Instantiation and comparison

In this section, we discuss parameters and signature sizes of (Fast)WaterSQI and PRISMO, and provide a comparison between WaterSQI, FastWaterSQI, PRISMO, Generalised CSI-FiSh and SQI-FiSh.

6.1 Parameters and signature sizes for (Fast)WaterSQI

Parameters The parameters and signature sizes for WaterSQI and FastWaterSQI are identical. We use the primes p_{500}, p_{1000} and p_{2000} listed in Table 2, which are the same as in PEGASIS [26].

The starting curve is the usual $E_0 : y^2 = x^3 + x$ and the orienting quadratic order is $\mathfrak{O} \simeq \mathbb{Z}[\pi]$, but the scheme could be adapted to work with any other

[3] Given an isogeny $\varphi : E \to E'$ where E is defined over $\mathbb{F}_p$ and the degree of φ is coprime to p, $\varphi^{(p)}$ is the isogeny of kernel $\pi(\ker \varphi)$.

quadratic order. The integer r is set to $r = \lceil \frac{1}{2} \log p \rceil$. In WaterSQI we have $e = \frac{3}{2}\lambda$ while in FastWaterSQI $e = \frac{5}{4}\lambda$. When discussing the parameters in a general context, for a given security parameter λ we will assume that $p = 2^a \cdot f - 1 \approx 2^{2\mu\lambda}$ with $\mu \geq 2$.

Signature sizes The signature has the same format in WaterSQI and FastWaterSQI. Recall that both schemes are commitment recoverable, hence the signature is made of the challenge $\mathsf{chal} = c \in \mathbb{Z}/2^\lambda\mathbb{Z}$ and the response $\mathsf{resp} = (E_\delta, \sigma_{\mathsf{real}} \circ \widehat{\delta}(E_\delta[2^{r-n_{\mathsf{bt}}}]), d_0, n_{\mathsf{nbt}}, n_{\mathsf{bt}})$. The elliptic curve E_δ can be represented by its j-invariant (or its Montgomery coefficient) which lies in $\mathbb{F}_{p^2}$ and has a $2\log p$ bits representation. The data $\sigma_{\mathsf{real}} \circ \widehat{\delta}(E_\delta[2^r])$ is provided as $(\sigma_{\mathsf{real}} \circ \widehat{\delta}(P_\delta), \sigma_{\mathsf{real}} \circ \widehat{\delta}(Q_\delta))$ where (P_δ, Q_δ) is a canonically generated basis of $E_\delta[2^r]$. One compresses $\sigma_{\mathsf{real}} \circ \widehat{\delta}(P_\delta)$ and $\sigma_{\mathsf{real}} \circ \widehat{\delta}(Q_\delta)$ by expressing them as $\sigma_{\mathsf{real}} \circ \widehat{\delta}(P_\delta) = [a_1]P_2 + [a_2]Q_2$, $\sigma_{\mathsf{real}} \circ \widehat{\delta}(Q_\delta) = [a_3]P_2 + [a_4]Q_2$ where (P_2, Q_2) is a canonically generated basis of $E_2[2^r]$, and using $a_1, a_2, a_3, a_4 \in \mathbb{Z}/2^r\mathbb{Z}$. Moreover, since we know the (odd) degree $d_0(2^{r-n} - d_0)$ of the isogeny $\sigma_{\mathsf{real}} \circ \widehat{\delta}$, one can further represent these points using only three of those scalars, at the cost of supplementary pairings and discrete logarithm computations during verification (see [28, Section 6.1] for further details). Since $d = 2^{n_{\mathsf{nbt}}+n_{\mathsf{bt}}} d_0 < 2^r$, then $d_0 || n_{\mathsf{nbt}} || n_{\mathsf{bt}}$ is represented using less than r bits.

Putting everything together, we have λ bits for the challenge and about $2\log p + 4r \approx 2\log p + 4(\frac{1}{2}\log p) \approx 4\log p$ for the response. Hence the size of the signature is roughly $\lambda + 4\log p$. When $p \approx 2^{2\mu\lambda}$, the signature size is $(8\mu + 1)\lambda$ bits, or $(\mu + 1/8)\lambda$ bytes. See Table 3 for a summary of the public key and signature sizes in (Fast)WaterSQI (and PRISMO).

6.2 Parameters and signature sizes for PRISMO

We use the same starting curve $E_0 : y^2 = x^3 + x$ and primes p (see Table 2) as in WaterSQI, and we set $u = 2\lambda$ (the bit length of the challenge prime q) where λ is the security parameter.

The signature in PRISMO is an isogeny $\sigma : E \to E'$. As in WaterSQI, a representation of this isogeny is given by $(E', \sigma(P), \sigma(Q))$ where (P, Q) is a canonically generated basis of $E[2^u]$. Similar compression techniques used for WaterSQI apply with the only difference being that the points $\sigma(P)$ and $\sigma(Q)$ now have order 2^u, meaning that the coefficients used to represent them lie in $\mathbb{Z}/2^u\mathbb{Z}$. Taking this into account, $(E', \sigma(P), \sigma(Q))$ can be represented using $2\log p + 3u \approx 2\log p + 6\lambda$ bits. For a generic prime $p \approx 2^{2\mu\lambda}$, the signature size is $2(2\mu + 3)\lambda$ bits, or $\frac{1}{4}(2\mu + 3)\lambda$ bytes. See Table 3 for a summary of the public key and signature sizes in PRISMO (and (Fast)WaterSQI).

6.3 Parameters and signature sizes for Generalised CSI-FiSh and SQI-FiSh.

Generalised CSI-FiSh is instantiated with the primes listed in Table 2. The starting curve E_0 here can be any supersingular curve defined over $\mathbb{F}_p$ such that

$\mathrm{End}_{\mathbb{F}_p}(E_0) \simeq \mathbb{Z}[\pi]$. One can also use a curve E_0 such that $\mathrm{End}_{\mathbb{F}_p}(E_0) \simeq \mathbb{Z}[\frac{1+\pi}{2}]$. In fact, PEGASIS [26] works best in the latter case, as the 2-torsion is $\mathbb{F}_p$-rational.

Let us assume that Generalised CSI-FiSh is being instantiated with the parameters (S, t, k), which means that the secret key is a tuple of $S-1$ secret ideals $(\mathfrak{a}_1, \ldots, \mathfrak{a}_{S-1})$, the public key is $(E_1 = \mathfrak{a}_1 E_0, \ldots, E_{S-1} = \mathfrak{a}_{S-1} E_0)$, the challenge is sampled from $\{-S+1, \ldots, S-1\}$ and the underlying sigma protocol is repeated t times (see section 2.4 for further details). Without loss of generality, we can assume that the secret ideals $\mathfrak{a}_i$ are the shortest in their class, which means that their respective norms n_i are bounded by $\sqrt{p}$. Following a result for Hardy and Ramanujan [43], one expects n_i to have be of the form $n_i = \prod_{j=1}^{e_i} p_{ij}^{e_{ij}}$ where $e_i \approx \log\log n_i \approx \log(\frac{1}{2}\log p) \approx \log\log p - 1$. We can hence represent the ideal $\mathfrak{a}_i$ as $((p_{ij})_j, (\epsilon_i e_{ij})_j)$ where $\epsilon_j \in \{-1, 1\}$ defines the choice of the eigen value of Frobenius moduli p_{ij}. Hence the ideal $\mathfrak{a}_i$ can be represented using about $\frac{1}{2}\log p + (\log\log p)^2$ bits.

The public key in Generalised CSI-FiSh is made up of $S-1$ curves defined over $\mathbb{F}_p$, hence it can be represented using $(S-1)\log p$ bits. The challenge is made up of t elements in $\{-S+1, \ldots, S-1\}$, hence it can be represented with $t\log(2S-1)$ bits. The response is made up of t ideals, hence it can be represented using $t(\frac{1}{2}\log p + (\log\log p)^2)$ bits. It follows that the signature can be represented using $t(\log(2S-1) + \frac{1}{2}\log p + (\log\log p)^2)$ bits.

SQI-FiSh uses the same parameters as Generalised CSI-FiSh and has the same key and signature sizes. Only the way the signer evaluates isogeny group actions differs as the signer in SQI-FiSh uses Qlapoti while the signer in Generalised CSI-FiSh uses PEGASIS.

6.4 Implementation and comparison.

In Table 5, we provide a theoretical comparison between Generalised CSI-FiSh, SQI-FiSh, WaterSQI and PRISMO for a generic prime p. Table 1 specialises Table 5 to the case where the 2031 bits prime p_{2000} is used. Relying on the code of Qlapoti [12, §5] and on the code of qt-PEGASIS [27, §5], we did a proof of concept implementation of PRISMO and Generalised CSI-FiSh in Sagemath. The average runtimes of both schemes when instantiated with the primes p_{500}, p_{1000} and p_{2000} are provided in Table 4.

Acknowledgements. We thank the anonymous reviewers of Eurocrypt 2026 for their detailed comments and suggestions that helped improve the quality of this paper. We thank Steven Galbraith and Fre Vercauteren for useful comments on a very early version of the WaterSQI protocol. We would also like to thank Antonin Leroux and the PQarrots team for helpful discussions, and Wouter Castryck for suggesting the name WaterSQI.

References

1. Aardal, M.A., Adj, G., Aranha, D.F., Basso, A., Canales Martínez, I.A., Chávez-Saab, J., Corte-Real Santos, M., Dartois, P., De Feo, L., Duparc, M., Eriksen, J.K., Fouotsa, T.B., Gazzoni Filho, D.L., Hess, B., Kohel, D., Leroux, A., Longa, P., Maino, L., Meyer, M., Nakagawa, K., Onuki, H., Panny, L., Patranabis, S., Petit, C., Pope, G., Reijnders, K., Robert, D., Rodríguez-Henríquez, F., Schaeffler, S., Wesolowski, B.: SQIsign. Tech. rep., National Institute of Standards and Technology (2025), https://sqisign.org
2. Aardal, M.A., Atapoor, S., Baghery, K., Basso, A., Bonnetain, X., Borin, G., De Feo, L., Cozzo, D., Dartois, P., Duparc, M., Eriksen, J.K., Fouotsa, T.B., Herlédan Le Merdy, A., Invernizzi, R., Jaques, S., Lazzarini, D., LeGrow, J.T., Martindale, C., Maino, L., Meers, J., Meyer, M., Patranabis, S., Pedersen, R., Pope, G., Riepel, D., Robert, D., Rueger, R., Sina Schaeffler, A., Schrottenloher, Vercauteren, F.: PQarrots: Macaw, Kea and Kakapo. Preview Writeup, NIST Multi-Party Threshold Cryptography (MPTC) (2026), https://csrc.nist.gov/csrc/media/Projects/threshold-cryptography/documents/TCall-1/PQarrots-PW01.pdf
3. Allombert, B., Biasse, J.F., Eriksen, J.K., Kutas, P., Leonardi, C., Page, A., Scheidler, R., Bagi, M.T.: PEARL-SCALLOP: Parameter extension applicable in real-life SCALLOP. Cryptology ePrint Archive, Paper 2024/1744 (2024), https://eprint.iacr.org/2024/1744
4. Basso, A., Borin, G., Castryck, W., Corte-Real Santos, M., Invernizzi, R., Leroux, A., Maino, L., Vercauteren, F., Wesolowski, B.: PRISM: Simple and Compact Identification and Signatures from Large Prime Degree Isogenies. In: Jager, T., Pan, J. (eds.) Public-Key Cryptography – PKC 2025. pp. 300–332. Springer Nature Switzerland, Cham (2025), https://doi.org/10.1007/978-3-031-91826-1_10
5. Basso, A., Codogni, G., Connolly, D., De Feo, L., Fouotsa, T.B., Lido, G.M., Morrison, T., Panny, L., Patranabis, S., Wesolowski, B.: Supersingular Curves You Can Trust. In: Hazay, C., Stam, M. (eds.) Advances in Cryptology – EUROCRYPT 2023. pp. 405–437. Springer Nature Switzerland, Cham (2023), https://doi.org/10.1007/978-3-031-30617-4_14
6. Basso, A., Dartois, P., De Feo, L., Leroux, A., Maino, L., Pope, G., Robert, D., Wesolowski, B.: SQIsign2D-West - the fast, the small, and the safer. In: Chung, K.M., Sasaki, Y. (eds.) ASIACRYPT 2024, Part III. LNCS, vol. 15486, pp. 339–370. Springer, Singapore (Dec 2024). https://doi.org/10.1007/978-981-96-0891-1_11
7. Bernstein, D.J., De Feo, L., Leroux, A., Smith, B.: Faster computation of isogenies of large prime degree. Open Book Series **4**(1), 39–55 (2020)
8. Bernstein, D.J., Lange, T., Martindale, C., Panny, L.: Quantum circuits for the CSIDH: Optimizing quantum evaluation of isogenies. In: Ishai, Y., Rijmen, V. (eds.) EUROCRYPT 2019, Part II. LNCS, vol. 11477, pp. 409–441. Springer, Cham (May 2019). https://doi.org/10.1007/978-3-030-17656-3_15
9. Beullens, W., Kleinjung, T., Vercauteren, F.: CSI-FiSh: Efficient isogeny based signatures through class group computations. In: Galbraith, S.D., Moriai, S. (eds.) ASIACRYPT 2019, Part I. LNCS, vol. 11921, pp. 227–247. Springer, Cham (Dec 2019). https://doi.org/10.1007/978-3-030-34578-5_9
10. Bonnetain, X., Schrottenloher, A.: Quantum security analysis of CSIDH. In: Canteaut, A., Ishai, Y. (eds.) EUROCRYPT 2020, Part II. LNCS, vol. 12106, pp. 493–522. Springer, Cham (May 2020). https://doi.org/10.1007/978-3-030-45724-2_17

11. Booher, J., Bowden, R., Doliskani, J., Boris Fouotsa, T., Galbraith, S.D., Kunzweiler, S., Merz, S.P., Petit, C., Smith, B., Stange, K.E., Ti, Y.B., Vincent, C., Voloch, J.F., Weitkämper, C., Zobernig, L.: Failing to hash into supersingular isogeny graphs. The Computer Journal **67**(8), 2702–2719 (05 2024). https://doi.org/10.1093/comjnl/bxae038, https://doi.org/10.1093/comjnl/bxae038
12. Borin, G., Corte-Real Santos, M., Eriksen, J.K., Invernizzi, R., Mula, M., Schaeffler, S., Vercauteren, F.: Qlapoti: Simple and Efficient Translation of Quaternion Ideals to Isogenies. In: Hanaoka, G., Yang, B.Y. (eds.) Advances in Cryptology – ASIACRYPT 2025. pp. 174–205. Springer Nature Singapore, Singapore (2026), https://doi.org/10.1007/978-981-95-5113-2_6
13. Borin, G., Persichetti, E., Pintore, F., Reijnders, K., Santini, P.: A Guide to the Design of Digital Signatures based on Cryptographic Group Actions. Journal of Cryptology **38**(3), 23 (2025), https://doi.org/10.1007/s00145-025-09542-9
14. Bruno, G., Corte-Real Santos, M., Costello, C., Eriksen, J.K., Meyer, M., Naehrig, M., Sterner, B.: Cryptographic smooth neighbors. In: Guo, J., Steinfeld, R. (eds.) ASIACRYPT 2023, Part VII. LNCS, vol. 14444, pp. 190–221. Springer, Singapore (Dec 2023). https://doi.org/10.1007/978-981-99-8739-9_7
15. Castryck, W., Decru, T.: CSIDH on the surface. In: Ding, J., Tillich, J.P. (eds.) Post-Quantum Cryptography - 11th International Conference, PQCrypto 2020. pp. 111–129. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-44223-1_7
16. Castryck, W., Decru, T.: An efficient key recovery attack on SIDH. In: Hazay, C., Stam, M. (eds.) EUROCRYPT 2023, Part V. LNCS, vol. 14008, pp. 423–447. Springer, Cham (Apr 2023). https://doi.org/10.1007/978-3-031-30589-4_15
17. Castryck, W., Lange, T., Martindale, C., Panny, L., Renes, J.: CSIDH: An efficient post-quantum commutative group action. In: Peyrin, T., Galbraith, S. (eds.) ASIACRYPT 2018, Part III. LNCS, vol. 11274, pp. 395–427. Springer, Cham (Dec 2018). https://doi.org/10.1007/978-3-030-03332-3_15
18. Castryck, W., Panny, L., Vercauteren, F.: Rational isogenies from irrational endomorphisms. In: Canteaut, A., Ishai, Y. (eds.) EUROCRYPT 2020, Part II. LNCS, vol. 12106, pp. 523–548. Springer, Cham (May 2020). https://doi.org/10.1007/978-3-030-45724-2_18
19. Chávez-Saab, J., Chi-Domínguez, J.J., Jaques, S., Rodríguez-Henríquez, F.: The SQALE of CSIDH: sublinear Vélu quantum-resistant isogeny action with low exponents. Journal of Cryptographic Engineering **12**(3), 349–368 (2022), https://doi.org/10.1007/s13389-021-00271-w
20. Chen, M., Leroux, A., Panny, L.: SCALLOP-HD: Group action from 2-dimensional isogenies. In: Tang, Q., Teague, V. (eds.) PKC 2024, Part II. LNCS, vol. 14603, pp. 190–216. Springer, Cham (Apr 2024). https://doi.org/10.1007/978-3-031-57725-3_7
21. Chen, M., Petit, C.: Computing the endomorphism ring of a supersingular elliptic curve from a full rank suborder. In: Fehr, S., Fouque, P.A. (eds.) EUROCRYPT 2025, Part VI. LNCS, vol. 15606, pp. 446–474. Springer, Cham (May 2025). https://doi.org/10.1007/978-3-031-91095-1_16
22. Colò, L., Kohel, D.: Orienting supersingular isogeny graphs. Journal of Mathematical Cryptology **14**(1), 414–437 (2020). https://doi.org/doi:10.1515/jmc-2019-0034, https://doi.org/10.1515/jmc-2019-0034
23. Corte-Real Santos, M., Eriksen, J.K., Meyer, M., Reijnders, K.: AprèsSQI: Extra fast verification for SQIsign using extension-field signing. In: Joye, M., Leander, G. (eds.) EUROCRYPT 2024, Part I. LNCS, vol. 14651, pp. 63–93. Springer, Cham (May 2024). https://doi.org/10.1007/978-3-031-58716-0_3

24. Costello, C.: B-SIDH: Supersingular isogeny Diffie-Hellman using twisted torsion. In: Moriai, S., Wang, H. (eds.) ASIACRYPT 2020, Part II. LNCS, vol. 12492, pp. 440–463. Springer, Cham (Dec 2020). https://doi.org/10.1007/978-3-030-64834-3_15
25. Costello, C., Meyer, M., Naehrig, M.: Sieving for twin smooth integers with solutions to the prouhet-tarry-escott problem. In: Canteaut, A., Standaert, F.X. (eds.) EUROCRYPT 2021, Part I. LNCS, vol. 12696, pp. 272–301. Springer, Cham (Oct 2021). https://doi.org/10.1007/978-3-030-77870-5_10
26. Dartois, P., Eriksen, J.K., Fouotsa, T.B., Merdy, A.H.L., Invernizzi, R., Robert, D., Rueger, R., Vercauteren, F., Wesolowski, B.: PEGASIS: Practical effective class group action using 4-dimensional isogenies. In: Kalai, Y.T., Kamara, S.F. (eds.) CRYPTO 2025, Part I. LNCS, vol. 16000, pp. 67–99. Springer, Cham (Aug 2025). https://doi.org/10.1007/978-3-032-01855-7_3
27. Dartois, P., Eriksen, J.K., Invernizzi, R., Vercauteren, F.: qt-Pegasis: Simpler and Faster Effective Class Group Actions. To appear at Eurocrypt 2026, https://eprint.iacr.org/2025/1859
28. Dartois, P., Leroux, A., Robert, D., Wesolowski, B.: SQIsignHD: New dimensions in cryptography. In: Joye, M., Leander, G. (eds.) EUROCRYPT 2024, Part I. LNCS, vol. 14651, pp. 3–32. Springer, Cham (May 2024). https://doi.org/10.1007/978-3-031-58716-0_1
29. De Feo, L., Fouotsa, T.B., Kutas, P., Leroux, A., Merz, S.P., Panny, L., Wesolowski, B.: SCALLOP: Scaling the CSI-FiSh. In: Boldyreva, A., Kolesnikov, V. (eds.) Public-Key Cryptography – PKC 2023. pp. 345–375. Springer Nature Switzerland, Cham (2023), https://doi.org/10.1007/978-3-031-31368-4_13
30. De Feo, L., Galbraith, S.D.: SeaSign: Compact isogeny signatures from class group actions. In: Ishai, Y., Rijmen, V. (eds.) EUROCRYPT 2019, Part III. LNCS, vol. 11478, pp. 759–789. Springer, Cham (May 2019). https://doi.org/10.1007/978-3-030-17659-4_26
31. De Feo, L., Jao, D., Plût, J.: Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. Journal of Mathematical Cryptology (2014), https://doi.org/10.1515/jmc-2012-0015
32. 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.) ASIACRYPT 2020, Part I. LNCS, vol. 12491, pp. 64–93. Springer, Cham (Dec 2020). https://doi.org/10.1007/978-3-030-64837-4_3
33. 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.) EUROCRYPT 2023, Part V. LNCS, vol. 14008, pp. 659–690. Springer, Cham (Apr 2023). https://doi.org/10.1007/978-3-031-30589-4_23
34. Delfs, C., Galbraith, S.D.: Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$. DCC **78**(2), 425–440 (2016). https://doi.org/10.1007/s10623-014-0010-1
35. Deuring, M.: Die typen der multiplikatorenringe elliptischer funktionenkörper: G. herglotz zum 60. geburtstag gewidmet. In: Abhandlungen aus dem mathematischen Seminar der Universität Hamburg. vol. 14, pp. 197–272. Springer (1941)
36. Duparc, M., Fouotsa, T.B.: SQIPrime: A dimension 2 variant of SQISignHD with non-smooth challenge isogenies. In: Chung, K.M., Sasaki, Y. (eds.) ASIACRYPT 2024, Part III. LNCS, vol. 15486, pp. 396–429. Springer, Singapore (Dec 2024). https://doi.org/10.1007/978-981-96-0891-1_13

37. Eisentraeger, K., Scullard, G.: Connecting kani's lemma and path-finding in the bruhat-tits tree to compute supersingular endomorphism rings (2026), https://arxiv.org/abs/2402.05059
38. Fouotsa, T.B.: WaterSQI and PRISMO: Quaternion Signatures for Supersingular Isogeny Group Actions. Cryptology ePrint Archive, Paper 2025/1737 (2025), https://eprint.iacr.org/archive/2025/1737/20260223:211757
39. Fouotsa, T.B.: WaterSQI and PRISMO: Quaternion Signatures for Supersingular Isogeny Group Actions. In: Advances in Cryptology – EUROCRYPT 2026: 45th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Rome, Italy, May 10–14, 2026, Proceedings, Part IV. p. 573–603. Springer-Verlag, Berlin, Heidelberg (2026). https://doi.org/10.1007/978-3-032-25327-9_20, https://doi.org/10.1007/978-3-032-25327-9_20
40. Galbraith, S.D., Petit, C., Silva, J.: Identification protocols and signature schemes based on supersingular isogeny problems. In: Takagi, T., Peyrin, T. (eds.) ASIACRYPT 2017, Part I. LNCS, vol. 10624, pp. 3–33. Springer, Cham (Dec 2017). https://doi.org/10.1007/978-3-319-70694-8_1
41. Goldreich, O., Micali, S., Wigderson, A.: Proofs that yield nothing but their validity or all languages in np have zero-knowledge proof systems. J. ACM **38**(3), 690–728 (Jul 1991), https://doi.org/10.1145/116825.116852
42. Hafner, J.L., McCurley, K.S.: A rigorous subexponential algorithm for computation of class groups. Journal of the American mathematical society **2**(4), 837–850 (1989)
43. Hardy, G.H., Ramanujan, S.: The normal number of prime factors of a number n. Quarterly Journal of Mathematics, 48: 76-92 (1917)
44. Jao, D., Azarderakhsh, R., Campagna, M., Costello, C., Feo, L.D., Hess, B., Hutchinson, A., Jalali, A., Karabina, K., Koziel, B., LaMacchia, B., Longa, P., Naehrig, M., Pereira, G., Renes, J., Soukharev, V., Urbanik, D.: Supersingular Isogeny Key Encapsulation (October 1, 2020), https://sike.org/files/SIDH-spec.pdf
45. 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), https://doi.org/10.1007/978-3-642-25405-5_2
46. Kani, E.: The number of curves of genus two with elliptic differentials. Walter de Gruyter, Berlin/New York Berlin, New York (1997)
47. Kohel, D., Lauter, K., Petit, C., Tignol, J.P.: On the quaternion ℓ-isogeny path problem. LMS Journal of Computation and Mathematics **17**(A), 418–432 (2014), https://doi.org/10.1112/S1461157014000151
48. Maino, L., Martindale, C., Panny, L., Pope, G., Wesolowski, B.: A direct key recovery attack on SIDH. In: Hazay, C., Stam, M. (eds.) EUROCRYPT 2023, Part V. LNCS, vol. 14008, pp. 448–471. Springer, Cham (Apr 2023). https://doi.org/10.1007/978-3-031-30589-4_16
49. Mokrani, Y., Jao, D.: Generating supersingular elliptic curves over $\mathbb{F}_p$ with unknown endomorphism ring. In: Chattopadhyay, A., Bhasin, S., Picek, S., Rebeiro, C. (eds.) INDOCRYPT 2023, Part I. LNCS, vol. 14459, pp. 159–174. Springer, Cham (Dec 2023). https://doi.org/10.1007/978-3-031-56232-7_8
50. Mula, M., Murru, N., Pintore, F.: On random sampling of supersingular elliptic curves. Annali di Matematica Pura ed Applicata (1923-) **204**(3), 1293–1335 (2025), https://doi.org/10.1007/s10231-024-01528-x
51. Nakagawa, K., Onuki, H.: QFESTA: Efficient algorithms and parameters for FESTA using quaternion algebras. In: Reyzin, L., Stebila, D. (eds.) CRYPTO 2024,

Part V. LNCS, vol. 14924, pp. 75–106. Springer, Cham (Aug 2024). https://doi.org/10.1007/978-3-031-68388-6_4
52. Nakagawa, K., Onuki, H.: Attacks on PRISM-id via torsion over small extension fields. Cryptology ePrint Archive, Paper 2025/1602 (2025), https://eprint.iacr.org/2025/1602
53. 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
54. 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.) ASIACRYPT 2024, Part III. LNCS, vol. 15486, pp. 272–303. Springer, Singapore (Dec 2024). https://doi.org/10.1007/978-981-96-0891-1_9
55. Onuki, H.: On oriented supersingular elliptic curves. Finite Fields and Their Applications **69**, 101777 (2021). https://doi.org/https://doi.org/10.1016/j.ffa.2020.101777
56. Page, A., Robert, D.: Introducing clapoti(s): Evaluating the isogeny class group action in polynomial time. Cryptology ePrint Archive, Report 2023/1766 (2023), https://eprint.iacr.org/2023/1766
57. Panny, L., Petit, C., Stopar, M.: KLaPoTi: An asymptotically efficient isogeny group action from 2-dimensional isogenies. Cryptology ePrint Archive, Paper 2024/1844 (2024), https://eprint.iacr.org/2024/1844
58. Peikert, C.: He gives C-sieves on the CSIDH. In: Canteaut, A., Ishai, Y. (eds.) EUROCRYPT 2020, Part II. LNCS, vol. 12106, pp. 463–492. Springer, Cham (May 2020). https://doi.org/10.1007/978-3-030-45724-2_16
59. Robert, D.: Evaluating isogenies in polylogarithmic time. Cryptology ePrint Archive, Paper 2022/1068 (2022), https://eprint.iacr.org/2022/1068
60. Robert, D.: Breaking SIDH in polynomial time. In: Hazay, C., Stam, M. (eds.) EUROCRYPT 2023, Part V. LNCS, vol. 14008, pp. 472–503. Springer, Cham (Apr 2023). https://doi.org/10.1007/978-3-031-30589-4_17
61. Shor, P.W.: Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings 35th Annual Symposium on Foundations of Computer Science. pp. 124–134 (1994)
62. Vélu, J.: Isogénies entre courbes elliptiques. Comptes-Rendus de l'Académie des Sciences **273**, 238–241 (1971)
63. Wesolowski, B.: Orientations and the supersingular endomorphism ring problem. In: Dunkelman, O., Dziembowski, S. (eds.) EUROCRYPT 2022, Part III. LNCS, vol. 13277, pp. 345–371. Springer, Cham (May / Jun 2022). https://doi.org/10.1007/978-3-031-07082-2_13
64. Xu, Z., Lin, K., Zhao, C.A., Ouyang, Y.: SQIsign2D^2: New SQIsign2D variant by leveraging power smooth isogenies in dimension one. Cryptology ePrint Archive, Paper 2025/920 (2025), https://eprint.iacr.org/2025/920

A Towards WaterSQI

In this section, we provide some intuition regarding the design choices made in WaterSQI. This hopefully gives a general idea on why the scheme is secure. Recall that the secret isogeny $\tau := \tau_{\mathfrak{a}} : E_0 \to E_A$ is $\mathbb{F}_p$-rational, that the hard

relation for our sigma protocol is

$$\mathcal{R}_p = \{(E, w), E/\mathbb{F}_p \text{ supersingular}, w \in \mathrm{End}(E) \setminus \mathrm{End}_{\mathbb{F}_p}(E)\}.$$

The commitment isogeny is $\psi : E_0 \to E_1$, the challenge isogeny is $\varphi : E_A \to E_2$ and the response isogeny is $\sigma : E_1 \to E_2$. The transcript is (E_1, φ, σ).

A.1 Requirement on the commitment curve E_1

Our first requirement is that the commitment curve E_1 should not be defined over $\mathbb{F}_p$. In fact, as the public key curve E_A is defined over $\mathbb{F}_p$, one is tempted to exploit the fact that ideal to isogeny and isogeny to ideal translations are quite straightforward for $\mathbb{F}_p$-rational isogenies. In that sense, one may want to replace the commitment isogeny $\psi : E_0 \to E_1$ and the challenge isogeny $\varphi : E_A \to E_2$ with $\mathbb{F}_p$-rational isogenies $\psi_{\mathfrak{b}} : E_0 \to E_1$ and $\varphi_{\mathfrak{c}} : E_A \to E_2$ respectively. One then samples a random response isogeny $\sigma : E_1 \to E_2$ and returns its representation as the response. Then comes the question:

What is the nature of the response isogeny $\sigma : E_1 \to E_2$?

In fact, this isogeny can either be $\mathbb{F}_p$-rational, or not. We discuss both cases and show that in the earlier case the extraction will fail, while in the latter the scheme is not zero-knowledge.

Case 1: σ is an $\mathbb{F}_p$-rational isogeny. Assume that $\sigma : E_1 \to E_2$ is an $\mathbb{F}_p$-rational isogeny. Then $\widehat{\sigma} \circ \varphi_{\mathfrak{c}} : E_A \longrightarrow E_1$ is an $\mathbb{F}_p$-rational isogeny. For knowledge soundness, given two transcripts $(E_1, \varphi_{\mathfrak{c}}, \sigma)$ and $(E_1, \varphi_{\mathfrak{c}'}, \sigma')$ with the same commitment curve E_1 but different challenges $\varphi_{\mathfrak{c}} \neq \varphi_{\mathfrak{c}'}$, one can extract a representation of non-trivial endomorphism $\alpha = \widehat{\varphi_{\mathfrak{c}'}} \circ \sigma' \circ \widehat{\sigma} \circ \varphi_{\mathfrak{c}}$ of E_A.

The issue here is that since the isogenies $\widehat{\sigma} \circ \varphi_{\mathfrak{c}}$ and $\widehat{\varphi_{\mathfrak{c}'}} \circ \sigma'$ are $\mathbb{F}_p$-rational, then α is also $\mathbb{F}_p$-rational, which means that α lies in $\mathrm{End}_{\mathbb{F}_p}(E_A)$. This clearly suggests that the knowledge of the full endomorphism ring of E_A (or an isogeny connecting E_A to E_0) is not required when producing valid signatures. In fact, a malicious prover who does not know any isogeny $E_0 \to E_A$ could cheat by proceeding as follows. He computes the commitment curve E_1 by sampling an $\mathbb{F}_p$-rational isogeny $\psi_{\mathfrak{b}} : E_A \longrightarrow E_1$, and when given a challenge isogeny $\varphi_{\mathfrak{c}} : E_A \longrightarrow E_2$, he finds a short ideal $\mathfrak{d}$ equivalent to $\mathfrak{b}^{-1}\mathfrak{c}$ returns the isogeny (can be computed using PEGASIS) corresponding to $\mathfrak{d}$ as the response. This process only requires the knowledge of $\mathrm{End}_{\mathbb{F}_p}(E_A) = \mathbb{Z}[\pi]$, which is public.

Case 2: σ is not an $\mathbb{F}_p$-rational isogeny. Assume that the response isogeny $\sigma : E_1 \longrightarrow E_2$ is not $\mathbb{F}_p$-rational. Let $\sigma^{(p)} : E_1 \to E_2$ be the isogeny whose kernel is $\ker \sigma^{(p)} = \pi(\ker \sigma)$. The isogeny $\sigma^{(p)}$ is called the Frobenius conjugate of the isogeny σ. Since σ is defined over $\mathbb{F}_{p^2}$ (and not over $\mathbb{F}_p$), then $\pi(\ker \sigma) \neq \ker \sigma$, implying that $\sigma^{(p)} \neq \sigma$. Consider the non trivial endomorphism $\alpha = \sigma^{(p)} \circ \widehat{\sigma} \in \mathrm{End}(E_2)$. Then we have the following lemma.

Lemma 23. *Let E_1 and E_2 be supersingular curves defined over $\mathbb{F}_p$ and let $\phi : E_1 \longrightarrow E_2$ be a degree d supersingular isogeny defined over $\mathbb{F}_{p^2}$ and not over $\mathbb{F}_p$. Let $\phi^{(p)} : E_1 \longrightarrow E_2$ be its Frobenius conjugate. Then $\alpha = \phi^{(p)} \circ \widehat{\phi} \in \mathrm{End}(E_2)$ is endomorphism of E_2 defined over $\mathbb{F}_{p^2}$ and not over not over $\mathbb{F}_p$.*

Proof. All supersingular isogenies are defined over $\mathbb{F}_{p^2}$, hence we only need to prove that the endomorphism $\alpha = \phi^{(p)} \circ \widehat{\phi} \in \mathrm{End}(E_2)$ is not defined over $\mathbb{F}_p$. We will proceed by contradiction. Let us assume that α is defined over $\mathbb{F}_p$. Since ϕ is defined over $\mathbb{F}_{p^2}$ (and not over $\mathbb{F}_p$), then $\ker \phi^{(p)} = \pi(\ker \phi) \neq \ker \phi$, implying that $\alpha = \phi^{(p)} \circ \widehat{\phi} \in \mathrm{End}(E_2)$ is a non scalar endomorphism.

Firstly, let us assume that ϕ does not factor through any $\mathbb{F}_p$-rational isogeny, meaning that no non-trivial subgroup of $\ker \phi$ is fixed by the Frobenius. Then it follows that α is cyclic. Since α is defined over $\mathbb{F}_p$, then $\ker \alpha$ is fixed by Frobenius. Since $\ker \alpha$ is a cyclic group of order d^2 where $d = \deg \phi$, then it admits a unique subgroup of order d. We have that $\ker \widehat{\phi}$ is an order d subgroup of $\ker \alpha$, and $\pi(\ker \widehat{\phi})$ is also an order d subgroup of $\pi(\ker \alpha) = \ker \alpha$. It follows that $\ker \widehat{\phi} = \pi(\ker \widehat{\phi})$ is the unique subgroup of $\ker \alpha$ of order d. This means that $\widehat{\phi}$ is an $\mathbb{F}_p$-rational isogeny, implying that ϕ is an $\mathbb{F}_p$-rational isogeny. This leads to a contradiction.

Now, if $\ker \phi$ has a non-trivial subgroup which is fixed by the Frobenius, then α is not cyclic. Nevertheless, ϕ and $\phi^{(p)}$ factor through the same $\mathbb{F}_p$-rational isogeny $\phi_1 : E_1 \to E_1'$, such that no non-trivial subgroup of the kernel of $\phi_2 : E_1' \to E_2$ is fixed by the Frobenius. Set $\alpha' = \phi_2^{(p)} \circ \widehat{\phi_2} \in \mathrm{End}(E_2)$, then α' is cyclic. If α' were to be $\mathbb{F}_p$-rational, then from the earlier case, we would get that ϕ_2 is $\mathbb{F}_p$-rational, meaning that $\phi = \phi_2 \circ \phi_1$ is $\mathbb{F}_p$-rational, which is a contradiction. Hence α' is not $\mathbb{F}_p$-rational, which implies that $\alpha = [\deg \phi_1]\alpha'$ is not $\mathbb{F}_p$-rational. □

By Lemma 23, when the response isogeny $\sigma : E_1 \longrightarrow E_2$ is defined over $\mathbb{F}_{p^2}$, a single execution of the protocol allows an adversary to recover a non trivial endomorphism $\alpha = \sigma^{(p)} \circ \widehat{\sigma} \in \mathrm{End}(E_2) \setminus \mathrm{End}_{\mathbb{F}_p}(E_2)$. The commitment isogeny $\varphi_{\mathfrak{c}} : E_A \longrightarrow E_2$ can be used to pull back this endomorphism to E_A, meaning that each execution of the protocol allows any adversary to recover a non $\mathbb{F}_p$-rational endomorphism of E_A, implying that the protocol is not zero-knowledge. In only few executions, the full endomorphism ring of E_A is rapidly recovered. Note that the attacks presented here generalise to the case where E_2 is not defined over $\mathbb{F}_p$ but the commitment curve E_1 is. In fact, $\widehat{\sigma} \circ \varphi_{\mathfrak{c}}$ will either be an $\mathbb{F}_p$-rational isogeny and the extraction will fail, or it will not be a an $\mathbb{F}_p$-rational isogeny and a single signature will reveal a non $\mathbb{F}_p$-rational endomorphism of E_A.

In conclusion, the commitment curve E_1 must not be defined over $\mathbb{F}_p$. In the following sections, we show that E_1 being defined over $\mathbb{F}_{p^2}$ (and not over $\mathbb{F}_p$) is not sufficient to obtain a secure signature scheme.

A.2 Requirement on the challenge φ and the response σ

In the proof of 2-special soundness, when extracting the witness candidate $\alpha = \widehat{\varphi'} \circ \sigma' \circ \widehat{\sigma} \circ \varphi \in \mathrm{End}(E_A)$, it may happen that the response isogenies σ and σ' cancel out and we are left with $\alpha' = \widehat{\varphi'} \circ \varphi \in \mathrm{End}(E_A)$; or when reordering the isogenies in α as $\alpha = \sigma'^* \circ \widehat{\sigma^*} \circ \widehat{\varphi'^*} \circ \varphi$, $\widehat{\varphi'^*}$ and φ cancel out and we are left with $\alpha' = \sigma'^* \circ \widehat{\sigma^*} \in \mathrm{End}(E_A)$. In both cases, after proving that α' is not a scalar, we need to prove that α' is not an $\mathbb{F}_p$-rational endomorphism of E_A. Requirements 2 and 3 enable us to produce such a proof.

The requirement that φ should not "trivially" factor through an $\mathbb{F}_p$-rational isogeny, enables us to prove that when the response isogenies σ and σ' cancel out, $\alpha' = \widehat{\varphi'} \circ \varphi \in \mathrm{End}(E_A)$ is not $\mathbb{F}_p$-rational. Intuitively, since the degree of α' is a prime power, after removing the non cyclic part of α', the first step of α' is equal to that of φ, that is $1_{\alpha'} = 1_\varphi$. Choosing 1_φ to not be $\mathbb{F}_p$-rational ensures that $1_{\alpha'}$ is not $\mathbb{F}_p$-rational, hence α' is also not $\mathbb{F}_p$-rational.

The requirement that the degree d of the response isogeny σ is bounded by $\sqrt{p}$ enables us to prove that when $\widehat{\varphi'^*}$ and φ cancel out after a reordering of the isogenies in α, $\alpha' = \sigma'^* \circ \widehat{\sigma^*} \in \mathrm{End}(E_A)$ is not $\mathbb{F}_p$-rational. Intuitively, if α' were $\mathbb{F}_p$-rational, we would get $\alpha' = u + v\pi$, $\deg \alpha' = u^2 + v^2 p < p$, implying that $\alpha' = u \in \mathbb{Z}$ which is a contradiction. Nevertheless, we would not like the response isogeny to backtrack the challenge isogeny, as it would reduce the resulting challenge space. When enforcing $\deg(\sigma) < \sqrt{p}$, it is very likely that in some cases, it is not possible to find such a response isogeny which does not backtrack the challenge isogeny. We hence increase the degree of the challenge isogeny by few bits $n_{\mathsf{bt}} < e - \lambda$ and allow the the response isogeny is to backtrack the challenge isogeny by up to n_{bt} steps.

B PRISMO$_2$: A different design choice for PRISMO

As an alternative design for PRISMO, instead of requiring that q is inert in $\mathfrak{O} \simeq \mathbb{Z}[\pi]$, we allow q to be any prime in Primes_u as in PRISM and make use of the following lemma when q is not inert.

Lemma 24. *Let E be a supersingular elliptic curve defined over $\mathbb{F}_p$, and let $\phi : E \to E'$ be a supersingular q-isogeny and let $N^2 > 4q$ an integer coprime with the characteristic p. Then ϕ is $\mathbb{F}_p$-rational if and only if $j(E') \in \mathbb{F}_p$ and $\pi_{E'} \circ \varphi(P) = \varphi \circ \pi_E(P)$ for all $P \in E[N]$.*

Proof. If ϕ is $\mathbb{F}_p$-rational, then $j(E') \in \mathbb{F}_p$ and $\pi_{E'} \circ \varphi = \varphi \circ \pi_E$, hence $\pi_{E'} \circ \varphi(P) = \varphi \circ \pi_E(P)$ for all $P \in E[N]$. Now, let us assume that $j(E') \in \mathbb{F}_p$ and $\pi_{E'} \circ \varphi(P) = \varphi \circ \pi_E(P)$ for all $P \in E[N]$. We need to show that $\pi_{E'} \circ \varphi = \varphi \circ \pi_E$. We know that $\pi_{E'} \circ \varphi = \varphi^{(p)} \circ \pi_E$ where $\ker \varphi^{(p)} = \pi_E(\ker \varphi)$, hence $\varphi \circ \pi_E(P) = \varphi^{(p)} \circ \pi_E(P)$ for all $P \in E[N]$, that is $(\varphi - \varphi^{(p)}) \circ \pi_E(P) = 0$ for all $P \in E[N]$. Since π_E is a group isomorphism when restricted to $E[N]$, then $E[N] \subset \ker(\varphi - \varphi^{(p)})$. Since $\deg(\varphi - \varphi^{(p)}) \leq 4 \deg \varphi = 4q < N^2 = \#E[N]$ (Cauchy Schwarz inequality), then $\varphi = \varphi^{(p)}$ and $\pi_{E'} \circ \varphi = \varphi \circ \pi_E$. This proves that φ is $\mathbb{F}_p$-rational. □

Lemma 24 allows us to describe PRISMO$_2$, an alternative design for PRISMO which is as follows. This time, the challenge is a large prime q as in PRISM. The response is a $q(2^u - q)$-isogeny $\sigma : E \to E'$ which can be written as $\sigma = \sigma_2 \circ \sigma_1$ with $\deg \sigma_1 = q$ and $\deg \sigma_2 = 2^u - q$. The isogeny σ is such that σ_1 is not $\mathbb{F}_p$-rational. During the verification, one verifies that $\sigma : E \to E'$ is an isogeny of degree $q(2^u - q)$, and that $\sigma = \sigma_2 \circ \sigma_1$ is such that $\deg \sigma_1 = q$ and σ_1 is not $\mathbb{F}_p$-rational. The PRISMO$_2$ identification scheme hence makes use of the following algorithms:

- $\sigma \leftarrow \mathsf{GenIsogeny}_{\mathsf{O}}(E, \phi, q)$ which takes a supersingular curve E, an isogeny $\phi : E_0 \to E$ and a large prime q as inputs, and returns a representation of an isogeny $\varphi : E \to E'$ of degree $q(2^u - q)$ which is uniformly distributed among isogenies $\varphi = \varphi_2 \circ \varphi_1$ of degree $q(2^u - q)$ from E such that φ_1 of degree q is not $\mathbb{F}_p$-rational. Since a random q-isogeny is $\mathbb{F}_p$-rational with probability at most $2/q$, then it suffices to generate a uniformly random $q(2^u - q)$-isogeny φ and to double-check[4] that φ_1 is not $\mathbb{F}_p$-rational. If one is unluckiest person on earth and φ_1 is $\mathbb{F}_p$-rational, one generates a new random isogeny φ.
- $\mathsf{accept/reject} \leftarrow \mathsf{VerIsogeny}_{\mathsf{O}}(\sigma, E, q)$ which takes a representation of an isogeny $\sigma : E \to E'$ and returns accept if its degree is $q(2^u - q)$ and it factors as $\sigma = \sigma_2 \circ \sigma_1$ where $\deg \sigma_1 = q$ and σ_1 is not $\mathbb{F}_p$-rational; reject if not. To verify that $\sigma_1 : E \to E_1$ is not $\mathbb{F}_p$-irrational, one first checks whether $j(E_1) \notin \mathbb{F}_p$. When $j(E_1) \notin \mathbb{F}_p$, then σ_1 is not $\mathbb{F}_p$ rational because it is a prime degree isogeny. When $j(E_1) \in \mathbb{F}_p$, then following Lemma 24, then one checks whether there exists $P \in E[N]$ such that $\pi_{E_1} \circ \varphi(P) \neq \varphi \circ \pi_E(P)$ for some integer $N > 4q$. For the latter check, we use $N = 2^{u+2}$ and the check is only performed on two points P_1, P_2 that form a basis of $E[N]$ as the opposite statement $\pi_{E_1} \circ \varphi(P) = \varphi \circ \pi_E(P)$ extends to $E[N]$ by linearity. One then accepts if $\pi_{E_1} \circ \varphi(P_1) \neq \varphi \circ \pi_E(P_1)$ or $\pi_{E_1} \circ \varphi(P_2) \neq \varphi \circ \pi_E(P_2)$, and rejects if not. In practice, as q and the characteristic p are of cryptographic size, when σ_1 is not $\mathbb{F}_p$-rational, $j(E') \notin \mathbb{F}_p$ with negligible probability (roughly $1/\sqrt{p}$ if one assumes that E_1 behaves like a random supersingular curve). Hence we do not expect the verification algorithm to go beyond the check $j(E_1) \notin \mathbb{F}_p$ for valid signatures.

With the above modifications, one follows similar steps as in PRISMO to obtain a digital signature whose security can be proven (by adapting that of [4, Prop. 2]) after adjusting the SPEDIO oracle and the underlying hard problem as summarised bellow.

Definition 25. *SPEDIO$_{\mathsf{O}_2}$ is an oracle which takes as input a supersingular elliptic curve E defined over $\mathbb{F}_p$ and a prime $q \in \mathsf{Primes}_u$, and returns a uniformly random cyclic isogeny φ of degree $q(2^u - q)$ from E where $\varphi = \varphi_2 \circ \varphi_1$ with φ_1 being a non $\mathbb{F}_p$-rational isogeny of degree q.*

[4] Note that in practice, one first generates a random ideal I of norm $q(2^u - q)$, then I is translated into an isogeny φ. Checking whether φ_1 is $\mathbb{F}_p$-rational or not can be done at the ideal level, which leads to the runtime of $\mathsf{GenIsogeny}_{\mathsf{O}}$ being practically the same as that of $\mathsf{GenIsogeny}$ for the same field size.

Problem 26. Given a random supersingular elliptic curve E defined over $\mathbb{F}_p$ and a $\mathrm{SPEDIO}_{\mathsf{O}_2}$, output an isogeny φ of degree $q'(2^u - q')$ with $q' \in \mathsf{Primes}_u$ different from all degrees q formerly generated by the oracle, and $\varphi = \varphi_2 \circ \varphi_1$ with φ_1 being a non $\mathbb{F}_p$-rational isogeny of degree q'.

Proposition 27. *If* $\mathsf{H}_{\mathsf{Prime}}$ *is a collision-resistant cryptographic hash function and Problem 26 is hard, then PRISMO*$_2$ *is EUF-CMA secure.*

C Tables

Name	Bitsize	Prime
p_{500}	508	$3 \cdot 11 \cdot 2^{503} - 1$
p_{1000}	1008	$3 \cdot 5 \cdot 2^{1004} - 1$
p_{2000}	2031	$3 \cdot 17 \cdot 2^{2026} - 1$

Table 2. The primes.

Prime	$\lvert\mathsf{pk}\rvert$	$\lvert\mathsf{sig}\rvert$	
		(Fast)WaterSQI	PRISMO
p_{500}	64	272	224
p_{1000}	128	528	352
p_{2000}	256	1040	608
$p \approx 2^{2\mu\lambda}$	$\mu\lambda/4$	$(\mu + 1/8)\lambda$	$(2\mu + 3)\lambda/4$

Table 3. Public key and signature sizes (in bytes) in (Fast)WaterSQI and in PRISMO. The public keys are identical in both schemes.

Protocol		p_{500}	p_{1000}	p_{2000}
PRISMO	KeyGen	0.603 s	2.179 s	11.087 s
	Sign	0.618 s	1.923 s	8.123 s
	Verify	0.133 s	0.213 s	0.442 s
Generalised CSI-FiSh $(2, 71, 15)$	KeyGen	0.875 s	2.35 s	9.17 s
	Sign	1.03 m	2.83 m	10.84 m
	Verify	1.03 m	2.82 m	10.73 m
Generalised CSI-FiSh $(2^4, 23, 14)$	KeyGen	13.37 s	36.19 s	2.29 m
	Sign	20.44 s	55.38 s	3.52 m
	Verify	20.29 s	55.16 s	3.48 m

Table 4. Runtimes estimates from our proof of concept implementation in Sagemath of PRISMO (100 runs) and Generalised CSI-FiSh (25 runs, using qt-PEGASIS [27]). Timing were obtained on a Macbook Pro with an M1 chip. We stress that for the proof of concept implementation of Generalised CSI-FiSh, we work with $\mathfrak{O} \simeq \mathbb{Z}[\frac{1+\pi}{2}]$.

Protocol	$p \approx 2^{2\mu\lambda}$					
				Type of isogeny		
	$\lvert\mathsf{pk}\rvert$	$\lvert\mathsf{sig}\rvert$		2	(2,2)	(2,2,2,2)
PRISMO	$\mu\lambda/4$	$(2\mu+3)\lambda/4$	KeyGen	-	$2\mu\lambda$	-
			Sign	-	$2\mu\lambda$	-
			Verify	-	2λ	-
FastWaterSQI	$\mu\lambda/4$	$(\mu+1/8)\lambda$	KeyGen	-	$2\mu\lambda$	-
			Sign	$\frac{21}{4}\lambda$	$\mu\lambda$	-
			Verify	$\frac{5}{4}\lambda$	$\mu\lambda$	-
WaterSQI	$\mu\lambda/4$		KeyGen	-	$2\mu\lambda$	-
			Sign	$\frac{3}{2}\lambda$	$4\mu\lambda$	-
			Verify	$\frac{3}{2}\lambda$	$\mu\lambda$	-
Generalised CSI-FiSh $(S = S_1 + 1, t, k)$	$S_1\mu\lambda/4$	$\frac{t}{8}[\log(2S_1+1)+$ $\mu\lambda + (\log 2\mu\lambda)^2]$	KeyGen*	-	-	$2S_1\mu\lambda$
			Sign*	-	-	$2t\mu\lambda$
			Verify*	-	-	$2t\mu\lambda$
SQI-FiSh $(S = S_1 + 1, t, k)$	$S_1\mu\lambda/4$		KeyGen	-	$2S_1\mu\lambda$	-
			Sign	-	$2t\mu\lambda$	-
			Verify*	-	-	$2t\mu\lambda$

Table 5. Estimates of the key and signature sizes (in bytes), and of the number of computed with a generic prime $p \approx 2^{2\mu\lambda}$. The $*$ indicates that the estimate does not include a small and variable number of small degree isogenies that occur in the algorithm.