WaterSQI and PRISMO: Quaternion Signatures for Supersingular Isogeny Group Actions

Tako Boris Fouotsa

École Polytechnique Fédérale de Lausanne, Switzerland
research@borisfouotsa.com

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 the 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 3x faster for key generation, 273x faster for signing and 4900x faster for verification, while also being 29x more compact (signature size).

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

1 Introduction

Peter Shor's quantum algorithm [52] 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 [16] and CSI-Fish [8], SQISign [25,1], SIDH/SIKE [37,31,36], and many others. SIDH was recently broken in polynomial time by the so-called SIDH attacks [15,40,51]. 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 [5,23,29,45,44], and PRISM [3].

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) [16]. 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 [24] and CSI-Fish [8]. These two digital signatures are designed using the generic graph isomorphism identification protocol (or GMW [33]) instantiated with the supersingular isogeny group action. For this reason, they rely on a sigma protocol whose challenge space has polynomial size (the size of the challenge space is 2 for the most basic variant). This implies that for a given security parameter λ, one needs $O(\lambda)$ repetitions in order to reduce the soundness error to negligible. This causes a great efficiency and signature size overhead. Moreover, CSI-FiSh [8], 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 [34]. A record class group computation was done for a 512 bits prime, which was then used to instantiate CSI-FiSh. Several works [7,9,49] have argued that a 512 bits prime does not provide enough quantum security, and the use of several thousand bits primes is recommended [17]. Instantiating CSI-FiSh for those primes with thousands bits is out of reach. Building on OSIDH [19] (a generalisation of CSIDH), it has been proposed (SCALLOP [30], SCALLOP-HD [18], Pear-SCALLOP [2]) 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 [47] and its more efficient variants KLaPoTi [48] and PEGASIS [22], 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 [1,25] and PRISM [3]. SQIsign is a digital signature scheme whose design is inspired by the GPS [32] 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.

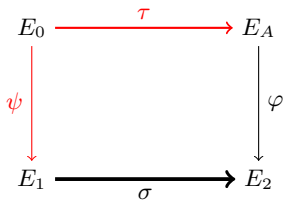


Fig. 1. The SQISign identification protocol.

PRISM [3] 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 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 supersingular isogeny group action?

From now on, we will be working with the set of supersingular elliptic curves defined over $\mathbb{F}_p$ and the action of the of the class group $\mathsf{cl}(\mathfrak{O})$ on this set, where

$\mathfrak{O} \simeq \mathbb{Z}[\pi]$ and π is the Frobenius endomorphism. All the results in this paper can easily be generalised to oriented supersingular 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 $\pi \in \text{End}(E_A) \setminus \mathbb{Z}$ would be a witness for the relation $\mathcal{R}$. For this reason, WaterSQI uses the relation

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

where $\text{End}_{\mathbb{F}_p}(E)$ is the subring of $\text{End}(E)$ 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 isogeny $\sigma : E_1 \to E_2$ is an isogeny such that the prime factors of its degree are inert in $\mathfrak{O} \simeq \mathbb{Z}[\pi]$. 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.

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 one of the two the $\mathbb{F}_p$-rational q-isogenies using Clapoti [47] or PEGASIS [22]. 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 fact the curve E is defined over $\mathbb{F}_p$ (or the knowledge of the orientation) are not helpful to an attacker trying to evaluate q-isogenies.

On our way, we also describe Generalised CSI-FiSh and SQI-FiSh. 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 ideals. As highlighted earlier, instantiating CSI-FiSh with larger parameters that offer enough quantum security is out of reach. Using recent class group evaluation algorithms such as PEGASIS, we describe a CSI-FiSh style signature, which we will call Generalised CSI-FiSh.

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, as its endomorphism ring is known. Since $\text{End}(E_0)$ is known, one can replace all instances of the generic class group evaluation algorithm in key generation and signing by the ideal to isogeny algorithm

used in SQIsin. 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 FastWaterSQI 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 primes $p_{2000} = 3 \cdot 17 \cdot 2^{2026} - 1$ and provides the runtimes of our Sagemath proof of concept implementation of PRISMO and Generalised CSI-FiSh.

Protocol	$p_{2000} = 3 \cdot 17 \cdot 2^{2026} - 1$						
				Type of isogeny			
	$\lvert\mathsf{pk}\rvert$	$\lvert\mathsf{sig}\rvert$		2	(2,2)	(2,2,2,2)	**Runtime**
PRISMO	254	604	KeyGen	-	2 026	-	11.087 s
			Sign	-	2 026	-	8.123 s
			Verify	-	256	-	0.442 s
FastWaterSQI	254	1 043	KeyGen	-	2 026	-	-
			Sign	640	1 038	-	-
			Verify	128	1 038	-	-
WaterSQI	254	1 043	KeyGen	-	2 026	-	-
			Sign	128	4 052	-	-
			Verify	128	1 038	-	-
Generalised CSI-FiSh $(2, 71, 15)$	254	18 040	KeyGen*	-	-	2 026	34.6 s
			Sign*	-	-	143 846	37.0 m
			Verify*	-	-	143 846	36.1 m
Generalised CSI-FiSh $(2^4, 23, 14)$	3 810	5 854	KeyGen*	-	-	2 026	7.8 m
			Sign*	-	-	46 598	12.1 m
			Verify*	-	-	46 598	11.7 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	-	2 026	-	-
			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.

Related work. A recent analysis [43] 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.

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

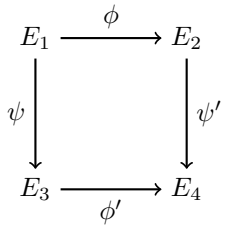
In this section, we briefly discuss isogeny representations, the Deuring correspondence, SQIsign and isogeny group action signatures. We also describe Generalised CSI-FiSh and SQI-FiSh, and detail techniques that will be used to generate the challenge isogeny in WaterSQI.

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 is defined over a relatively small extension of $\mathbb{F}_{p^2}$ as one can use using Vélu formulas [53] or the square root Vélu formulas [6] for computing 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 SIDH attacks, or of Kani's lemma [38] precisely, Robert [50] 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, 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:



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 tat 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 he can generate all this data using the Deuring correspondence which we describe in the next section.

2.2 Quaternion algebras and 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 $\mathrm{End}(E_0)$ 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 [28]) 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 [5,42] for further details.

Sampling a random isogeny of given degree from E_0 (KaniDoublePath). Let d be an 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 [42].

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 [25,26] is a digital signature scheme whose design is inspired by the GPS [32] 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 $\varphi : E_1 \to E_2$. The response consists of a random isogeny $\sigma : E_A \to E_2$. Figure 1 illustrates this identification protocol.

The response computation heavily relies the Deuring correspondence [28] 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 [39] and the use of primes p which are the sum of smooth twins (which are difficult to generate [20,25,26,21,13]). Today, with the new higher dimensional isogeny representation [50] that arose from the SIDH attacks, this requirement has been lifted and further adjustments have been made. Instead of returning a random isogeny $\sigma : E_1 \to E_2$ of large smooth degree, one returns a random short isogeny $\varphi_I : E_1 \to E_2$ 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 $\mathbb{Z}[\frac{1+\pi}{2}]$ [27]. 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 $\mathfrak{O}$ [16, Theorem 7].

In CSIDH [16], $\mathfrak{O} \simeq \mathbb{Z}[\pi]$ while in CSURF [14] $\mathfrak{O} \simeq \mathbb{Z}[\frac{1+\pi}{2}]$. This can be generalised [46] to OSIDH [19] 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 [24] and CSI-FiSh [8]. 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 [30] and its variants [18,2] 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 [47], KLaPoTi [48] and PEGASIS [22] 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.

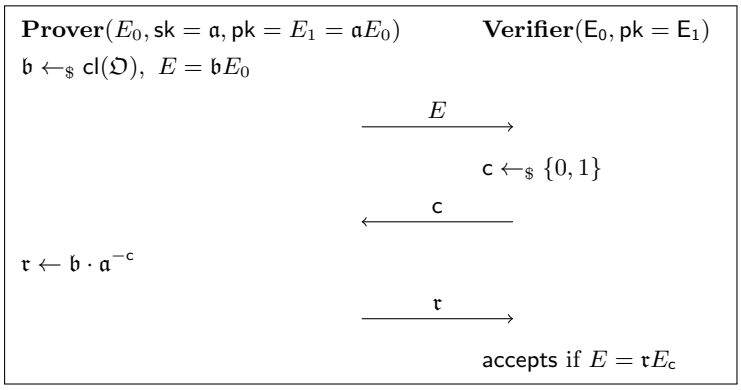


Fig. 2. Graph isomorphism type sigma protocol for isogeny group actions.

Generalised CSI-FiSh. At a high level, the graph isomorphism (or GMW [33]) 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 [8, 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 to $2^{-k}(2S-1)^{-t}$, hence reducing the number of repetitions t and the signature size. We refer to [8, Section 5.2] and [11] 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 is $\mathrm{End}(E_0)$ is known. In fact, generating supersingular elliptic curves with unknown endomorphism is an open research question [10,41], the only known solution being to rely on a trusted party or to use a secure multiparty computation such as the one described in [4]. 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 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 curves $\mathfrak{a}E_0$ and the commitment curves $\mathfrak{b}E_0$, as $\mathrm{End}(E_0)$ is available. During verification, the verifier uses PEGASIS as usual.

Remark 1. One should note that even through 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 best 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 $\phi = \phi_e \circ \cdots \circ \phi_1$ 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 an 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 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 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 $P' = [\ell^{e-e'}]P, Q' = [\ell^{e-e'}]Q$, 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 [14,27] 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 Q are linearly independent is such that 1_ϕ is not $\mathbb{F}_p$-rational. To samples points S that are linearly independent with 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* $s \in \mathbb{Z}_{2^e}$, *the isogeny* $\phi : E \to E/\langle P + [s]Q \rangle$ *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:

1. The commitment curve E_1 should not be defined over $\mathbb{F}_p$.
2. The prime factors of the degree of the response isogeny σ should all be inert in $\mathfrak{O} \simeq \mathbb{Z}[\pi]$.
3. The challenge isogeny φ should not "trivially" factor through an $\mathbb{F}_p$-rational isogeny, meaning that no non-trivial subgroup of $\ker \varphi$ should be fixed by the Frobenius. When φ has prime power degree, this is equivalent to 1_φ not being $\mathbb{F}_p$-rational.

We motivate these choices in Appendix 2.2. 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 isogeny $\varphi : E_A \to E_2$ whose degree is a power of 2 and such that 1_φ is not $\mathbb{F}_p$-rational. The response isogeny $\sigma : E_2 \to E_1$ is an isogeny such that the prime factors of its degree are odd inert in $\mathfrak{O} \simeq \mathbb{Z}[\pi]$. WaterSQI uses isogenies in dimension 1 and 2 only. The response isogeny σ is provided to the verifier using dimension 2 representation, which necessitates an auxiliary isogeny $\delta : E_1 \to E_\delta$ of degree $2^r - \deg \sigma$ for some integer $r > \log(\deg \sigma)$.

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 $\mathfrak{O} \simeq \mathbb{Z}[\pi] \subset \mathrm{End}(E_0)$. When generating the response isogeny, we will first extract the B-smooth part d_1 of its degree d and check if d/d_1 is a prime. The public parameters are $\mathsf{pp} = (p, a, r, B, E_0, \mathfrak{O}, \mathrm{End}(E_0) \simeq \mathcal{O}_0)$, where r is such that 2^r is an upper bound on the degree of the response isogeny.

Algorithm 1 Key generation

Require: $\mathsf{pp} = (p, a, r, B, E_0, \mathfrak{O}, \mathrm{End}(E_0) \simeq \mathcal{O}_0)$
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: $\mathsf{pp} = (p, a, r, B, E_0, \mathfrak{O}, \mathrm{End}(E_0) \simeq \mathcal{O}_0)$
Ensure: $\mathrm{sec} = (I, \psi(E_0[2^a]))$, $\mathsf{com} = E_1$
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** $\mathsf{sec} = (I, \psi(E_0[2^a]))$, $\mathsf{com} = E_1$

Algorithm 3 Challenge isogeny computation

Require: $\mathsf{pp} = (p, a, r, B, E_0, \mathfrak{O}, \mathrm{End}(E_0) \simeq \mathcal{O}_0)$, $\mathsf{pk} = E_A$, $\mathsf{chal} = c$
Ensure: The challenge isogeny $\varphi : E_A \to E_2$ of degree 2^λ
1: Canonically generate a basis (P_A, Q_A) of $E_A[2^\lambda]$ such that $E_A(\mathbb{F}_p)[2] = \langle [2^{\lambda-1}]Q_A \rangle$
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** $\varphi : E_A \to E_2$

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 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.

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^λ derived from the challenge

Algorithm 4 Response

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

Ensure: The response $\mathsf{resp} = (E_\delta, \sigma \circ \widehat{\delta}(E_\delta[2^r]), d_1, d_2)$

//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 random ideal $I_\sigma \sim I$ of odd norm $d < 2^r$

Write $d = d_1 d_2$ where d_1 is the largest B-smooth factor of d

if the prime factors of d_1 are not inert in $\mathfrak{O}$ or d_2 is not a prime inert in $\mathfrak{O}$ **then**

    Go back to Step 5

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

//Generating the auxiliary isogeny and computing the response

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

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 $\delta(E_2[2^r])$ from $\psi(E_0[2^r])$ and $\delta \circ \psi(E_0[2^r])$

Deduce $\sigma \circ \widehat{\delta}(E_\delta[2^r])$ from $\delta(E_2[2^r])$ and $\sigma(E_1[2^r])$

return $\mathsf{resp} = (E_\delta, \sigma \circ \widehat{\delta}(E_\delta[2^r]), d_1, d_2)$

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 $E_A[2^\lambda]$ such that $E_A(\mathbb{F}_p)[2] = \langle [2^{\lambda-1}]Q_A \rangle$, 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

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 $I := \overline{I_\psi}\mathfrak{a}I_\varphi$. Find a random ideal $I_\sigma \sim I$ of odd norm $d < 2^r$ such that all the prime factors of d are inert in $\mathfrak{O} \simeq \mathbb{Z}[\pi]$. This is achieved by repeatedly sampling random ideals $I_\sigma \sim I$ of norm d smaller than 2^r, factoring out the largest divisor d_1 of d such that all the prime

Algorithm 5 Verify

Require: $\mathsf{pp} = (p, a, r, B, E_0, \mathfrak{O}, \mathrm{End}(E_0) \simeq \mathcal{O}_0)$, $\mathsf{pk} = E_A$, $\mathsf{com} = E_1$, $\mathsf{chal} = c$, $\mathsf{resp} = (E_\delta, \sigma \circ \widehat{\delta}(E_\delta[2^r]), d)$
Ensure: Accept or Reject

```
Compute the B-smooth part d_1 of d
if d/d_1 is not a prime or (d/d_1 and the prime factors of d_1 are not inert in 𝔒) then
    return Reject
Compute the challenge isogeny φ : E_A → E_2 using Algorithm 3
Compute a canonical basis (P_δ, Q_δ) E_δ[2^r]
Recover P_2 = σ ∘ δ̂(P_δ) and Q_2 = σ ∘ δ̂(Q_δ)
Compute the isogeny Ψ : E_δ × E_2 → F_1 × F_2 of kernel ⟨([d]P_δ, P_2), ([d]Q_δ, Q_2)⟩
if the computation of Ψ fails or F_1 ≇ E_1 then
    return Reject
Compute (P_1, −) = Ψ(0, P_2) and (Q_1, −) = Ψ(0, Q_2)
if e_{2^r}(P_1, Q_1) = e_{2^r}(P_2, Q_2)^d then
    return Accept
return Reject
```

factors of d_1 are smaller than B and are inert in $\mathfrak{O} \simeq \mathbb{Z}[\pi]$, and checking whether $d_2 = d/d_1$ is a prime inert in $\mathfrak{O} \simeq \mathbb{Z}[\pi]$. The ideal I_σ corresponds to the response isogeny $\sigma : E_1 \to E_2$.

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

Remark 4 (On the size of r). The integer $r \leq a - \lambda$ needs to be such that one can find a response isogeny whose degree $d < 2^r$ has all its prime factor inert in $\mathfrak{O} \simeq \mathbb{Z}[\pi]$. One easy way to achieve this would be to require that d is a prime inert in $\mathfrak{O} \simeq \mathbb{Z}[\pi]$, in which case $r > \frac{1}{2}\log p + c_0 \log\log p$ for some small constant c_0 is sufficient in practice (see [23, Section 4.2] for further details). Since allowing d to have several inert prime factors is a relaxation, then the bound above is sufficient for our application. In this paper, we use $c_0 = 2$.

Verification. Given the public key $\mathsf{pk} = E_A$, the commitment $\mathsf{com} = E_1$, the challenge $\mathsf{chal} = c$ and the response $(E_\delta, \sigma \circ \widehat{\delta}(E_\delta[2^r]), d_1, d_2)$, one first checks

that $d = d_1 d_2 < 2^r$, d_1 is a B-smooth integer whose prime factors are inert in $\mathfrak{O} \simeq \mathbb{Z}[\pi]$ and d_2 is a prime inert in $\mathfrak{O} \simeq \mathbb{Z}[\pi]$. One then computes the challenge isogeny $\varphi : E_A \to E_2$ using Algorithm 3 to recover E_2. Note that in practice, the response contains E_δ, d and the coordinates of $\sigma \circ \widehat{\delta}(P)$ and $\sigma \circ \widehat{\delta}(Q)$ in a canonical basis of $E_2[2^r]$ where (P, Q) is a canonical basis of $E_\delta[2^r]$. One hence generates a canonical basis (P, Q) of $E_2[2^r]$ and a canonical basis (P_δ, Q_δ) of $E_\delta[2^r]$, and recovers $P_2 = \sigma \circ \widehat{\delta}(P_\delta)$ and $Q_2 = \sigma \circ \widehat{\delta}(Q_\delta)$ from the information available in the response. One then computes the dimension 2 isogeny

$$\Psi = \begin{pmatrix} \widehat{\delta} & -\widehat{\sigma} \\ \sigma' & \delta' \end{pmatrix} : E_\delta \times E_2 \to F_1 \times F_2$$

of kernel $\{([d]S, \sigma \circ \widehat{\delta}(S)), S \in E_\delta[2^r]\}$. By definition, the codomain Ψ should be $E_1 \times E_{\delta'}$. If the computation of Ψ fails or F_1 is not isomorphic to E_1 one rejects the response. One then computes $(P_1, -) = \Psi(0, P_2)$ and $(Q_1, -) = \Psi(0, Q_2)$ and checks that $e_{2^r}(P_1, Q_1) = e_{2^r}(P_2, Q_2)^d$. This check confirms that the degree of the response isogeny is d. The verification algorithm 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 on WaterSQI 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 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 and $\sigma_2 : E_1 \to E_2'$ of degree d' be the two corresponding response isogenies where $\varphi : E_A \to E_2$ and $\varphi' : E_A \to E_2'$. Since we have a representation of σ and σ', then we can derive a representation of $\alpha_0 = \widehat{\varphi'} \circ \sigma' \circ \widehat{\sigma} \circ \varphi \in \mathrm{End}(E_A)$. Let $\alpha \in \mathrm{End}(E_A)$ be the cyclic component of α_0.

If $\sigma' \circ \widehat{\sigma} \notin \mathbb{Z}$, then its cyclic component appears in α. This cyclic component has odd degree d_0 dividing dd' and d_0 divides the degree of α. Since α is cyclic and the prime factors of d_0 are inert in $\mathbb{Z}[\pi]$, then $\alpha \in \mathrm{End}(E_A) \setminus \mathrm{End}_{\mathbb{F}_p}(E_A)$.

If $\sigma' \circ \widehat{\sigma} \in \mathbb{Z}$, then since σ and σ' are cyclic, we must have $\sigma' \circ \widehat{\sigma} = [d]$ and $d = d'$. This implies that $\alpha \in \mathrm{End}(E_A)$ is in fact the cyclic component of $\alpha_0 = [d]\widehat{\varphi'} \circ \varphi$. Clearly, $\widehat{\varphi'} \circ \varphi \notin \mathbb{Z}$ since the contrary would imply that $\ker\varphi = \ker\varphi'$ (which is a contradiction). Hence $\alpha \notin \mathbb{Z}$ and α has degree 2^{2b} where $1 \leq b \leq \lambda$, and $\alpha_0 = [2^{\lambda-b}d]\alpha$. Let $\ker\varphi = \langle S \rangle$. Then $\alpha_0(S) = 0$, implying that $[2^{\lambda-b}]\alpha(S) = 0$ (because d is odd), that is $\alpha(S) \in E_2[2^{\lambda-b}]$. Since S has order 2^λ, then $[2^{\lambda-b}]S \in \ker\alpha$. 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 $\langle [2^{\lambda-b}]S \rangle$. Hence

$$\ker 1_\alpha = [2^{b-1}]\langle [2^{\lambda-b}]S \rangle = \langle [2^{\lambda-1}]S \rangle = \ker 1_\varphi.$$

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 $\alpha \in \mathrm{End}(E_A) \setminus \mathrm{End}_{\mathbb{F}_p}(E_A)$. □

Zero-knowledge. As in all dimension two variants [5,45,29] of SQIsign, each valid signature reveals two random non-smooth 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 Inert Degree Isogeny Oracle *(RUBIDIO) is an oracle that takes as input a supersingular curve E and returns an efficient representation of an isogeny $\sigma : E \to E'$ of odd degree $d < 2^r$, with $r \geq \frac{1}{2}\log p + c_0 \log\log p$ for some small constant c_0, such that:*

- *E' is uniformly distributed in the supersingular isogeny graph.*
- *The conditional distribution of σ given E' is uniform among isogenies $\sigma : E \to E'$ of degree $d < 2^r$ where d factors as $d = d_1 d_2$ with d_2 being an inert prime in $\mathfrak{O} \simeq \mathbb{Z}[\pi]$, and the prime factors of d_1 are inert in $\mathfrak{O} \simeq \mathbb{Z}[\pi]$ and smaller than B.*

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

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 RUBIDIO 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 RUBIDIO on E_2 and gets an efficient representation of a random isogeny $\widehat{\sigma} : E_2 \to E_1$ whose degree d factors as $d = d_1 d_2 < 2^r$ with d_2 being an inert prime in $\mathfrak{O} \simeq \mathbb{Z}[\pi]$, and the prime factors of d_1 are inert in $\mathfrak{O} \simeq \mathbb{Z}[\pi]$ and smaller than B. It then calls RAIO on E_1 and gets an efficient representation of a random isogeny $\delta : E_1 \to E_\delta$ of degree $2^r - d$. It computes $\sigma \circ \widehat{\delta}(E_\delta[2^r])$ and returns $(E_\delta, \sigma \circ \widehat{\delta}(E_\delta[2^r]), d_1, d_2)$ as the transcript.

The degree of the commitment isogeny is $d_{\mathsf{com}} \geq 2^{2(\mu+1)\lambda}$. Applying [23, 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. Therefore, with respect to the definition of RUBIDIO and RAIO, 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 RUBIDIO 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 $2^r - d$, then we compute its push-forward through the commitment isogeny ψ to obtain $\delta = [\psi]_* \delta_0$. The remainder of the scheme is unchanged.

4.1 Public parameters, key generation, commitment and challenge

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

Algorithm 6 Fast commitment isogeny computation

Require: $\mathsf{pp} = (p, a, r, B, E_0, \mathfrak{O}, \mathrm{End}(E_0) \simeq \mathcal{O}_0)$
Ensure: $\mathrm{sec} = (I_\psi, u)$, $\mathsf{com} = E_1$
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 siogeny ψ
8: **return** $\mathrm{sec} = (I_\psi, u)$, $\mathsf{com} = E_1$

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 E_1 is defined over $\mathbb{F}_p$, 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.

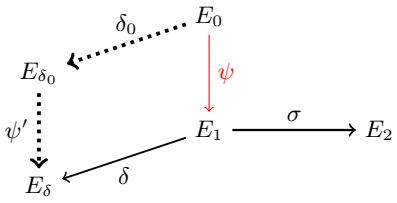


Fig. 3. Fast aux. isogeny computation.

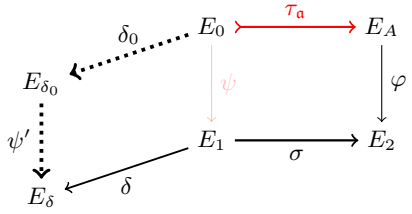


Fig. 4. Fast response computation.

Response. The response algorithm follows several steps.

1. Compute the ideal I_φ corresponding to the challenge isogeny $\varphi : E_A \to E_2$, generate the ideal I_σ of norm $d = d_1 d_2 < 2^r$ corresponding to the response isogeny $\sigma : E_1 \to E_2$ as described in WaterSQI (section 3.2). Contrarily to WaterSQI where we evaluate σ and the auxiliary isogeny δ separately, in FastWaterSQI, we first generate the auxiliary isogeny and evaluate $\sigma \circ \widehat{\delta}(E_\delta[2^r])$ directly.

Algorithm 7 Fast response

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

Ensure: The response $\widehat{\delta} \circ \sigma(E_1[2^r])$

//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 random ideal $I_\sigma \sim I$ of norm $d < 2^r$

Write $d = d_1 d_2$ where d_1 is the largest B-smooth factor of d

if the prime factors of d_1 are not inert in $\mathfrak{O}$ or d_2 is not a prime inert in $\mathfrak{O}$ **then**

    Go back to Step 5

//Generating the auxiliary isogeny and computing the response

Sample a random isogeny $\delta_0 : E_0 \to E_{\delta_0}$ of degree $2^r - d$ 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 ideal push-forward $I_\delta := [I_\psi]_* I_{\delta_0}$ of I_{δ_0} through I_ψ

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

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

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

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

return $\mathsf{resp} = (E_\delta, \sigma \circ \widehat{\delta}(E_\delta[2^r]), d_1, d_2)$

2. To generate a random auxiliary isogeny $\delta : E_1 \to E_\delta$ of degree $2^r - d$, one proceeds as follows. Use KaniDoublePath to sample a random isogeny $\delta_0 : E_0 \to E_{\delta_0}$ of degree $2^r - d$ 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 $\theta = \widehat{\tau} \circ \widehat{\varphi} \circ \sigma \circ \widehat{\delta} \circ \psi' \circ \delta_0 = [2^r - d] \widehat{\tau} \circ \widehat{\varphi} \circ \sigma \circ \psi \in \mathrm{End}(E_0)$ from the principal ideal $I_{\delta_0} I_{\psi'} I_\delta I_\sigma \overline{I_\varphi} \overline{\mathfrak{a}} = (2^r - d) I_\psi I_\sigma \overline{I_\varphi} \overline{\mathfrak{a}}$ 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 $\sigma \circ \widehat{\delta}(E_\delta[2^{a-3\lambda}]) = \frac{1}{\deg \delta_0 \cdot \deg \tau} \varphi \circ \tau \circ \theta \circ \widehat{\delta_0} \circ \widehat{\psi'}(E_\delta[2^a])$. Deduce $\sigma \circ \widehat{\delta}(E_\delta[2^r])$. 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 $(E_\delta, \sigma \circ \widehat{\delta}(E_\delta[2^r]), d_1, d_2)$. The auxiliary isogeny computation and the response computation are illustrated in Figure 3 and Figure 4 respectively, and the fast response algorithm is summarised in Algorithm 7.

4.3 The FastWaterSQI signature algorithm

As usual, we prove that the FastWaterSQI is a Σ-protocol by showing that it is 2-special sound and honest-verifier zero knowledge, before applying[1] 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 look alike, the only difference being the distribution of the commitment curve E_1. 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 $2^{2\lambda}$-isogeny and let $d < 2^r$ be an integer. An isogeny $\delta : E_1 \to E_\delta$ 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 RUBIDIO and a RAIO, outputs random transcripts which are computationally indistinguishable from honest transcripts in FastWaterSQI.*

Proof. Given an honestly generated challenge $\varphi : E_A \to E_2$, the simulator calls RUBIDIO on E_2 and gets an efficient representation of a random isogeny $\widehat{\sigma} : E_2 \to E_1$ whose degree d factors as $d = d_1 d_2 < 2^r$ with d_2 being an inert prime in $\mathfrak{O} \simeq \mathbb{Z}[\pi]$, and the prime factors of d_1 are inert in $\mathfrak{O} \simeq \mathbb{Z}[\pi]$ and smaller than B. It then calls RAIO on E_1 and gets an efficient representation of a random isogeny $\delta : E_1 \to E_\delta$ of degree $2^r - d$. It computes $\sigma \circ \widehat{\delta}(E_\delta[2^r])$ and returns $(E_\delta, \sigma \circ \widehat{\delta}(E_\delta[2^r]), d_1, d_2)$ as the transcript.

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.

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

5 PRISMO: PRISM for Oriented supersingular curves

In this section, we briefly recall PRISM and describe PRISMO.

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 supersingular curve $\mathsf{pk} = E_A$ and his secret key is an isogeny $\tau : E_0 \to E_A$. 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.

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 5. 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 [3, Prop. 2] to be EUF-CMA secure under the assumption that $\mathsf{H}_{\mathsf{Prime}}$ is a collision resistance hash function and Problem 15 is hard.

Definition 14. *A special degree isogeny oracle (SPEDIO) is an oracle which takes as input 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 15. 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 generated by the oracle.

Proposition 16 ([3, Prop. 2]). *If $\mathsf{H}_{\mathsf{Prime}}$ is a collision-resistant cryptographic hash function and Problem 15 is hard, then PRISM is EUF-CMA secure.*

5.2 The PRISMO signature

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

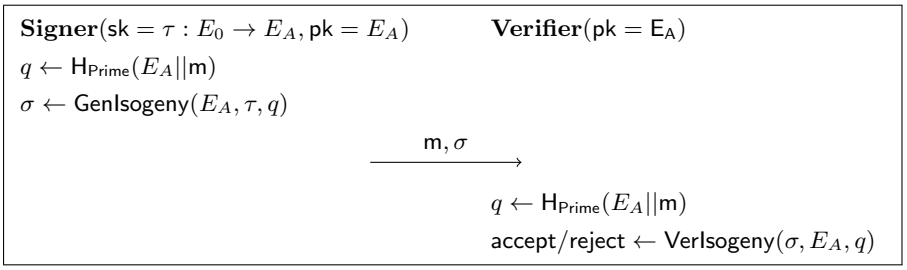


Fig. 5. PRISM signature scheme.

1. *Sieve for the message to be forged.* Here we randomly sample messages m till we get one for which $q = \mathsf{H}_{\mathsf{Prime}}(E_A||\mathsf{m})$ 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.
2. *Generate the quadratic ideal.* Once we have found a message m such that $q = \mathsf{H}_{\mathsf{Prime}}(E_A||\mathsf{m})$ 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 [22] to compute the v-isogeny $\sigma_1 : E_A \to E_1$ 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 $\sigma : E_A \to E'$ is $sv = stq = q(2^u - q)$ and $q = \mathsf{H}_{\mathsf{Prime}}(E_A||\mathsf{m})$. Computing $\sigma_1 : E_A \to E_1$ 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 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 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 $\mathsf{pk} = E_A$ is a curve defined over $\mathbb{F}_p$, and the secret key is an $\mathbb{F}_p$-rational isogeny $\tau_{\mathfrak{a}} : E_0 \to E_A$. 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 $\sigma : E_A \to E'$. During the verification, one verifies that $\sigma : E_A \to E'$ 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 $\mathsf{H}_{\mathsf{InertPrime}} : \{0,1\}^* \to \mathsf{InertPrimes}_u$. 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_A, $\mathsf{H}_{\mathsf{Prime}}(E_A||\mathsf{m})$ is obtained by repeatedly computing $2^{u-1} + 2\mathsf{H}_{u-2}(E_A||\mathsf{m}||\mathsf{counter}) + 1$ 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 6, where $\mathsf{InertPrimes}_u$ is the set of primes q such that $2^{u-1} < q < 2^u$ and q is inert $\mathfrak{O} \simeq \mathbb{Z}[\pi]$.

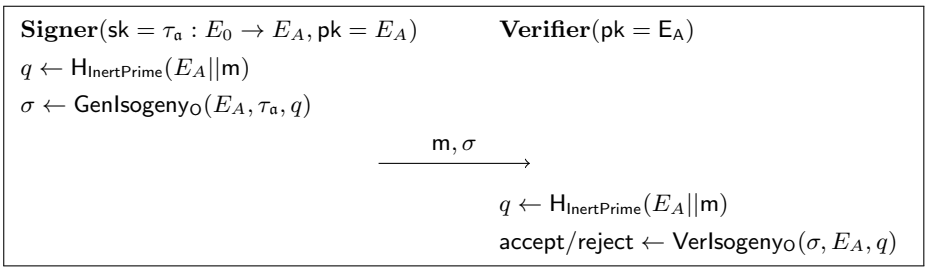


Fig. 6. PRISMO signature scheme.

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 $\text{SPEDIO}_{\mathsf{O}}$ oracle in Definition 17 and the new hard problem in Problem 18. We then state in Proposition 19 that PRISMO is EUF-CMA secure under the assumption that $\mathsf{H}_{\mathsf{InertPrime}}$ is a collision resistance hash function and Problem 18 is hard. We omit the proof of as it can be obtained from that of Proposition 16 (see [3, Prop. 2]) where one replaces SPEDIO by $\text{SPEDIO}_{\mathsf{O}}$ and Problem 15 by Problem 18.

Definition 17. *$\text{SPEDIO}_{\mathsf{O}}$ 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 18. Given a random supersingular elliptic curve E defined over $\mathbb{F}_p$ and a $\text{SPEDIO}_{\mathsf{O}}$, output an isogeny φ of degree $q'(2^u - q')$ with $q' \in \mathsf{InertPrimes}_u$ different from all degrees q formerly generated by the oracle ($u = 2\lambda$).

Proposition 19. *If $\mathsf{H}_{\mathsf{InertPrime}}$ is a collision-resistant cryptographic hash function and Problem 18 is hard, then PRISMO is EUF-CMA secure.*

We believe that Problem 18 in PRISMO is as hard as Problem 15 in PRISM because as the prime q is inert in $\mathfrak{O} \simeq \mathbb{Z}[\pi]$, the sub-ring $\mathbb{Z}[\pi]$ of $\text{End}(E)$ is not useful at all when trying to evaluate a q-isogeny when q has not been queried to $\text{SPEDIO}_{\mathsf{O}}$. Meaning that even if one were able to compute a $(2^u\text{-}q)$-isogeny, the degree q one would be infeasible to compute as the best known algorithm would run in time $O(q^2)$ [3, §4.4].

Remark 20. In Problem 18, since we have one non-trivial endomorphism $\pi \in \text{End}(E)$, given one $q(2^u - q)$-isogeny $\varphi : E \to E'$ returned by $\text{SPEDIO}_{\mathsf{O}}$, one can efficiently compute a representation of the isogeny[2] $\varphi^{(p)} : E \to E'^{(p)}$. But, since the degree of $\varphi^{(p)}$ is also $q(2^u - q)$, $\varphi^{(p)}$ is not a solution to Problem 18. 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.

[2] 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 $\pi(\ker \varphi)$.

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 [22].

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 quadratic order. The integer r is set to $r = \lceil \frac{1}{2}\log p + 2\log\log p \rceil$ and $B = r$.

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 $\mu > 1$ for WaterSQI so that it is possible to have $r < a - \lambda$, and $\mu > 3\lambda$ for FastWaterSQI so that it is possible to have $r < a - 3\lambda$.

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 $\mathsf{resp} = (E_\delta, \sigma \circ \widehat{\delta}(E_\delta[2^r]), d_1, d_2)$. 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 $\sigma \circ \widehat{\delta}(E_\delta[2^r])$ is provided as $(\sigma \circ \widehat{\delta}(P_\delta), \sigma \circ \widehat{\delta}(Q_\delta))$ where (P_δ, Q_δ) is a canonically generated basis of $E_\delta[2^r]$. One compresses $\sigma \circ \widehat{\delta}(P_\delta)$ and $\sigma \circ \widehat{\delta}(Q_\delta)$ by expressing them as $\sigma \circ \widehat{\delta}(P_\delta) = [a_1]P_2 + [a_2]Q_2$, $\sigma \circ \widehat{\delta}(Q_\delta) = [a_3]P_2 + [a_4]Q_2$ 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 $d(2^r - d)$ of the isogeny $\sigma \circ \widehat{\delta}$, 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 [23, Section 6.1] for further details). Since $d = d_1 d_2 < 2^r$, then (d_1, d_2) is represented using r bits.

Putting everything together, we have λ bits for the challenge and about $2\log p + 4r \approx 2\log p + 4(\frac{1}{2}\log p + 2\log\log p) \approx 4\log p + 8\log\log p$ for the response. Hence the size of the signature is roughly $\lambda + 4\log p + 8\log\log p$. When $p \approx 2^{2\mu\lambda}$, the signature size is $(8\mu+1)\lambda + 8\log(2\mu\lambda)$ bits, or $(\mu+1/8)\lambda + \log(2\mu\lambda)$ 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 $\sigma : E_A \to E'$. 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 $E_A[2^u]$. 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 [22] 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 [35], 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 PEGASIS [22, §5], we did a proof of concept implementation of PRISMO and Generalised CSI-FiSh in Sagemath. The average runtime of both schemes when instantiated with the primes p_{500}, p_{1000} and p_{2000} are provided in Table 4.

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. 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
3. 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)
4. 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)
5. 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.) Advances in Cryptology – ASIACRYPT 2024, Part III. Lecture Notes in Computer Science, vol. 15486, pp. 339–370. Springer, Singapore, Singapore, Kolkata, India (Dec 9–13, 2024). https://doi.org/10.1007/978-981-96-0891-1_11
6. 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)
7. 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.) Advances in Cryptology – EUROCRYPT 2019, Part II. Lecture Notes in Computer Science, vol. 11477, pp. 409–441. Springer, Cham, Switzerland, Darmstadt, Germany (May 19–23, 2019). https://doi.org/10.1007/978-3-030-17656-3_15
8. Beullens, W., Kleinjung, T., Vercauteren, F.: CSI-FiSh: Efficient isogeny based signatures through class group computations. In: Galbraith, S.D., Moriai, S. (eds.) Advances in Cryptology – ASIACRYPT 2019, Part I. Lecture Notes in Computer Science, vol. 11921, pp. 227–247. Springer, Cham, Switzerland, Kobe, Japan (Dec 8–12, 2019). https://doi.org/10.1007/978-3-030-34578-5_9
9. Bonnetain, X., Schrottenloher, A.: Quantum security analysis of CSIDH. In: Canteaut, A., Ishai, Y. (eds.) Advances in Cryptology – EUROCRYPT 2020, Part II. Lecture Notes in Computer Science, vol. 12106, pp. 493–522. Springer, Cham, Switzerland, Zagreb, Croatia (May 10–14, 2020). https://doi.org/10.1007/978-3-030-45724-2_17
10. 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

11. Borin, G., Persichetti, E., Pintore, F., Reijnders, K., Santini, P.: A guide to the design of digital signatures based on cryptographic group actions: G. borin et al. Journal of Cryptology **38**(3), 23 (2025)
12. Borin, G., Santos, M.C.R., Eriksen, J.K., Invernizzi, R., Mula, M., Schaeffler, S., Vercauteren, F.: Qlapoti: Simple and efficient translation of quaternion ideals to isogenies. Cryptology ePrint Archive, Paper 2025/1604 (2025), https://eprint.iacr.org/2025/1604
13. Bruno, G., Santos, M.C.R., Costello, C., Eriksen, J.K., Meyer, M., Naehrig, M., Sterner, B.: Cryptographic smooth neighbors. In: Guo, J., Steinfeld, R. (eds.) Advances in Cryptology – ASIACRYPT 2023, Part VII. Lecture Notes in Computer Science, vol. 14444, pp. 190–221. Springer, Singapore, Singapore, Guangzhou, China (Dec 4–8, 2023). https://doi.org/10.1007/978-981-99-8739-9_7
14. 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, Switzerland, Paris, France (Apr 15–17, 2020). https://doi.org/10.1007/978-3-030-44223-1_7
15. Castryck, W., Decru, T.: An efficient key recovery attack on SIDH. In: Hazay, C., Stam, M. (eds.) Advances in Cryptology – EUROCRYPT 2023, Part V. Lecture Notes in Computer Science, vol. 14008, pp. 423–447. Springer, Cham, Switzerland, Lyon, France (Apr 23–27, 2023). https://doi.org/10.1007/978-3-031-30589-4_15
16. Castryck, W., Lange, T., Martindale, C., Panny, L., Renes, J.: CSIDH: An efficient post-quantum commutative group action. In: Peyrin, T., Galbraith, S. (eds.) Advances in Cryptology – ASIACRYPT 2018, Part III. Lecture Notes in Computer Science, vol. 11274, pp. 395–427. Springer, Cham, Switzerland, Brisbane, Queensland, Australia (Dec 2–6, 2018). https://doi.org/10.1007/978-3-030-03332-3_15
17. 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)
18. Chen, M., Leroux, A., Panny, L.: SCALLOP-HD: Group action from 2-dimensional isogenies. In: Tang, Q., Teague, V. (eds.) PKC 2024: 27th International Conference on Theory and Practice of Public Key Cryptography, Part III. Lecture Notes in Computer Science, vol. 14603, pp. 190–216. Springer, Cham, Switzerland, Sydney, NSW, Australia (Apr 15–17, 2024). https://doi.org/10.1007/978-3-031-57725-3_7
19. 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
20. Costello, C.: B-SIDH: Supersingular isogeny Diffie-Hellman using twisted torsion. In: Moriai, S., Wang, H. (eds.) Advances in Cryptology – ASIACRYPT 2020, Part II. Lecture Notes in Computer Science, vol. 12492, pp. 440–463. Springer, Cham, Switzerland, Daejeon, South Korea (Dec 7–11, 2020). https://doi.org/10.1007/978-3-030-64834-3_15
21. 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.) Advances in Cryptology – EUROCRYPT 2021, Part I. Lecture Notes in Computer Science, vol. 12696, pp. 272–301. Springer, Cham, Switzerland, Zagreb, Croatia (Oct 17–21, 2021). https://doi.org/10.1007/978-3-030-77870-5_10

22. Dartois, P., Eriksen, J.K., Fouotsa, T.B., Herlédan Le Merdy, A., Invernizzi, R., Robert, D., Rueger, R., Vercauteren, F., Wesolowski, B.: Pegasis: Practical effective class group action using 4-dimensional isogenies. In: Tauman Kalai, Y., Kamara, S.F. (eds.) Advances in Cryptology – CRYPTO 2025. pp. 67–99. Springer Nature Switzerland, Cham (2025)
23. Dartois, P., Leroux, A., Robert, D., Wesolowski, B.: SQIsignHD: New dimensions in cryptography. In: Joye, M., Leander, G. (eds.) Advances in Cryptology – EUROCRYPT 2024, Part I. Lecture Notes in Computer Science, vol. 14651, pp. 3–32. Springer, Cham, Switzerland, Zurich, Switzerland (May 26–30, 2024). https://doi.org/10.1007/978-3-031-58716-0_1
24. De Feo, L., Galbraith, S.D.: SeaSign: Compact isogeny signatures from class group actions. In: Ishai, Y., Rijmen, V. (eds.) Advances in Cryptology – EUROCRYPT 2019, Part III. Lecture Notes in Computer Science, vol. 11478, pp. 759–789. Springer, Cham, Switzerland, Darmstadt, Germany (May 19–23, 2019). https://doi.org/10.1007/978-3-030-17659-4_26
25. De Feo, L., Kohel, D., Leroux, A., Petit, C., Wesolowski, B.: SQISign: Compact post-quantum signatures from quaternions and isogenies. In: Moriai, S., Wang, H. (eds.) Advances in Cryptology – ASIACRYPT 2020, Part I. Lecture Notes in Computer Science, vol. 12491, pp. 64–93. Springer, Cham, Switzerland, Daejeon, South Korea (Dec 7–11, 2020). https://doi.org/10.1007/978-3-030-64837-4_3
26. De Feo, L., Leroux, A., Longa, P., Wesolowski, B.: New algorithms for the Deuring correspondence - towards practical and secure SQISign signatures. In: Hazay, C., Stam, M. (eds.) Advances in Cryptology – EUROCRYPT 2023, Part V. Lecture Notes in Computer Science, vol. 14008, pp. 659–690. Springer, Cham, Switzerland, Lyon, France (Apr 23–27, 2023). https://doi.org/10.1007/978-3-031-30589-4_23
27. Delfs, C., Galbraith, S.D.: Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$. Designs, Codes and Cryptography **78**(2), 425–440 (2016). https://doi.org/10.1007/s10623-014-0010-1
28. 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)
29. Duparc, M., Fouotsa, T.B.: SQIPrime: A dimension 2 variant of SQISignHD with non-smooth challenge isogenies. In: Chung, K.M., Sasaki, Y. (eds.) Advances in Cryptology – ASIACRYPT 2024, Part III. Lecture Notes in Computer Science, vol. 15486, pp. 396–429. Springer, Singapore, Singapore, Kolkata, India (Dec 9–13, 2024). https://doi.org/10.1007/978-981-96-0891-1_13
30. Feo, L.D., 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)
31. Feo, L.D., Jao, D., Plût, J.: Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies (2014), pagesn 209-247
32. Galbraith, S.D., Petit, C., Silva, J.: Identification protocols and signature schemes based on supersingular isogeny problems. In: Takagi, T., Peyrin, T. (eds.) Advances in Cryptology – ASIACRYPT 2017, Part I. Lecture Notes in Computer Science, vol. 10624, pp. 3–33. Springer, Cham, Switzerland, Hong Kong, China (Dec 3–7, 2017). https://doi.org/10.1007/978-3-319-70694-8_1
33. 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, https://doi.org/10.1145/116825.116852
34. 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)
35. Hardy, G.H., Ramanujan, S.: The normal number of prime factors of a number n. Quarterly Journal of Mathematics, 48: 76-92 (1917)
36. 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
37. 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)
38. Kani, E.: The number of curves of genus two with elliptic differentials. Walter de Gruyter, Berlin/New York Berlin, New York (1997)
39. 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)
40. Maino, L., Martindale, C., Panny, L., Pope, G., Wesolowski, B.: A direct key recovery attack on SIDH. In: Hazay, C., Stam, M. (eds.) Advances in Cryptology – EUROCRYPT 2023, Part V. Lecture Notes in Computer Science, vol. 14008, pp. 448–471. Springer, Cham, Switzerland, Lyon, France (Apr 23–27, 2023). https://doi.org/10.1007/978-3-031-30589-4_16
41. Mula, M., Murru, N., Pintore, F.: On random sampling of supersingular elliptic curves. Annali di Matematica Pura ed Applicata (1923 -) **204**(3), 1293–1335 (06 2025). https://doi.org/10.1007/s10231-024-01528-x, https://doi.org/10.1007/s10231-024-01528-x
42. Nakagawa, K., Onuki, H.: QFESTA: Efficient algorithms and parameters for FESTA using quaternion algebras. In: Reyzin, L., Stebila, D. (eds.) Advances in Cryptology – CRYPTO 2024, Part V. Lecture Notes in Computer Science, vol. 14924, pp. 75–106. Springer, Cham, Switzerland, Santa Barbara, CA, USA (Aug 18–22, 2024). https://doi.org/10.1007/978-3-031-68388-6_4
43. 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
44. 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
45. Nakagawa, K., Onuki, H., Castryck, W., Chen, M., Invernizzi, R., Lorenzon, G., Vercauteren, F.: SQIsign2D-East: A new signature scheme using 2-dimensional isogenies. In: Chung, K.M., Sasaki, Y. (eds.) Advances in Cryptology – ASIACRYPT 2024, Part III. Lecture Notes in Computer Science, vol. 15486, pp. 272–303. Springer, Singapore, Singapore, Kolkata, India (Dec 9–13, 2024). https://doi.org/10.1007/978-981-96-0891-1_9
46. 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, https://www.sciencedirect.com/science/article/pii/S1071579720301465
47. 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

48. 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
49. Peikert, C.: He gives C-sieves on the CSIDH. In: Canteaut, A., Ishai, Y. (eds.) Advances in Cryptology – EUROCRYPT 2020, Part II. Lecture Notes in Computer Science, vol. 12106, pp. 463–492. Springer, Cham, Switzerland, Zagreb, Croatia (May 10–14, 2020). https://doi.org/10.1007/978-3-030-45724-2_16
50. Robert, D.: Evaluating isogenies in polylogarithmic time. Cryptology ePrint Archive, Paper 2022/1068 (2022), https://eprint.iacr.org/2022/1068, https://eprint.iacr.org/2022/1068
51. Robert, D.: Breaking SIDH in polynomial time. In: Hazay, C., Stam, M. (eds.) Advances in Cryptology – EUROCRYPT 2023, Part V. Lecture Notes in Computer Science, vol. 14008, pp. 472–503. Springer, Cham, Switzerland, Lyon, France (Apr 23–27, 2023). https://doi.org/10.1007/978-3-031-30589-4_17
52. 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)
53. Vélu, J.: Isogénies entre courbes elliptiques. Comptes-Rendus de l'Académie des Sciences **273**, 238–241 (1971)

A Towards WaterSQI

In this section, we describe some failed attempts to instantiate SQIsign with $\mathbb{F}_p$-rational secret isogenies. These failed attempts will hopefully help in understanding the design choices we made in WaterSQI. 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

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

and for our scheme to be sound, we need to be able to extract a non $\mathbb{F}_p$-rational endomorphism of E_A from two valid transcripts.

A.1 Towards WaterSQI: A first attempt

An overview of the identification protocol 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 would like 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.

Since E_0 is defined over $\mathbb{F}_p$ and the isogenies $\tau_{\mathfrak{a}} : E_0 \to E_A$, $\psi_{\mathfrak{b}} : E_0 \to E_1$ and $\varphi_{\mathfrak{c}} : E_A \to E_2$ are all $\mathbb{F}_p$-rational, then the curves E_1 and E_2 are also defined over $\mathbb{F}_p$. 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 insecure.

Returning σ as 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 then 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 $\mathrm{End}_{\mathbb{F}_p}(E_A) = \mathbb{Z}[\pi]$.

Returning σ as an isogeny defined over $\mathbb{F}_{p^2}$ (and not over $\mathbb{F}_p$). Assume that the response isogeny $\sigma : E_1 \longrightarrow E_2$ is defined over $\mathbb{F}_{p^2}$. 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 21. *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 ϕ_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 21, 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. 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 section, 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 Towards WaterSQI: A second attempt

Now we assume that the commitment isogeny $\psi : E_0 \longrightarrow E_1$ is such that E_1 is not defined over $\mathbb{F}_p$. We will assume that the challenge isogeny $\varphi : E_A \longrightarrow E_2$ factors through some $\mathbb{F}_p$ part $\varphi_1 : E_A \longrightarrow E_2'$, such that $\varphi = \varphi_2 \circ \varphi_1$ with $\varphi_2 : E_2' \longrightarrow E_2$. Note that when the challenge isogeny is $\mathbb{F}_p$-rational, φ_2 is an automorphism of E_2. In this setting, the isogeny $\widehat{\sigma} \circ \varphi_{\mathfrak{c}} : E_A \longrightarrow E_1$ goes from an $\mathbb{F}_p$ curve to a curve defined over $\mathbb{F}_{p^2}$ (and not over $\mathbb{F}_p$). This implies that the burdens of the previous section are avoided. Nevertheless, we show that is is possible to forge signatures.

Forging valid signatures. To forge a signature, a malicious signer proceeds as follows. They generate the commitment curve by sampling an $\mathbb{F}_p$-rational isogeny $\psi_1 : E_A \to E_1'$, and completing it with a very short non $\mathbb{F}_p$-rational isogeny $\psi_2 : E_1' \to E_1$ to obtain $\psi := \psi_2 \circ \psi_1 : E_A \to E_1$. When they receive the challenge $\varphi : E_A \to E_2$, they factor it as $\varphi = \varphi_2 \circ \varphi_1$ where $\varphi_1 : E_A \longrightarrow E_2'$ is $\mathbb{F}_p$-rational and $\varphi_2 : E_2' \longrightarrow E_2$, if any, is not $\mathbb{F}_p$-rational. From the knowledge of $\varphi_1 \circ \widehat{\psi_1} : E_1' \longrightarrow E_2'$, they generate a short ($\mathbb{F}_p$-rational) isogeny $\sigma_0 : E_1' \to E_2$ using PEGASIS. They return $\sigma = \varphi_2 \circ \sigma_0 \circ \widehat{\psi_2} : E_1 \to E_2$ as response. The attack is illustrated in Figure 7.

Note that in the attack described above, the response isogeny is allowed to backtrack the challenge isogeny as they both factor through φ_2. While this is allowed in SQISIgn2D-West [5] and in the official version of SQIsign [1], several variants of SQIsign do not allow it. When the response isogeny is not allowed to

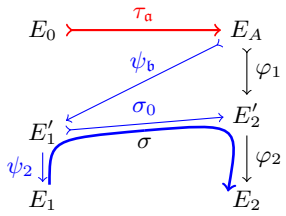


Fig. 7. Attack when the challenge isogeny factors through $\mathbb{F}_p$.

backtrack the challenge isogeny, then the attack only applies when E_2 is defined over $\mathbb{F}_p$.

To prevent the attacks and failures we have discussed up to now and to ensure a successful design of the extractor we will use when proving soundness, we impose the following requirements:

1. The commitment curve E_1 should be defined over $\mathbb{F}_{p^2}$ (and not over $\mathbb{F}_p$).
2. The prime factors of the degree of the response isogeny σ should all be inert in $\mathfrak{O} \simeq \mathbb{Z}[\pi]$.
3. The challenge isogeny should not "trivially" factor through an $\mathbb{F}_p$-rational isogeny. By this we mean that no non-trivial subgroup of the kernel of the challenge isogeny should be fixed by the Frobenius.

The first requirement is to prevent the attack/issues from Section A.1 while the second and third ones are to prevent the attack/issues described earlier in this section. Now that the prime factors of the degree of the response isogeny are all inert in $\mathfrak{O} \simeq \mathbb{Z}[\pi]$, with respect to the attack depicted in Figure 7, the attacker needs to know at least a rank 4 suborder of the endomorphism ring of the curves at play in order to be successful. This means that they need to know a non $\mathbb{F}_p$-rational endomorphism of E_A, which is exactly the hard problem underlying the security of WaterSQI.

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 22. *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 22 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 $\sigma : E_A \to E'$ 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 $\sigma : E_A \to E'$ 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:

- $\sigma \leftarrow \mathsf{GenIsogeny_O}(E, \phi, q)$ 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[3] 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.
- $\mathsf{accept/reject} \leftarrow \mathsf{VerIsogeny_O}(\sigma, E, q)$ 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 22, 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 [3,

[3] 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 $\mathsf{GenIsogeny_O}$ being practically the same as that of $\mathsf{GenIsogeny}$ for the same field size.

Prop. 2]) after adjusting the SPEDIO oracle and the underlying hard problem as summarised bellow.

Definition 23. *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.*

Problem 24. Given a random supersingular elliptic curve E defined over $\mathbb{F}_p$ and a 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 25. *If $\mathsf{H}_{\mathsf{Prime}}$ is a collision-resistant cryptographic hash function and Problem 24 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	279	223
p_{1000}	126	530	348
p_{2000}	254	1043	604
$p \approx 2^{2\mu\lambda}$	$\mu\lambda/4$	$(\mu + 1/8)\lambda + \log(2\mu\lambda)$	$(2\mu + 3)\lambda/4$

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	1.9 s	5.8 s	34.6 s
	Sign	2.2 m	6.7 m	37.0 m
	Verify	2.2 m	6.6 m	36.1 m
Generalised CSI-FiSh $(2^4, 23, 14)$	KeyGen	28.0 s	1.4 m	7.8 m
	Sign	43.0 s	2.2 m	12.1 m
	Verify	42.8 s	2.2 m	11.7 m

Table 4. Runtimes estimates from our proof of concept implementation in Sagemath of PRISMO (100 runs) and Generalised CSI-FiSh (10 runs). Timing were obtained on a Macbook Pro with an M1 chip.

Protocol	$p \approx 2^{2\mu\lambda}$					
				Type of isogeny		
	$\|\mathsf{pk}\|$	$\|\mathsf{sig}\|$		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	$\mu\lambda/4$	$(\mu+1/8)\lambda$ $+\log(2\mu\lambda)$	KeyGen	-	$2\mu\lambda$	-
			Sign	5λ	$\mu\lambda + 2\log(2\mu\lambda)$	-
			Verify	λ	$\mu\lambda + 2\log(2\mu\lambda)$	-
WaterSQI	$\mu\lambda/4$	$(\mu+1/8)\lambda$ $+\log(2\mu\lambda)$	KeyGen	-	$2\mu\lambda$	-
			Sign	λ	$4\mu\lambda$	-
			Verify	λ	$\mu\lambda + 2\log(2\mu\lambda)$	-
Generalised CSI-FiSh (S, t, k)	$(S-1)\mu\lambda/4$		KeyGen*	-	-	$2(S-1)\mu\lambda$
			Sign*	-	-	$2t\mu\lambda$
			Verify*	-	-	$2t\mu\lambda$
SQI-FiSh (S, t, k)	$(S-1)\mu\lambda/4$		KeyGen	-	$2(S-1)\mu\lambda$	-
			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.