Exploring SIDH-based Signature Parameters

Andrea Basso[1], Mingjie Chen[2], Tako Boris Fouotsa[3], Péter Kutas[2,4], Abel Laval[5], Laurane Marco[3], and Gustave Tchoffo Saah[6]

[1] University of Bristol, Bristol, United Kingdom; andrea.basso@bristol.ac.uk
[2] University of Birmingham, Birmingham, United Kingdom; m.chen.1@bham.ac.uk
[3] EPFL, Lausanne, Switzerland {tako.fouotsa, laurane.marco}@epfl.ch
[4] Eötvös Loránd University; p.kutas@bham.ac.uk
[5] Université Libre de Bruxelles; abel.laval@ulb.be
[6] Université de Yaoundé 1, Cameroon; gustavesaah@gmail.com

Abstract. Isogeny-based cryptography is an instance of post-quantum cryptography whose fundamental problem consists of finding an isogeny between two (isogenous) elliptic curves E and E'. This problem is closely related to that of computing the endomorphism ring of an elliptic curve. Therefore, many isogeny-based protocols require the endomorphism ring of at least one of the curves involved to be unknown. In this paper, we explore the design of isogeny based protocols in a scenario where one assumes that the endomorphism ring of all the curves are public. In particular, we identify digital signatures based on proof of isogeny knowledge from SIDH squares as such a candidate. We explore the design choices for such constructions and propose two variants with practical instantiations. We analyze their security according to three lines, the first consists of attacks based on KLPT with both polynomial and superpolynomial adversary, the second consists of attacks derived from the SIDH attacks and finally we study the zero-knowledge property of the underlying proof of knowledge.

1 Introduction

Isogeny-based cryptography is a promising candidate to develop quantum-secure protocols. At its core, lies the fundamental assumption that it is computationally hard to find an isogeny between two isogenous elliptic curves. When the curves are supersingular, the setting of nearly all modern constructions [18, 41, 16, 27, 38, 25, 21, 33, 10], the isogeny problem is strictly linked to the endomorphism ring problem. The latter asks to find a basis of the ring of all the endomorphisms of a supersingular elliptic curve, i.e. all the isogenies from the curve to itself. The problem of finding an isogeny between two elliptic curves reduces to the endomorphism-ring problem: given two curves and a representation of their endomorphism rings, it is possible to compute an isogeny connecting them in polynomial time [42, 55].

Due to this connection, the endomorphism ring problem and its relationship to the security of many isogeny-based protocols have been extensively studied. The best known algorithm to compute endomorphism rings is due to Eisenträger, Hallgren, Leonardi, Morrison, and Park [29], and it runs in $\tilde{\mathcal{O}}(p^{1/2})$ time, where p is

the characteristic of the underlying finite field (the result relies on some heuristics which were removed in [35]). Given a curve E_0 with known endomorphism ring $\mathrm{End}(E_0)$, and an isogeny $\phi : E_0 \to E$, one can push the endomorphism ring $\mathrm{End}(E_0)$ of E_0 through ϕ to recover $\mathrm{End}(E)$ [42, 55]. Thus, finding an isogeny between a curve E_0 with known endomorphism ring, and a given curve E solves the endomorphism ring problem for the curve E. Since the characteristic p is exponential in the security parameter in practice, the general endomorphism ring problem remains hard.

It remains of interest to understand how the security of isogeny-based protocols is affected when an attacker has knowledge of the endomorphism rings. In several protocols, such as the GPS signature [37], SÉTA [21], SQISign [25] and SQISignHD [20], the secret keys are directly linked to a description of the endomorphism ring. Thus, solving the endomorphism ring problem trivially breaks such protocols. In other schemes, such as SIDH [41], CSIDH [16] and SCALLOP [23], CSI-FiSh–[13], SeaSign [24] , the secret isogenies have specific properties: if the endomorphisms of all curves were known, a direct application of [42, 55] would prevent obtaining the correct isogeny. Nonetheless, it has been shown that the additional information that such protocols reveal, such as short degrees, torsion images or orientations, is sufficient to recover the secret isogeny [36, 17, 54, 32]. More recently proposed schemes, such as M-SIDH/MD-SIDH [33], FESTA [10] and binSIDH/terSIDH [8] compute isogenies of degree roughly $\sqrt{p}$ or even smaller, hence the attack in [36] trivially extends to those cases when endomorphism rings of curves are public. Moreover, many other protocols are insecure when the starting curves have known endomorphism ring. This is the case, for instance, for the CGL hash function [18, 28], the CSIDH-based oblivious transfer protocols [43, 5], the commitment scheme by Sterner [50], the SIDH-based oblivious pseudorandom functions [14, 9, 6], and the hash proof systems and dual-mode PKEs based on group actions [3].

The relevance of endomorphism rings in isogeny-based cryptography and the consequences of their knowledge on security raises the following natural question:

Can we construct a secure cryptographic protocol where the endomorphism rings of all curves are public?

One has to remark that one of the most natural algorithmic problems, namely finding an isogeny of a fixed degree d between supersingular elliptic curves, is not known to be equivalent to the endomorphism ring problem. An efficient classical equivalence between finding fixed degree isogenies and computing endomorphism rings would have important consequences, e.g., a significant speed-up of SQIsign. Understanding whether we can build protocols which are secure even if endomorphism rings of all curves is public has both theoretical and practical consequences. On the theoretical side, a protocol that remains secure when the endomorphism rings of all curves are known shows that, even if the endomorphism ring problem is efficiently solvable, some isogeny-based constructions are still possible, and retain some security. On the practical side, the complexity of the endomorphism-recovering attacks generally imposes primes p with $p > 2^{2\lambda}$; without requiring

endomorphism rings to remain secret, it is possible to design protocols with smaller primes, leading to more efficient and more compact protocols.

Contributions. In this paper, we develop two protocols that appear to be secure, even if the endomorphism rings of all elliptic curves are public. This suggests an affirmative response to the question set out in the introduction (even though further cryptanalysis is necessary).

Both protocols are digital signatures, based on a proof of isogeny knowledge built on top of SIDH squares. In this work, we focus on digital signatures since it is the primitive that is most likely to be secure when endomorphism rings are known: the SIDH-based constructions generally reveal little information besides the degrees and the end curves of secret isogenies. Indeed, it is possible to construct SIDH-based signatures that do not reveal any torsion information [22] or that are statistically independent from the secret key [7].

In this work, we analyze existing constructions of proofs of isogeny knowledge and identify three main design choices (Section 3). We also propose two practical instantiations, which are plausibly secure despite the underlying prime field having characteristic smaller than $2^{2\lambda}$.

To analyze the security of the proposed constructions, we identify and study three main lines of attacks. The first approach relies on the knowledge of endomorphism rings and the KLPT algorithm [42]. We analyze these attacks extensively in Section 4. Moreover, the KLPT algorithm has always been considered for constructive applications, and thus its analysis in the literature is bounded to polynomial running times. In this work, we study the output of the KLPT algorithm when running in superpolynomial time, which may be of independent interest. The method used is a variation of [45, Section 3.4.].

We also consider attacks based on the recent attacks on SIDH (Section 5.1) and based on the lack of zero-knowledge of the underlying sigma protocol (Section 5.2). The results of these analyses shows that it is possible to design signatures based on proofs of isogeny knowledge with binary challenges, which are more efficient and compact than those based on proofs with ternary challenges (see (**??** for an estimate of the concrete sizes). Combined with the previous analysis of KLPT-based attacks, this provides an argument for the security of the proposed constructions.

2 Preliminaries

2.1 Σ protocols and digital signatures

Definition 1 (Sigma Protocol). *A sigma protocol is a three-move proof system for a language $\mathcal{L}$ consisting of oracle-calling PPT algorithms $(P = (P_1, P_2), V = (V_1, V_2))$, where V_2 is deterministic. We assume P_1 and P_2 share states and so do V_1 and V_2. Let* ChallSet *denote the challenge set. Then, the protocol proceeds as follows.*

– *The prover, on input* $(\mathsf{st}, \mathsf{wt}) \in \mathcal{L}$*, computes* $\mathsf{com} \longleftarrow P_1(\mathsf{st}, \mathsf{wt})$ *and sends the commitment* com *to the verifier.*
– *The verifier computes* $\mathsf{chall} \longleftarrow V_1(1^\lambda)$*, drawing a random challenge from* ChallSet*, and sends it to the prover.*
– *The prover, given* chall*, computes* $\mathsf{resp} \longleftarrow P_2(\mathsf{st}, \mathsf{wt}, \mathsf{chall})$ *and returns a response* resp *to the verifier.*
– *The verifier runs* $V_2(\mathsf{st}, \mathsf{com}, \mathsf{chall}, \mathsf{resp})$ *and outputs* $\top$ *(accept) or* $\bot$ *(reject).*

A sigma protocol is said to be *correct* if knowing wt is enough for the prover to convince the verifier that they indeed know the witness; it is said to be n-*special sound* if being able to produce n valid transcripts $(\mathsf{st}, \mathsf{com}, \mathsf{chall}_i, \mathsf{resp}_i)$, $i \in \{1, 2, \ldots, n\}$ for the same statement and commitment but for different challenges implies being able to compute a witness for this given statement st; it is zero-knowledge if anyone can simulate it and produce a valid transcript computationally indistinguishable from one obtained by actually running the protocol. If the soundness error of the protocol is too high, one can reduce it is using repetition.

If the statement is a public key and the witness is the corresponding secret key, we call such a protocol an *identification scheme*. It is typically used to give, as its name indicates, a proof of identity. Furthermore, a sigma protocol can be turned into a digital signature in the Random Oracle Model using the *Fiat-Shamir transform* [31].

2.2 Supersingular isogenies

Let E_1 and E_2 be two supersingular curves defined over a finite field $\mathbb{F}_{p^2}$. An isogeny $\phi : E_1 \to E_2$ is a non-constant rational map which is also a group morphism with respect to the group structure of the elliptic curves. The degree of an isogeny is its degree as a rational map. It is always of the form $d = p^r d'$, and when $r = 0$ (that is $d = d'$ is coprime to p) we say the isogeny ϕ is separable and we have $d = \#\ker\phi$. The isogenies considered in this work are all separable, unless stated otherwise. An isogeny of small prime degree can be efficiently computed (and evaluated on torsion points) from a description of its kernel using Vélu formulas [52] or the square root Vélu formulas [11]. Isogenies of smooth degree can also be efficiently computed by writing them as a composition of isogenies of small prime degrees. For any isogeny $\phi : E_1 \to E_2$, there exists a unique isogeny $\widehat{\phi} : E_2 \to E_1$ such that $\widehat{\phi} \circ \phi = [\deg\phi]_{E_1}$ and $\phi \circ \widehat{\phi} = [\deg\phi]_{E_2}$. The isogeny $\widehat{\phi}$ is called the dual of ϕ. An endomorphism of an elliptic curve E is an isogeny from E to E. The set of all the endomorphisms of E forms a ring under addition and composition. It is denoted by $\mathrm{End}(E)$ and its called the endomorphism ring of E. Over finite fields, the endomorphism ring of an elliptic curve is either an order in an imaginary quadratic field or a maximal order in a quaternion algebra. The earlier case occurs for ordinary curves while the later occurs for supersingular curves, which are the ones used in this paper.

2.3 Quaternion Algebra

Let p be a prime. We write $\mathcal{B}_{p,\infty}$ for the quaternion algebra ramified only at p and ∞, which is defined by

$$\mathcal{B}_{p,\infty} = \left(\frac{-q,-p}{\mathbb{Q}}\right) = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + k\mathbb{Q}$$

where $0 \neq q \in \mathbb{N}$, $i^2 = -q$, $j^2 = -p$, and $k = ij = -ji$.

A p-extremal maximal order is a maximal order containing j. Examples of p-extremal maximal order are those containing $\mathbb{Z}\langle i, j\rangle = \mathbb{Z} + i\mathbb{Z} + j\mathbb{Z} + k\mathbb{Z}$ as subring. For such a maximal order $\mathcal{O}$, if $R = \mathcal{O} \cap \mathbb{Q}[i]$ is the ring of integers $\mathbb{Z}[\omega]$ of $\mathbb{Q}[i]$, then the restriction of the norm to $R + Rj$ is given by

$$\mathrm{Nrd}(x_1 + y_1\omega + (x_2 + y_2\omega)j) = f(x_1, y_1) + pf(x_2, y_2)$$

where f is a principal quadratic form of discriminant $\mathrm{disc}(R)$ [42]. We have

$$f(x, y) = x^2 + \mathrm{Trd}(\omega)xy + \mathrm{Nrd}(\omega)y^2$$

We give below a few examples of the structure of $\mathcal{B}_{p,\infty}$, together with p-extremal order $\mathcal{O}$, R and $f(x, y)$ as defined above for different values of p.

Example 2.

1. For $p \equiv 3 \bmod 4$: $\mathcal{B}_{p,\infty} = \left(\frac{-1,-p}{\mathbb{Q}}\right)$; $\mathcal{O} = \langle 1, i, \frac{1+k}{2}, \frac{i+j}{2}\rangle$; $R = \mathbb{Z}[i]$; $f(x, y) = x^2 + y^2$.
2. For $p \equiv 5 \bmod 8$: $\mathcal{B}_{p,\infty} = \left(\frac{-2,-p}{\mathbb{Q}}\right)$; $\mathcal{O} = \langle 1, i, \frac{1+j+k}{2}, \frac{i+2j+k}{4}\rangle$; $R = \mathbb{Z}[i]$; $f(x, y) = x^2 + 2y^2$.
3. For $p \equiv 3 \bmod 4$: $\mathcal{B}_{p,\infty} = \left(\frac{-q,-p}{\mathbb{Q}}\right)$, where $q \equiv 1 \bmod 4$ is a prime such that $\left(\frac{-p}{q}\right) = 1$; $\mathcal{O} = \langle 1, \frac{1+i}{2}, j, \frac{ci+k}{q}\rangle$, where $c^2 \equiv -p \bmod q$; $R = \mathbb{Z}[\frac{1+i}{2}]$; $f(x, y) = x^2 - xy + \frac{1+q}{4}y^2$.

2.4 SIDH

The Supersingular Isogeny Diffie-Hellman (SIDH) protocol was introduced in 2011 by Jao and De Feo [41]. It is a Diffie-Hellman type key exchange that uses supersingular isogenies. Supersingular isogenies do not commute in general. In order to get a commutative diagram that will help compute the shared secret in SIDH, the images of some torsion points basis through the secret isogenies are included in the public keys (see Figure Fig. 1). Moreover, in order to achieve the best possible efficiency, one uses isogenies of degree 2^a or 3^b between supersingular elliptic curves defined over $\mathbb{F}_{p^2}$ where the characteristic p is of the form $p = 2^a 3^b f - 1$, with f being a small co-factor. Primes of the form $p = 2^a 3^b f - 1$ (or $p = \ell_1^{e_1}\ell_2^{e_2} f - 1$ more generally) are usually referred to as *SIDH primes*.

The detailed description of SIDH is as follows.

Setup. Let $p = 2^a 3^b f - 1$ be an SIDH prime and let E_0 be a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$. Let $E_0[2^a] = \langle P_a, Q_a\rangle$ and $E_0[3^b] = \langle P_b, Q_b\rangle$.

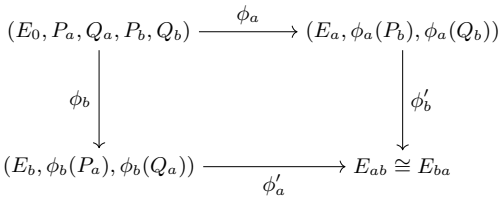
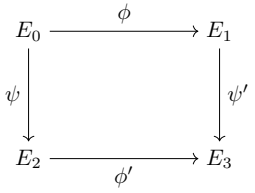


Fig. 1: The SIDH key exchange protocol

Key generation. Alice samples a random scalar $k_a \in \mathbb{Z}/2^a\mathbb{Z}$, and computes the isogeny $\phi_a : E_0 \to E_A$ whose kernel is $\langle P_a + [k_a]Q_a \rangle$. Her secret key is k_a and her public key is $(E_a, \phi_a(P_b), \phi_a(Q_b))$. Similarly, Bob samples a random scalar $k_b \in \mathbb{Z}/3^b\mathbb{Z}$, and computes the isogeny $\phi_b : E_0 \to E_B$ whose kernel is $\langle P_b + [k_b]Q_b \rangle$. His secret key is k_b and his public key is $(E_b, \phi_b(P_a), \phi_b(Q_a))$.

Shared secret. Given Bob's public key $(E_b, \phi_b(P_a), \phi_b(Q_a))$, Alice computes the isogeny $\phi'_a : E_b \to E_{ba}$ whose kernel is generated by $\phi_b(P_a) + [k_a]\phi_b(Q_a)$. Given Alice's public key $(E_a, \phi_a(P_b), \phi_a(Q_b))$, Bob computes the isogeny $\phi'_b : E_a \to E_{ab}$ whose kernel is generated by $\phi_a(P_b) + [k_b]\phi_a(Q_b)$. The shared secret is $j(E_{ab}) = j(E_{ba})$.

In SIDH, the isogenies ϕ_A and ϕ'_A (resp. ϕ_B and ϕ'_B) are said to be *parallel isogenies*. In general, two isogenies $\phi : E_0 \to E_1$ and $\phi' : E_2 \to E_3$ are said to be parallel if there exists an isogeny $\psi : E_0 \to E_2$ such that $\ker \phi' = \psi(\ker \phi)$. Note that if $\phi : E_0 \to E_1$ and $\phi' : E_2 \to E_3$ are parallel, then $\widehat{\phi} : E_1 \to E_0$ and $\widehat{\phi'} : E_3 \to E_2$ are also parallel since $\ker \widehat{\phi'} = \psi'(\ker \widehat{\phi})$ where ψ' is the isogeny whose kernel is given by $\ker \psi' = \phi(\ker \psi)$. We hence obtain a square (Eq. (1)) which is called an *SIDH square*.



(1)

2.5 Algorithms for computing isogenies

We discuss some existing algorithms for computing isogenies that will be of interest in this paper. The main problem, which is that of finding an isogeny connecting two isogenous supersingular curves is believed to be hard. Nevertheless, it may not be the case when more information is provided: the endomorphism rings of the curves and/or some torsion point information and/or the degree of the isogeny.

When the endomorphism rings of the curves are public, then a result of [36] shows that the secret isogeny $\phi : E_1 \to E_2$ can be recovered whenever it is

the shortest isogeny connecting E_1 to E_2. This result is formally given by the following theorem.

Theorem 3. *Let E_1 and E_2 be two supersingular curves, and let $\phi : E_1 \to E_2$ be the shortest isogeny connecting E_1 and E_2. Given a description the endomorphism rings $\mathcal{O}_1 \simeq End(E_1)$ and $\mathcal{O}_2 \simeq End(E_2)$, there exists an efficient algorithm that computes the isogeny ϕ.*

Note that Theorem 3 is a straightforward generalization of [36, Theorem 1] where the degree of the isogeny ϕ is a prime power to the case where there is no restriction on the degree of the isogeny. Two uniformly random supersingular curves are always connected by an isogeny of degree at most $O(\sqrt{p})$. Hence the attack in Theorem 3 does not help to recover isogenies of degree $d \gg \sqrt{p}$. In [32], it is shown that if some reasonable amount of torsion point information is provided beside the endomorphism rings, then the secret isogeny can be efficiently recovered. More precisely, we have the following theorem which can be found in [32, Theorem 3.8].

Theorem 4. *Let E_1 and E_2 be two supersingular curves, and let d be the degree of the shortest isogeny connecting E_1 and E_2. Let $\phi : E_1 \to E_2$ be an isogeny of degree $N_1 \geq d$. Let N_2 be a smooth integer, set $E_1[N_2] = \langle P, Q \rangle$. Given $\phi(P)$, $\phi(Q)$ and a description the endomorphism rings $\mathcal{O}_1 \simeq End(E_1)$ and $\mathcal{O}_2 \simeq End(E_2)$, there exists an efficient algorithm that computes the isogeny ϕ provided that $N_1 \leq \frac{dN_2}{16}$.*

In practice, the endomorphism ring of the co-domain curve of the isogeny is not provided. In 2017, Petit [47] described an attack that only requires the knowledge of a special endomorphism on the starting curve, and a large amount of torsion point information. This attack was later improved in [48] but still required torsion point images of large order. In 2022, a series of three papers [15, 44, 49] consecutively improved the state of art to reach a point where no known endomorphism is required and the amount of torsion point needed is way smaller than the degree of the isogeny: a supersingular isogeny of degree N_1 can be efficiently recovered from its action on torsion points of smooth order N_2 where $N_1 < N_2^2$. These results led to a complete break of SIDH and are summarized in Theorem 5, which is based on [49, Theorem 1].

Theorem 5. *Let E_1 and E_2 be two supersingular curves, let N_2 be a smooth integer and let $E_1[N_2] = \langle P, Q \rangle$. Let $\phi : E_1 \to E_2$ be an isogeny of degree N_1. Given $\phi(P)$, $\phi(Q)$ there exists an efficient algorithm that computes the isogeny ϕ provided that $N_1 < N_2^2$.*

It may happen that when attempting to recover the secret isogeny, one does not directly have access to torsion point images, but to images of some cyclic groups of the same order N. In [9, 34], it is proven that if N has $O(\log \log p)$ prime factors, then one can efficiently recover the torsion point information from the images of three disjoint cyclic groups of order N. This implies that the secret isogeny can in fact be recovered from the images of three disjoint cyclic groups of order N.

3 Signatures based on SIDH squares

In this section, we recall various constructions of proofs of isogeny knowledge from the literature and we highlight the main design options. We also introduce the potential lines of attack against some constructions, which are analyzed in detail in the following sections. For a comprehensive survey of proofs of isogeny, we refer the reader to [12], [40].

Let us assume that a prover wants to demonstrate knowledge of a cyclic isogeny $\phi : E_0 \to E_1$ of smooth degree d. The main framework, on which the following proofs are based on, is a sigma protocol due to De Feo, Jao, and Plût [30]. The prover generates the SIDH square in Eq. (1) where ψ has degree ℓ^n for some ℓ coprime with d, and they commit to E_2 and E_3. The verifier sends a challenge bit $c \in \{0, 1\}$: if $c = 0$, the prover responds with the horizontal isogeny ϕ', and if $c = 1$, the prover reveals the vertical isogenies ψ and ψ'. The verifier accepts if the response isogenies have the correct domain and codomain. The protocol has soundness error of $1/2$, and thus it needs to be repeated λ times to obtain a negligible soundness error of $2^{-\lambda}$. As pointed out in [39, 22] , a malicious prover may not necessarily know ϕ (such an isogeny might not exist at all); the proof in [30] is thus sound with respect to the weaker relation

$$\mathcal{R}_{\mathsf{weak}} = \left\{ ((E_0, E_1), \phi) \;\middle|\; \begin{array}{c} \phi : E_0 \to E_1 \text{ is a cyclic } \ell^{2i}d\text{-isogeny,} \\ \text{for some integer } i \text{ and } \ell \text{ coprime with } d \end{array} \right\}. \tag{2}$$

In the case of an honest prover, this proof also reveals the action of ϕ on the torsion $E[\deg \psi]$ since the isogenies ψ and ψ' are parallel. This makes it potentially vulnerable to the recent attacks on SIDH [15, 44, 49].

The authors of [22] showed that it is possible to have a proof that is sound with respect to the strong relation

$$\mathcal{R}_{\mathsf{strg}} = \{((E_0, E_1), \phi) \mid \phi : E_0 \to E_1 \text{ is a cyclic } d\text{-isogeny}\} \tag{3}$$

by ensuring that ψ and ψ' are parallel. However, to avoid the SIDH attacks and a technical issue with zero-knowledge[7], they have to resort to a proof with ternary challenges. Thus, to prove parallelness, the prover constructs the same SIDH square as in Eq. (1), but additionally commits to P_2, Q_2[8], a basis of $E_2[d]$, its image $P_3 := \phi'(P_2), Q_3 := \phi'(Q_2)$ on E_3, and the coefficients a, b such that $\ker \hat{\psi} = \langle [a]P_2 + [b]Q_2 \rangle$ and $\ker \hat{\psi}' = \langle [a]P_3 + [b]Q_3 \rangle$. The curves E_2 and E_3 are also committed with a hiding commitment scheme. Then, the challenges are ternary, i.e. $c \in \{-1, 0, 1\}$. When $c = \pm 1$, the verifier reveals a, b and either $(E_2, (P_2, Q_2))$ or $(E_3, (P_3, Q_3))$; the verifier reconstructs ψ or ψ' and ensures they have the correct codomain. In the case of $c = 0$, the verifier receives $(\phi', (E_2, P_2, Q_2), (E_3, P_3, Q_3))$ and checks that the points P_3, Q_3 are the images

[7] The Σ protocol with binary challenges does not satisfy the common definitions of zero-knowledge. This, however, does not constitute a problem when it is transformed into a signature scheme, as shown in Section 5.2.

[8] This basis can be generated canonically, which avoids the need of its commitment.

of P_2, Q_2 under ϕ'. In all cases, the verifier also ensures the revealed values match the previously committed ones.

More recently, [7] introduced the concept of an *SIDH ladder*, which is obtained by gluing multiple SIDH squares together. This removes the requirement on the prime being an SIDH prime. It is thus possible to prove knowledge of an isogeny ϕ in *any* characteristic and even if ϕ and ψ have kernels that are not defined over $\mathbb{F}_{p^2}$.

This historical overview suggests there are three main design choices that determine how a proof of isogeny knowledge works:

1. The soundness relation: strong vs weak,
2. The challenge space: binary vs ternary,
3. The characteristic p and the degrees of ϕ and ψ.

Note that not all combinations are possible. For instance, when the kernels of ψ and ψ' are not rational over $\mathbb{F}_{p^2}$, which requires using the SIDH ladder method proposed by [7], there is no known technique to prove the strong relation.

3.1 Proposed constructions

We now discuss some promising combinations and study their securities in later sections. Let E_0 be a random supersingular elliptic curve, ℓ_1 be a small prime and e_1 be a positive integer. Our goal is to prove the knowledge of a secret isogeny $\phi : E_0 \to E_1$ of degree $\ell_1^{e_1}$ in $\mathcal{R}_{\mathsf{strg}}$.

Variant 1. This variant proves the knowledge of the **strong** relation, and uses a **binary** challenge space. Let public parameters $pp = (p, \ell_1, \ell_2, e_1, e_2, E_0)$ be such that $\#E_0(\mathbb{F}_{p^2}) = (\ell_1 \ell_2^{e_2} f)^2$, for $\ell_2^{e_2}$ of roughly the same size as in SIDH ([2]) and $d = \ell_1^{e_1} \gg \ell_2^{e_2}$, or $d = \ell_1^{e_1} \approx 2^{\lambda}(\ell_2^{e_2})^2$. Note that in this setting, $p = \ell_1 \ell_2^{e_2} f - 1 \approx \ell_2^{e_2}$ and thus it is smaller than $2^{2\lambda}$. Note also that E_0 is not a special curve and can in fact be generated by taking a long enough walk from $j = 1728$.
Intuitively, the protocol is as described earlier in this section and the rigorous version is given in [22, Figure 2]. The only difference is, the horizontal isogeny ϕ' is represented by a sequence of isogenies of degree ℓ_1 instead of a kernel point of order $\ell_1^{e_1}$. As noted in [22], this sigma protocol has 2-special soundness, but does not satisfy the zero-knowledge (ZK) property if the distinguisher used in the ZK definition has access to the witness. We explore in Section 5.2 how we can still retain the security of the derived signature.

Variant 2. This variant also proves the knowledge of the **strong** relation, but uses a **ternary** challenge space. The requirements on the public parameters are similar to Variant 1, with $p \approx \ell_1^{e_1} \ell_2^{e_2}$ as in SIDH, so $p \approx 2^{216}$ for $\lambda = 128$. The description of the protocol is as given in [22, Figure 3]. Note again that we represent ϕ' by a sequence of isogenies of degree ℓ_1. This sigma protocol has 3-special soundness and zero-knowledge. Note that in this variant, E_0 does not need to be a random supersingular elliptic curve, and rather can be taken to be a special curve with an extremal order as endomorphism ring.

4 Analysis of KLPT-based attacks

In this section, we analyze KLPT-based attacks that break the security of SIDH-based signatures and proofs of knowledge. The attacks follow two main approaches: they can either recover the secret key from the public information, or they can forge a valid signature even if they fail to recover the secret key.

In the first approach, the attacker recovers a d-isogeny $\phi : E_0 \to E_1$, given the domain and codomain curves E_0, E_1 and their endomorphism rings.

This problem is linked to the problem of finding an ideal of norm d, connecting the maximal orders $\mathcal{O}_0 \cong \mathrm{End}(E_0)$ and $\mathcal{O}_1 \cong \mathrm{End}(E_1)$ through the computational Deuring correspondence [37, 26]. In [42, 37], the authors propose polynomial algorithms to find such ideal of smooth norm. A strategy to find a witness for the above relations could then be as follows:

1. Find an ideal I connecting $\mathcal{O}_0$ to $\mathcal{O}_1$;
2. Use the KLPT algorithm to compute an ideal J of norm d equivalent to I;
3. Use the computational Deuring correspondence to compute an isogeny corresponding to J.

The KLPT algorithm produces ideals of norm in $O(3\log(p))$ if either $\mathcal{O}_0$ or $\mathcal{O}_1$ is a special extremal order [46, 42, 37], and $O(\frac{9}{2}\log(p))$ in the general case [46, 25]. Hence, this strategy potentially fails for some $d \leq p^3$ or $d \leq p^{\frac{9}{2}}$, depending on the curves E_0 and E_1.

A second attack strategy sidesteps these limitations and can possibly break the security of the protocol even when the secret isogeny is shorter than p^3. When the underlying sigma protocol is sound with respect to the weak relation $\mathcal{R}_{\mathsf{weak}}$, the prover demonstrates knowledge of an isogeny between E_0 and E_1 of degree $\ell^{2i}d$, for some integer i and ℓ coprime with d. An attacker can thus attempt to forge a proof, even without knowing the witness, by using the KLPT-based approach described above to compute an isogeny of degree $\ell^{2i}d$. Such an isogeny can then be written as the composition $\hat{\psi}' \circ \phi' \circ \psi$, where ϕ' is a d isogeny and ψ, ψ' have degree ℓ^i; the attacker can then correctly reply to any challenge. This attack can be avoided if the composition isogeny is shorter than the shortest isogeny returned by KLPT, or if the Sigma protocol is sound with respect to $\mathcal{R}_{\mathsf{strg}}$: in that case, this approach would fail to produce isogenies $\hat{\psi}'$ and ψ that are parallel, because the isogenies ϕ' and parallel isogenies $\hat{\psi}'$ and ψ uniquely determine ϕ, which is too short to be determined by a KLPT-based attack.

In this section, we analyze the minimal norm of the ideal that KLPT can return. We extend the previous results by studying exponential-time algorithms and showing that there is a trade-off between KLPT's running time and the norm of the smallest ideal it can produce.

4.1 The KLPT algorithm for extremal order

We recall the following lemma from [42].

Lemma 6 ([42]). *Let I be a left $\mathcal{O}$-ideal and $\alpha \in I$. Then $I\frac{\bar{\alpha}}{Nrd(I)}$ is a left $\mathcal{O}$-ideal of norm $\frac{Nrd(\alpha)}{Nrd(I)}$.*

As consequence of this lemma, finding an equivalent $\mathcal{O}$-ideal of I which has a norm in a certain set $\mathcal{N}$ consists of finding an element in I of norm $nNrd(I)$, for some $n \in \mathcal{N}$. Let $\mathcal{O}$ be one of the special extremal maximal orders given in Example 2; I an $\mathcal{O}$-left ideal and ℓ a small prime. KLPT algorithm can be summarized as follows:

1. Compute an ideal J of prime norm equivalent to I, such that ℓ is a quadratic non-residue modulo N;
2. Find an element $\gamma \in \mathcal{O}$ of norm $N\ell^{e_1}$ for some $e_1 \in \mathbb{N}$;
3. Find an element $\alpha \in J$ such that $J = \mathcal{O}\alpha + N\mathcal{O}$;
4. Compute $\mu_0 \in Rj$ such that $\gamma\mu_0 \equiv \alpha \bmod N\mathcal{O}$;
5. Compute $\lambda \in \mathbb{Z}/N\mathbb{Z}^*$ and $\mu_1 \in \mathcal{O}$ such that $\mu = \lambda\mu_0 + N\mu_1$ has norm ℓ^{e_2}, for some $e_2 \in \mathbb{N}$
6. Return $J\frac{\bar{\beta}}{N}$, where $\beta = \gamma\mu$.

In Step 1, one computes a reduced basis of I and generates a small set of short elements until an element of norm $N\,\mathrm{Nrd}(I)$ is found for which N is prime. Experimentally, this algorithm returns an ideal of prime norm N, where $N \simeq \sqrt{p}$.

In Step 2, one solves the norm equation

$$f(x_1, y_1) = N\ell^{e_1} - pf(x_2, y_2). \tag{4}$$

In Step 3, it is enough to find an element $\alpha \in J$ such that $gcd(N^2, \mathrm{Nrd}(\alpha)) = N$. For such α, we have $J = \mathcal{O}\alpha + N\mathcal{O}$ i.e $J/N\mathcal{O} = \mathcal{O}\alpha/N\mathcal{O}$.

The idea of Step 4 is that $\mathcal{O}/N\mathcal{O}$ is isomorphic to $M_2(\mathbb{Z}/N\mathbb{Z})$ (an explicit isomorphism can be computed using [53, Proposition 7.6.2]) and thus every left ideal only differs by a quaternion whose reduced norm is coprime to N and such an element can actually be chosen from Rj. Step 5 consists of finding $\mu \equiv \lambda\mu_0$ mod $N\mathcal{O}$ of norm ℓ^{e_2}. One has to look for $\mu_1 = x + y\omega + (z + t\omega)j \in R + Rj$ and $\lambda \in \mathbb{Z}/N\mathbb{Z}$ such that $\mathrm{Nrd}(\mu) = \ell^{e_2}$ where $\mu = \lambda\mu_0 + N\mu_1$. For such μ, we have

$$\mu = N(x + y\omega) + [Nz + \lambda C + (Nt + \lambda D)\omega]j.$$

Hence $\mathrm{Nrd}(\mu) = \ell^{e_2}$ is equivalent to

$$N^2 f(x, y) + pf(Nz + \lambda C, Nt + \lambda D) = \ell^{e_2}. \tag{5}$$

Modulo N, the previous equation becomes

$$\lambda^2 pf(C, D) \equiv \ell^{e_2} \bmod N.$$

Since l is a quadratic non-residue modulo N, the parity of e_2 should be adjusted so that $\left(\frac{pf(C,D)}{N}\right) = \left(\frac{\ell^{e_2}}{N}\right)$. We then have $\lambda = \sqrt{\frac{\ell^{e_2}}{pf(C,D)}} \bmod N$.

Furthermore, we also have

$$f(Nz + \lambda C, Nt + \lambda D) = N^2 f(z, t) + \lambda^2 f(C, D) + N\lambda L((C, D), (z, t)),$$

where

$$L((C, D), (z, t)) = 2Cz + \mathrm{Trd}(\omega)(Dz + Ct) + 2\,\mathrm{Nrd}(\omega)Dt = \langle C + D\omega, z + t\omega\rangle.$$

Hence, Eq. (5) is equivalent to

$$\lambda pL((C,D),(z,t)) = \frac{\ell^{e_2} - \lambda^2 pf(C,D)}{N} - N(f(x,y) + pf(z,t)). \tag{6}$$

(We recall that λ is chosen so that N divides $\ell^{e_2} - \lambda^2 pf(C,D)$). Modulo N, Eq. (6) yields the linear equation

$$\lambda pL((C,D),(z,t)) = \frac{\ell^{e_2} - \lambda^2 pf(C,D)}{N} \bmod N. \tag{7}$$

This linear equation has N solutions (z,t) [42].

To find (x,y), one takes a random solution (z,t) and tries to solve the following equation, which is equivalent to Eq. (5):

$$f(x,y) = \frac{\ell^{e_2} - pf(Nz + \lambda C, Nt + \lambda D)}{N^2} =: r \tag{8}$$

Remark 7. In this step, there are two ways to proceed:

1. Take e_2 large enough so that r is always positive, and randomly take (z,t) so that r is a norm in R (as done in [42]);
2. Adjust e_2 for each value of (z,t) so that Eq. (8) has a solution. This method gives an exponential approach that is studied next.

We summarize our discussion about the KLPT algorithm in the following lemma. Note that this result is already implied in [46].

Lemma 8. *Let $\mathcal{O}_0$ be a special extremal maximal order in $\mathcal{B}_{p,\infty}$, where $p \equiv 3$ mod 4 or $p \equiv 5$ mod 8. Let I be a $\mathcal{O}_0$-left ideal. Using KLPT algorithm, we can compute an ideal of smooth norm d equivalent to I, where $d = \ell^e \approx p^{\frac{5}{2}}$.*

Proof. In Step 1, the ideal J can be found such that N is split in R. For such N, the equation $f(x,y) = N$ has a solution since $h_\Delta = 1$, where $\Delta = disc(R)$. Hence, we can take $e_1 = 0$ in Step 2 and Eq. (5) has a solution for $x_2 = y_2 = 0$. Using the strategy in [46] in Step 5, we have $e_2 \approx \frac{5}{2}\log_\ell(p)$. Thus, $e = e_2 \approx \frac{5}{2}\log_\ell(p)$, and the result follows.

Remark 9. For a general value of p, this approach work with probability $\frac{1}{h_\Delta}$.

Superpolynomial-time KLPT

We now analyze the second strategy discussed in Remark 7, with a particular focus on superpolynomial-time algorithms. Note that the ideas of the strategy we present here first appeared in [45, Section 3.4], and we give a variant of it.

Given $C, D \in \mathbb{Z}$, we look for solutions $(z,t) \in \mathbb{Z}^2$ such that Eq. (7) holds. In [46], it was shown that the solutions (z,t) for Eq. (7) can be viewed as a translated lattice as follows. We let $\Phi = p\lambda(2C + \mathsf{tr}(\omega)D), \Psi = p\lambda(\mathsf{tr}(\omega)C + 2n(\omega)D)$, and $\chi := \frac{l^{e_2} - \lambda^2 pf(C,D)}{N}$, then (z,t) satisfies

$$\Psi z + \Psi t \equiv \chi \mod N.$$

Let (z_0,t_0) denote one solution of this equation, then all solutions $(z,t) \in \mathbb{Z}^2$ are contained in the translated lattice $\mathcal{L} = (z_0,t_0)^T + \mathcal{L}_0$, where $\mathcal{L}_0 =$

$\mathbb{Z}(\Phi, -\Psi)^T + \mathbb{Z}(0, N)^T$. To reduce the output length of KLPT, we aim to reduce $pf(Nz + \lambda C, Nt + \lambda D)$. In [46], this is reduced to a closest-vector problem where the involved lattice $\mathcal{L}$ is a deformation of $\mathcal{L}_0$. For our purpose, we do not recall the concrete basis of $\mathcal{L}_0$ here, but only note that this lattice is determined by C and D, and it has volume $pN^3\sqrt{\Delta_{\mathbb{Q}(\omega)}}$. By the Gaussian heuristic, we estimate that the lattice contains a basis of size $\sqrt{p}N^{\frac{3}{2}}\Delta_{\mathbb{Q}(\omega)}^{\frac{1}{4}}$. This gives rise to the estimation that one can find (z, t) such that $pf(Nz + \lambda C, Nt + \lambda D) \approx pN^3\sqrt{\Delta_{\mathbb{Q}(\omega)}}$. Hence, $\ell^{e_2} \approx pN^3\sqrt{\Delta_{\mathbb{Q}(\omega)}} \approx p^{\frac{5}{2}}$. Below is a theorem that estimates the expected shortest vector of n independent random matrices from [4, Section 4.1].

Theorem 10. *Let $Z_1, ...Z_n$ be the length of the shortest vectors in n independent random matrices of unit volume and $Z_{\min} := \min\{Z_1, ..., Z_n\}$, then $\mathbb{E}(Z_{\min}) \leq O(\frac{1}{\sqrt{n}})$ for $n \geq 2$.*

If we can generate n pairs of C, D that gives rise to n independent random lattices, then according to Theorem 10, the expected shortest vector among these n lattices has length $\frac{\sqrt{p}N^{\frac{3}{2}}\Delta_{\mathbb{Q}(\omega)}^{\frac{1}{4}}}{\sqrt{n}}$. Therefore, $pf(Nz + \lambda C, Nt + \lambda D)$ would be $\frac{pN^3\sqrt{\Delta_{\mathbb{Q}(\omega)}}}{n}$. Let $n \approx N^{e_3}$, then $\frac{pN^3\sqrt{\Delta_{\mathbb{Q}(\omega)}}}{n} \approx pN^{3-e_3}\sqrt{\Delta_{\mathbb{Q}(\omega)}} \approx p^{\frac{5}{2}-\frac{e_3}{2}}$.

Hence, the length of the path returned using this approach reaches $e = \frac{5-e_3}{2}\log(p)$. The number n is exactly the number of solutions provided by the modular constrain Step 4 that we want to analyze.

On the modular constraint

In a general context, the modular constraint step consists of finding an element $[\mu] \in (\mathcal{O}/N\mathcal{O})^* \equiv GL_2(\mathbb{Z}/N\mathbb{Z})$ such that $(\mathcal{O}\gamma/N\mathcal{O})[\mu] = J/N\mathcal{O}$. The existence of such element is justified by the transitivity of the action of $GL_2(\mathbb{Z}/N\mathbb{Z})$ on $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$. We recall the following lemma:

Lemma 11 ([42]). *Let N be a prime and $A = M_2(\mathbb{Z}/N\mathbb{Z})$. The set of proper nontrivial left A-ideals is in bijection with the set*

$$\left\{\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) \times \{(x : y)\};\ (x : y) \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})\right\},$$

and the right action of $PGL_2((\mathbb{Z}/N\mathbb{Z})$ on left A-ideals is transitive and induced by the natural action on $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$.

We recall that the action of $PGL_2((\mathbb{Z}/N\mathbb{Z})$ on $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ is induced by the action of $GL_2(\mathbb{Z}/N\mathbb{Z})$ which has kernel $(\mathbb{Z}/N\mathbb{Z})^*$. Using an explicit isomorphism between $\mathcal{O}/N\mathcal{O}$ and $M_2(\mathbb{Z}/N\mathbb{Z})$ we have an action of $(\mathcal{O}/N\mathcal{O})^*$ on the left $\mathcal{O}/N\mathcal{O}$-ideals. In the context of the KLPT algorithm, this action is restricted to the action of $Rj/N\mathcal{O}$. That is why Step 4 just consists to find a pair (C, D). Hence, the number n is upper bounded by the number of $[\mu]$. The number of such $[\mu]$ is exactly $\#Stab([x : y])$ (where $Stab([x : y])$ denotes the stabilizer of $[x : y]$) for some $[x : y] \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$, since the action is transitive. Furthermore, we have $\#Stab([x : y]) = \frac{\#PLG_2(\mathbb{Z}/N\mathbb{Z})}{\#\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})} = N(N + 1)$. Hence, we have $n \approx N^2$. We summarize the discussion into the following theorem.

Theorem 12. *Let I be a left $\mathcal{O}$-ideal for an extremal order $\mathcal{O}$. Then applying the KLPT algorithm to I one could find an equivalent left $\mathcal{O}$-ideal J such that $n(J)$ is an ℓ-power and is of length $\frac{5-e}{2}\log p$ in time $\tilde{O}(n)$ where n is any positive integer less than p and e is a rational number such that $(\sqrt{p})^e \approx n$, for $p \equiv 3$ mod 4 or $p \equiv 5$ mod 8.*

Proof. We set $n(J) = \ell^{e_1+e_2}$ where e_1 and e_2 are given respectively by Step 2 and Step 5. Following the arguments in the proof of Lemma 8, we have $e_1 = 0$. Let e be such that $N^e \approx (\sqrt{p})^e$ is the number of solutions we generate in the modular constrain step, then based on the discussions above, we have that $e_2 \approx \frac{5-e}{2}\log_\ell(p)$. This approach then has complexity in $\tilde{O}(\sqrt{p}^e)$. The number of solutions that can be generated in the modular constrain step is bounded above by $N^2 \approx p$.

The shortest path returned by this approach has length $\frac{3}{2}\log p$ which takes time $\tilde{O}(p)$. Note that in both our variants p is a slightly smaller than $2^{2\lambda}$. The cost of this attack to generate a path of length $\frac{3}{2}\log p$ is thus far greater than the security parameter. On the other hand, if we choose the runtime to be $\sqrt{p} \approx 2^\lambda$, then the output path length from this approach is $2\log p$.

4.2 KLPT algorithm for non-extremal order

Let E and E_1 be two supersingular elliptic curve defined over $\mathbb{F}_{p^2}$, of known endomorphism rings $\mathcal{O}$ and $\mathcal{O}_1$. Let I be a connecting ideal of $\mathcal{O}$ and $\mathcal{O}_1$. Let $\mathcal{O}_0$ be a special extremal order, and $I_0 = I(\mathcal{O}_0, \mathcal{O})$. The problem is to find an $\mathcal{O}$-left ideal of smooth norm equivalent to I.

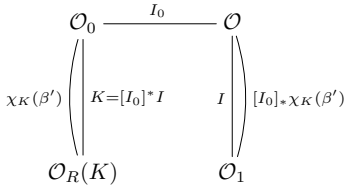
Approach from [42] The idea in [42] is as follows:

1. Compute $I_1 = I_0 \frac{\bar{\gamma_1}}{\mathrm{Nrd}(I_0)}$ where $\mathrm{Nrd}(\gamma_1) = n_1 \mathrm{Nrd}(I_0)$;
2. Compute $I_2 = I_0 I \frac{\bar{\gamma_2}}{\mathrm{Nrd}(I_0 I)}$ where $\mathrm{Nrd}(\gamma_2) = n_2 \mathrm{Nrd}(I_0 I)$;
3. Return $I \frac{\bar{\gamma}}{\mathrm{Nrd}(I)}$, where $\gamma = \bar{\gamma_1}\gamma_2$.

With this approach, the length of the shortest path is greater than $4\log(p)$.

The SQISign approach The idea in SQISign [25] is to transfer the problem in the special case using pullback and push forward through I_0

.



Where $\chi_K(\beta') = K\frac{\bar{\beta'}}{\mathrm{Nrd}(K)}$. To obtain this, one must have $\beta' \in K \cap \mathfrak{D}$, where $\mathfrak{D} = \mathcal{O}_0 \cap \mathcal{O} = \mathbb{Z} + I_0$ [25, Corollary 1]. For $n = \ell^e$, the algorithm can be described as follows: We suppose that $\mathrm{Nrd}(I_0) = N_0$ is prime inert in R such that ℓ is a quadratic non residue modulo N_0.

1. Compute $K = [I_0]^* I$;
2. Compute an ideal L of prime norm N equivalent to K, such that ℓ is a quadratic non-residue modulo N. Let δ such that $L = \chi_K(\delta)$;
3. Find an element $\gamma \in \mathcal{O}$ of norm $N\ell^{e_1}$ for some $e_1 \in \mathbb{N}$;
4. Find an element $\alpha \in \mathcal{O}$ such that $L = \mathcal{O}\alpha + N\mathcal{O}$;
5. Compute $\mu_0 = (C_0 + \omega D_0)j \in Rj$ such that $\gamma\mu_0 \equiv \alpha \bmod N\mathcal{O}$;
6. Compute $\mu_1 = (C_1 + \omega D_1)j \in Rj$ such that $\gamma\mu_0\delta \in \mathcal{O} \cap \mathcal{O}_0$;
7. Compute $C = CRT_{N_0,N}(C_0, C_1)$ and $D = CRT_{N_0,N}(D_0, D_1)$ and let $\mu' = (C + \omega D)j$
8. Compute $\lambda \in \mathbb{Z}/NN_0\mathbb{Z}^*$ and $\mu_1' \in \mathcal{O}_0$ such that $\mu = \lambda\mu' + NN_0\mu_1'$ has norm l^{e_2}, for some $e_2 \in \mathbb{N}$.
9. Return $\chi_L(\beta)$, where $\beta = \gamma\mu$.

The main difference between this algorithm and the algorithm from [42] described in Section 4.1 is Step 8. Here the approximation is done modulo NN_0 and then the computation of λ becomes more delicate than what we have in Step 5, Section 4.1. In the present context, the approximation equation is Eq. (9), which corresponds to Eq. (5), replacing N by NN_0.

$$N^2N_0^2 f(x, y) + pf(NN_0z + \lambda C, NN_0t + \lambda D) = \ell^{e_2}. \tag{9}$$

Modulo NN_0, this equation becomes

$$\lambda^2 pf(C, D) \equiv \ell^{e_2} \bmod NN_0.$$

For this equation to have a solution, we need the following equality:

$$\left(\frac{pf(C,D)}{N}\right) = \left(\frac{\ell^{e_2}}{N}\right) \text{ and } \left(\frac{pf(C,D)}{N_0}\right) = \left(\frac{\ell^{e_2}}{N_0}\right).$$

Since ℓ is a quadratic non residue modulo N and N_0, we always have $\left(\frac{\ell^{e_2}}{N}\right) = \left(\frac{\ell^{e_2}}{N_0}\right)$. Hence, we need

$$\left(\frac{pf(C,D)}{N}\right) = \left(\frac{pf(C,D)}{N_0}\right). \tag{10}$$

This last equality has a probability $\frac{3}{4}$ to fail, for given γ from Step 3 and δ from Step 2 [25]. To minimize this failure probability, the authors of [25] take e_1 large enough so that there are many possibilities for γ (we recall that γ is computed by solving Eq. (4)). The advantage of this method is that it only modifies the parameters (C, D), and N remains fixed. Since we need e_1 to be as small as possible and Eq. (4) has a solution for $e_1 = 0$ when N is split in R, we would like to take $e_1 = 0$. We summarize the result in the following lemma.

Lemma 13. *Let $\mathcal{O}$ and $\mathcal{O}_1$ be two non extremal maximal orders in $\mathcal{B}_{p,\infty}$ where $p \equiv 3 \bmod 4$ or $p \equiv 5 \bmod 8$. Given a connecting ideal I of $\mathcal{O}$ and $\mathcal{O}_1$, there is a probabilistic polynomial time algorithm which find an equivalent ideal of norm ℓ^e, for some small prime ℓ and $e \approx 4\log(p)$.*

Proof. Following the idea in Lemma 8, we can obtain $e_1 = 0$ in step 3 in which case Equation 4 is solved by setting $x_1 = x_2 = 0$. Eq. (4) become $f(x_1, x_2) = N$, which has at most 4 solutions leading to different values of $[C : D] \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$.

Hence, the success probability is $1 - \left(\frac{3}{4}\right)^4 \approx 68.4\%$. In the failure case we can either go back to Step 2 and compute an other L, or compute an other I_0. In Step 8, we can use the strategy of [46] to obtain $e_2 \approx 4 \log_l p$ and the result follows.

Remark 14. The exponential approach of Section 4.1 can be applied here. Using similar analysis, we see that the output length is $(4-e)\log p$ in time $\tilde{O}(n)$ where n is any positive integer less than p and e is a rational number such that $(\sqrt{p})^e \approx n$, for $p \equiv 3 \bmod 4$ or $p \equiv 5 \bmod 8$. And in this case, if we bound the runtime by $\sqrt{p}$, then the shortest path returned is of length $3 \log p$.

4.3 Parameters secure against KLPT-based attacks

Combining the analysis presented so far, we obtain the following limitations for an attacker of complexity 2^λ. Since $O(p) = O(2^\epsilon)$ and $\lambda < \epsilon \leq 2\lambda$, we use $O(\sqrt{p})$ as an upper bound for the runtime of exponential KLPT, and we summarize the output length here.

Takeaway 1 *Consider an isogeny $\phi : E_0 \to E_1$ of degree d. Given the endomorphism rings of E_0 and E_1, KLPT-based methods cannot recover ϕ in time $\tilde{O}(\sqrt{p}) < \tilde{O}(2^\lambda)$ if:*

1. *E_0 is a special curve, $p \in \{3, 5, 7\} \bmod 8$, and $\log d < 2 \log p$;*
2. *E_0 is a special curve, $p \notin \{3, 5, 7\} \bmod 8$, and $\log d < \frac{5}{2} \log p$;*
3. *E_0 is not a special curve, $p \in \{3, 5, 7\} \bmod 8$, and $\log d < 3 \log p$;*
4. *E_0 is not a special curve, $p \notin \{3, 5, 7\} \bmod 8$, and $\log d < \frac{7}{2} \log p$.*

Given these results, we obtain that the two protocols proposed in Section 3 are secure against KLPT-based attacks. In both instances, E_0 is chosen to not be a special curve, hence the limits 3 and 4 apply. In the first variant, from Takeaway 2, the isogeny ϕ has degree $d \approx 2^\lambda p^2$ and ψ has degree $\approx p$, **Variant 1** is secure according to the summary above. Similarly, **Variant 2** relies on isogenies of degree $\approx p$, and thus KLPT-based attacks do not apply. In both instantiations, the signatures rely on the stronger relation, and thus the attack that recovers the composition $\hat{\psi} \circ \phi' \circ \psi'$ cannot be used.

5 Analysis of other attacks

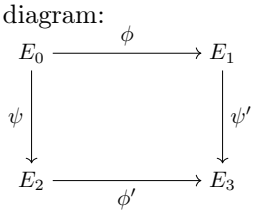
5.1 Attacks based on the SIDH attacks

The SIDH attacks [15, 44, 49] recover an isogeny $\phi : E_0 \to E_1$ of degree d given:
- The curves E_0 and E_1;
- The degree d;
- The image of a torsion basis of smooth order n with $n \geq \sqrt{d}$.

However, it is possible to brute-force part of an unknown isogeny (which is always cheaper than brute-forcing torsion point information), thus we need $d \geq 2^\lambda \sqrt{\ell}$ to avoid the attacks.

Binary challenges. The proofs of isogeny knowledge with binary challenges are potentially vulnerable to the SIDH attacks.

Consider the following diagram:



When the proof has binary challenges, the isogenies ψ and ψ' are revealed together. If the prover is honest, we have

$$\ker \psi' = \phi(\ker \psi),$$

which allows an attacker to recover the image of the subgroup $\ker \psi$ under the secret isogeny ϕ. After three such challenges, the attacker has recovered enough information to apply the SIDH attacks. In fact, as shown in [9, 34] this allows the attacker to recover the image of a torsion basis on E_0 under ϕ, up to the same scalar. The square of this scalar can be computed through Weil pairing. If the degrees of ψ and ψ' are prime powers, as in SIDH, there are only two possible square roots. It is easy to apply the SIDH attacks each time $\deg \phi < (\deg \psi)^2$, assuming the degree of ψ is not much smaller than that of ϕ, and recover ϕ. In practice, it is enough to have $2^\lambda (\deg \psi)^2 \leq \deg \phi$, so that one needs to first guess an isogeny of degree at least 2^λ before being able to apply the SIDH attacks.

Takeaway 2 *Binary challenges require* $2^\lambda (\deg \psi)^2 \leq \deg \phi$.

Remark 15. An alternative idea could be to use commitment isogenies ψ and ψ' with non-rational torsion as the torsion point images are defined over large extensions fields and thus the SIDH attacks do not apply directly. However, in our case we know endomorphism rings and can go on a different route. As described in [19], one has that $(\mathrm{End}(E)/N\mathrm{End}(E))^*$ acts on the set of degree N isogenies. In general without any extra information this action is hard to compute when only the codomain of the isogeny is known. In our case however, this action is exactly provided by the parallel isogenies. Thus one can compute the stabilizer of this action as in [19] using a polynomial-time quantum algorithm which essentially reveals the connecting ideal corresponding to the secret isogeny. Since the secret isogeny here is smooth, one can recover the isogeny itself step by step. Note that just knowing the codomain of the parallel isogeny would not always have been enough (as it does not determine the action precisely as one might have several degree N isogenies between two supersingular elliptic curves). However, knowing the second vertical isogeny already is enough information to evaluate the group action (assuming that the torsion is large enough to ensure unicity).

5.2 Attacks on the zero-knowledge property

In this section, we explore the zero-knowledge property of the underlying sigma protocol for the binary challenge variant as described in Section 3.

We set ourselves in the setting of **Variant 1**, from Section 3.1, since the others variants use ternary challenges and are provably (honest-verifier) zero-knowledge. The question we explore is whether we can address the zero-knowledge issue that arises in Variant 1 in the context where we only use the identification protocol for the purpose of turning it into a signature scheme.

This turns out to be a key observation: we turn the Sigma protocol into a signature scheme via the Fiat-Shamir transform [31], and a natural question that arises is whether we can allow a relaxation of the zero-knowledge property of the underlying Sigma protocol whilst still retaining the security of the Fiat-Shamir transform. In other words, what are the minimal assumptions for the security of the Fiat-Shamir transform and can we achieve them? In [1], they introduce a new notion of security for sigma-protocols, namely *security against impersonation under passive attacks*. They show that this is a minimal assumption for the Fiat-Shamir transform to be secure. We define this notion formally below:

Definition 16 ([1]). *We say that a sigma protocol is secure against impersonation under passive attacks if for any polynomial time adversary $\mathcal{A}$ the advantage $Adv^{\mathsf{Impersonate}}(\mathcal{A})$ of $\mathcal{A}$ in the* Impersonate *game is negligible, where*

$$\mathrm{Adv}^{\mathsf{Impersonate}}(\mathcal{A}) = \Pr[\mathsf{Impersonate}(\mathcal{A}) \to 1] = negl(\lambda)$$

The Impersonate *game is described below.*

$\underline{\mathsf{Impersonate}(\mathcal{A})}$
1: $\mathsf{Setup}(1^\lambda) \to \mathsf{pp}$
2: $\mathsf{KeyGen}(\mathsf{pp}) \to (\mathsf{sk}, \mathsf{pk})$
3: $\mathcal{A}^{\mathcal{OTG}}(\mathsf{pk}) \to \mathsf{com}, \mathrm{st}$
4: $\mathsf{ch} \xleftarrow{\$} \mathcal{C}$
5: $\mathcal{A}(\mathrm{st}, \mathsf{ch}) \to \mathsf{resp}$
6: **return** $\mathcal{V}(\mathsf{pk}, \mathsf{com}, \mathsf{ch}, \mathsf{resp})$

$\underline{\mathcal{OTG}}$
1: $R_p \xleftarrow{\$} \mathcal{R}$ (generate randomness)
2: $\mathsf{com} \leftarrow \mathcal{P}(\mathsf{sk}; R_p)$
3: $\mathsf{ch} \xleftarrow{\$} \mathcal{C}$
4: $\mathsf{resp} \leftarrow \mathcal{P}(\mathsf{sk}, \mathsf{com}, \mathsf{ch}; R_p)$
5: **return** $(\mathsf{com}, \mathsf{ch}, \mathsf{resp})$

Theorem 17 ([1], Theorem 3.3). *Let Π_Σ be a non-trivial sigma-protocol, and $\mathcal{DS}_\Sigma$ be the associated digital signature scheme obtained via the Fiat-Shamir transform, then $\mathcal{DS}_\Sigma$ is secure against existential forgery under chosen-message attacks if and only if Π_Σ is secure against impersonation under passive attacks.*

Remark 18. Note that non-triviality here requires the challenge space to be super-polynomial. Otherwise, a trivial winning strategy would be to replay a transcript obtained from the oracle and then one gets a probably $1/|\mathcal{C}|$ of winning. So if the size of the challenge space is polynomial, we have a winning strategy with probability that is not negligible.

We claim that this relaxed security notion is achieved by the parallel repetition of the binary challenge version under some conditions, and we hence get a secure signature scheme by applying the Fiat-Shamir transform. Let us formulate this more formally.

Problem 19. Consider two supersingular elliptic curves E_0, E_1 and an isogeny $\phi : E_0 \to E_1$ of degree $D = \ell_1^{e_1}$ in $\mathcal{R}_{\mathsf{strg}}$ such that $\#E_0(\mathbb{F}_{p^2}) = (\ell_1 \ell_2^{e_2} f)^2$ as defined in **Variant 1** . Given access to an oracle that outputs either :

- two isogenies $E_0 \to E_2$, $E_1 \to E_3$ and the images of the torsion basis on the codomain curves;
- an isogeny $E_2 \to E_3$ of degree D;

then the adversary must recover the secret isogeny ϕ.

Theorem 20. *Under the hardness of Problem 19, the λ parallel repetition of the sigma protocol is secure against impersonation under passive attacks.*

Proof. Problem 19 is the translation of the impersonate game to our setting.

This problem has already been discussed in the previous subsections. Notably if we ensure that the takeaways from Sections 4 and 5.1 are respected then we can reasonably assume its hardness.

> **Takeaway 3** *Under reasonable assumptions, a digital signature derived from a proof of isogeny knowledge with binary challenges via the Fiat-Shamir transform is secure.*

6 Concrete instantiations and parameters size

In this section, we analyze the size of the signatures derived from the sigma protocols described in Section 3.1 using the Fiat-Shamir transform [31]. We rely on a hash function $\mathcal{H} : \{0,1\}^* \to \{0,1\}^{2\lambda}$, where λ is the security parameter.

Variant 1. We first fix $\ell_1 = 2, \ell_2 = 3$ for efficiency reasons. Then, we choose the value e_2 such that isogenies of degree 3^{e_2} are hard to recover via meet-in-the-middle or van Oorschot-Wiener attacks [51] (e.g., we have $e_2 = 137$ for $\lambda = 128$). The exponent e_1 is chosen such that the isogenies of degree 2^{e_2} are hard to recover, even when their action on the 3^{e_2} torsion is known, i.e. $e_1 = \lambda + \lceil 2e_2 \log 3 \rceil$. We define the prime p to be of the form $p = 2 \cdot 3^{e_2} f - 1$, where f is a small cofactor. The public parameters of the signature are then $pp = (p, e_1, e_2, E_0, T_0, P_0, Q_0)$, where E_0 is a random supersingular elliptic curve defined over $\mathbb{F}_{p^2}$. The point $T_0 \in E_0$ is an auxiliary point of order 2, used in the CGL hash function computations [18], and and $\{P_0, Q_0\}$ is a basis of $E_0[3^{e_2}]$.

By the definition of p, any point of order 2^{e_1} is defined over a large extension of $\mathbb{F}_{p^2}$. We then represent the secret isogeny $\phi : E_0 \to E_1$ (of degree 2^{e_1}) by a sequence of 2-isogenies. To do that, we represent it as a seed $s \in \{0,1\}^{e_1}$ that has to be hashed using CGL hash function [18], with the first step chosen between the 2-torsion points that are not T_0. The secret key can then be represented by $e_1 \approx \lambda + 2 \log p \approx 5\lambda$ bits. The public key is (E_1, P_1, Q_1) where $P_1 = \phi(P_0)$ and $Q_1 = \phi(Q_0)$. This requires $6 \log p \approx 12\lambda$ bits.

In this variant, the soundness error is $\frac{1}{2}$: this means the signature needs to repeat the sigma protocol $k = \lambda$ times to obtain a negligible soundness error.

Since we are in the binary case, the response to both challenges includes all the committed values; thus, we rely on hashed commitments only for compression, but we do not require any hiding property. Using some of the compression techniques from [40], the size of the response for the horizontal challenge is $3\log p + 2\lambda$, while the vertical challenge is $\log p$. Repeating λ times and including the hashed commitment sizes of $2 \times 2\lambda$, we obtain an asymptotic size of $\lambda(5\lambda + 2\log p) \approx 9\lambda^2$ bits. Note that this is asymptotic and based on the assumption that $e_3 \approx 2\lambda/\log 3$, but we can choose smaller parameters based on the cost of the van Oorschoot-Wiener attack, as done in SIDH. For $\lambda = 128$, this results in a 218-bit prime and a signature of about 17 kB, which may be reduced even further by relying on seed trees [40].

Variant 2. The second variant relies on ternary challenges, and thus torsion images under the secret isogeny is not revealed. The public key hence consists of a single curve, which then requires $2\log p$ bits.

In this variant, we need to rely on a computationally binding and statistically hiding commitment scheme C: we construct one from a hash function $\mathcal{H} : \{0,1\}^* \to \{0,1\}^{2\lambda}$ by defining $\mathsf{C}(m) = \mathcal{H}(m|r)$, for some random string r of λ bits. For each execution of the sigma protocol, we need 6λ bits to represent the three commitments (following the commitment algorithm in [22, Figure 3]), $\lambda + \log p$ for the responses to the vertical isogeny challenges, and $\lambda + 3\log p$ for the response to the horizontal isogeny challenge. The soundness error of the underlying sigma protocol is $\frac{2}{3}$, which means the signature needs to repeat the sigma protocol $k = \lceil -\lambda/\log 2/3 \rceil$ times to obtain a negligible soundness error. This results in an average signature of asymptotic size $\frac{31}{3}\lambda\lceil -\lambda/\log 2/3 \rceil$ bits.

7 Conclusion

In this paper, we explore the feasibility of SIDH-based signatures when the endomorphism ring of all curves are public. We identify two variants of the construction that are secure in this setting, where the difference resides in the use of binary or ternary challenges and give concrete parameters. We provide a thorough security analysis of our proposals notably in terms of attacks based on KLPT, with both a polynomial and superpolynomial adversary, attacks derived from the recent SIDH-attacks and analyze the zero-knowledge property of the binary challenge variant. Note that the results we derive from the KLPT attacks could be affected by improvements on the output size of KLPT but this would only require to adjust the parameters to retain the security.

Acknowledgements. The first author has been supported in part by EPSRC via grant EP/R012288/1, under the RISE (http://www.ukrise.org) programme. Péter Kutas is supported by the Hungarian Ministry of Innovation and Technology NRDI Office within the framework of the Quantum Information National Laboratory Program, the János Bolyai Research Scholarship of the Hungarian

Academy of Sciences and by the UNKP-23-5 New National Excellence Program. Mingjie Chen and Péter Kutas are partly supported by EPSRC through grant number EP/V011324/1.

References

1. Abdalla, M., An, J.H., Bellare, M., Namprempre, C.: From identification to signatures via the Fiat-Shamir transform: Minimizing assumptions for security and forward-security. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 418–433. Springer, Heidelberg (Apr / May 2002). https://doi.org/10.1007/3-540-46035-7_28
2. Adj, G., Cervantes-Vázquez, D., Chi-Domínguez, J.J., Menezes, A., Rodríguez-Henríquez, F.: On the cost of computing isogenies between supersingular elliptic curves. In: Cid, C., Jacobson Jr:, M.J. (eds.) SAC 2018. LNCS, vol. 11349, pp. 322–343. Springer, Heidelberg (Aug 2019). https://doi.org/10.1007/978-3-030-10970-7_15
3. Alamati, N., De Feo, L., Montgomery, H., Patranabis, S.: Cryptographic group actions and applications. In: Moriai, S., Wang, H. (eds.) ASIACRYPT 2020, Part II. LNCS, vol. 12492, pp. 411–439. Springer, Heidelberg (Dec 2020). https://doi.org/10.1007/978-3-030-64834-3_14
4. Aono, Y., Espitau, T., Nguyen, P.Q.: Random lattices: Theory and practice. Preprint. https://espitau.github.io/bin/random_lattice.pdf
5. Badrinarayanan, S., Masny, D., Mukherjee, P., Patranabis, S., Raghuraman, S., Sarkar, P.: Round-optimal oblivious transfer and MPC from computational CSIDH. In: Boldyreva, A., Kolesnikov, V. (eds.) PKC 2023, Part I. LNCS, vol. 13940, pp. 376–405. Springer, Heidelberg (May 2023). https://doi.org/10.1007/978-3-031-31368-4_14
6. Basso, A.: A post-quantum round-optimal oblivious PRF from isogenies. Cryptology ePrint Archive, Report 2023/225 (2023), https://eprint.iacr.org/2023/225
7. 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.) EUROCRYPT 2023, Part II. LNCS, vol. 14005, pp. 405–437. Springer, Heidelberg (Apr 2023). https://doi.org/10.1007/978-3-031-30617-4_14
8. Basso, A., Fouotsa, T.B.: New sidh countermeasures for a more efficient key exchange. Cryptology ePrint Archive, Paper 2023/791 (2023), https://eprint.iacr.org/2023/791, https://eprint.iacr.org/2023/791
9. Basso, A., Kutas, P., Merz, S.P., Petit, C., Sanso, A.: Cryptanalysis of an oblivious PRF from supersingular isogenies. In: Tibouchi, M., Wang, H. (eds.) ASIACRYPT 2021, Part I. LNCS, vol. 13090, pp. 160–184. Springer, Heidelberg (Dec 2021). https://doi.org/10.1007/978-3-030-92062-3_6
10. Basso, A., Maino, L., Pope, G.: Festa: Fast encryption from supersingular torsion attacks. Cryptology ePrint Archive, Paper 2023/660 (2023), https://eprint.iacr.org/2023/660, https://eprint.iacr.org/2023/660
11. 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)
12. Beullens, W., De Feo, L., Galbraith, S.D., Petit, C.: Proving knowledge of isogenies: a survey. Designs, Codes and Cryptography (Jun 2023). https://doi.org/10.1007/s10623-023-01243-3, https://doi.org/10.1007/s10623-023-01243-3

13. Beullens, W., Kleinjung, T., Vercauteren, F.: CSI-FiSh: Efficient isogeny based signatures through class group computations. In: Galbraith, S.D., Moriai, S. (eds.) ASIACRYPT 2019, Part I. LNCS, vol. 11921, pp. 227–247. Springer, Heidelberg (Dec 2019). https://doi.org/10.1007/978-3-030-34578-5_9
14. Boneh, D., Kogan, D., Woo, K.: Oblivious pseudorandom functions from isogenies. In: Moriai, S., Wang, H. (eds.) ASIACRYPT 2020, Part II. LNCS, vol. 12492, pp. 520–550. Springer, Heidelberg (Dec 2020). https://doi.org/10.1007/978-3-030-64834-3_18
15. Castryck, W., Decru, T.: An efficient key recovery attack on SIDH. In: Hazay, C., Stam, M. (eds.) EUROCRYPT 2023, Part V. LNCS, vol. 14008, pp. 423–447. Springer, Heidelberg (Apr 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.) ASIACRYPT 2018, Part III. LNCS, vol. 11274, pp. 395–427. Springer, Heidelberg (Dec 2018). https://doi.org/10.1007/978-3-030-03332-3_15
17. Castryck, W., Panny, L., Vercauteren, F.: Rational isogenies from irrational endomorphisms. In: Canteaut, A., Ishai, Y. (eds.) EUROCRYPT 2020, Part II. LNCS, vol. 12106, pp. 523–548. Springer, Heidelberg (May 2020). https://doi.org/10.1007/978-3-030-45724-2_18
18. Charles, D.X., Lauter, K.E., Goren, E.Z.: Cryptographic hash functions from expander graphs. Journal of Cryptology **22**(1), 93–113 (Jan 2009). https://doi.org/10.1007/s00145-007-9002-x
19. Chen, M., Imran, M., Ivanyos, G., Kutas, P., Leroux, A., Petit, C.: Hidden stabilizers, the isogeny to endomorphism ring problem and the cryptanalysis of psidh. Cryptology ePrint Archive (2023)
20. Dartois, P., Leroux, A., Robert, D., Wesolowski, B.: SQISignHD: New Dimensions in Cryptography. Cryptology ePrint Archive, Paper 2023/436 (2023), https://eprint.iacr.org/2023/436, https://eprint.iacr.org/2023/436
21. De Feo, L., Delpech de Saint Guilhem, C., Fouotsa, T.B., Kutas, P., Leroux, A., Petit, C., Silva, J., Wesolowski, B.: Séta: Supersingular encryption from torsion attacks. In: Tibouchi, M., Wang, H. (eds.) ASIACRYPT 2021, Part IV. LNCS, vol. 13093, pp. 249–278. Springer, Heidelberg (Dec 2021). https://doi.org/10.1007/978-3-030-92068-5_9
22. De Feo, L., Dobson, S., Galbraith, S.D., Zobernig, L.: SIDH proof of knowledge. In: Agrawal, S., Lin, D. (eds.) ASIACRYPT 2022, Part II. LNCS, vol. 13792, pp. 310–339. Springer, Heidelberg (Dec 2022). https://doi.org/10.1007/978-3-031-22966-4_11
23. De Feo, L., Fouotsa, T.B., Kutas, P., Leroux, A., Merz, S.P., Panny, L., Wesolowski, B.: SCALLOP: Scaling the CSI-FiSh. In: Boldyreva, A., Kolesnikov, V. (eds.) PKC 2023, Part I. LNCS, vol. 13940, pp. 345–375. Springer, Heidelberg (May 2023). https://doi.org/10.1007/978-3-031-31368-4_13
24. De Feo, L., Galbraith, S.D.: SeaSign: Compact isogeny signatures from class group actions. In: Ishai, Y., Rijmen, V. (eds.) EUROCRYPT 2019, Part III. LNCS, vol. 11478, pp. 759–789. Springer, Heidelberg (May 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.) ASIACRYPT 2020, Part I. LNCS, vol. 12491, pp. 64–93. Springer, Heidelberg (Dec 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.) EUROCRYPT 2023, Part V. LNCS, vol. 14008, pp. 659–690. Springer, Heidelberg (Apr 2023). https://doi.org/10.1007/978-3-031-30589-4_23
27. De Feo, L., Masson, S., Petit, C., Sanso, A.: Verifiable delay functions from supersingular isogenies and pairings. In: Galbraith, S.D., Moriai, S. (eds.) ASIACRYPT 2019, Part I. LNCS, vol. 11921, pp. 248–277. Springer, Heidelberg (Dec 2019). https://doi.org/10.1007/978-3-030-34578-5_10
28. Eisenträger, K., Hallgren, S., Lauter, K.E., Morrison, T., Petit, C.: Supersingular isogeny graphs and endomorphism rings: Reductions and solutions. In: Nielsen, J.B., Rijmen, V. (eds.) EUROCRYPT 2018, Part III. LNCS, vol. 10822, pp. 329–368. Springer, Heidelberg (Apr / May 2018). https://doi.org/10.1007/978-3-319-78372-7_11
29. Eisenträger, K., Hallgren, S., Leonardi, C., Morrison, T., Park, J.: Computing endomorphism rings of supersingular elliptic curves and connections to path-finding in isogeny graphs. Open Book Series **4**(1), 215–232 (2020)
30. Feo, L.D., Jao, D., Plût, J.: Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. Journal of Mathematical Cryptology **8**(3), 209–247 (2014). https://doi.org/doi:10.1515/jmc-2012-0015, https://doi.org/10.1515/jmc-2012-0015
31. Fiat, A., Shamir, A.: How to prove yourself: Practical solutions to identification and signature problems. In: Odlyzko, A.M. (ed.) CRYPTO'86. LNCS, vol. 263, pp. 186–194. Springer, Heidelberg (Aug 1987). https://doi.org/10.1007/3-540-47721-7_12
32. Fouotsa, T.B., Kutas, P., Merz, S.P., Ti, Y.B.: On the isogeny problem with torsion point information. In: Hanaoka, G., Shikata, J., Watanabe, Y. (eds.) PKC 2022, Part I. LNCS, vol. 13177, pp. 142–161. Springer, Heidelberg (Mar 2022). https://doi.org/10.1007/978-3-030-97121-2_6
33. Fouotsa, T.B., Moriya, T., Petit, C.: M-SIDH and MD-SIDH: Countering SIDH attacks by masking information. In: Hazay, C., Stam, M. (eds.) EUROCRYPT 2023, Part V. LNCS, vol. 14008, pp. 282–309. Springer, Heidelberg (Apr 2023). https://doi.org/10.1007/978-3-031-30589-4_10
34. Fouotsa, T.B., Petit, C.: A new adaptive attack on SIDH. In: Galbraith, S.D. (ed.) CT-RSA 2022. LNCS, vol. 13161, pp. 322–344. Springer, Heidelberg (Mar 2022). https://doi.org/10.1007/978-3-030-95312-6_14
35. Fuselier, J., Iezzi, A., Kozek, M., Morrison, T., Namoijam, C.: Computing supersingular endomorphism rings using inseparable endomorphisms. arXiv preprint arXiv:2306.03051 (2023)
36. Galbraith, S.D., Petit, C., Shani, B., Ti, Y.B.: On the security of supersingular isogeny cryptosystems. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016, Part I. LNCS, vol. 10031, pp. 63–91. Springer, Heidelberg (Dec 2016). https://doi.org/10.1007/978-3-662-53887-6_3
37. Galbraith, S.D., Petit, C., Silva, J.: Identification protocols and signature schemes based on supersingular isogeny problems. In: Takagi, T., Peyrin, T. (eds.) ASIACRYPT 2017, Part I. LNCS, vol. 10624, pp. 3–33. Springer, Heidelberg (Dec 2017). https://doi.org/10.1007/978-3-319-70694-8_1
38. Galbraith, S.D., Petit, C., Silva, J.: Identification protocols and signature schemes based on supersingular isogeny problems. Journal of Cryptology **33**(1), 130–175 (Jan 2020). https://doi.org/10.1007/s00145-019-09316-0
39. Ghantous, W., Katsumata, S., Pintore, F., Veroni, M.: Collisions in supersingular isogeny graphs and the sidh-based identification protocol. Cryptology ePrint Archive,

Paper 2021/1051 (2021), https://eprint.iacr.org/2021/1051, https://eprint.iacr.org/2021/1051
40. Ghantous, W., Pintore, F., Veroni, M.: Efficiency of sidh-based signatures (yes, sidh). Cryptology ePrint Archive, Paper 2023/433 (2023), https://eprint.iacr.org/2023/433, https://eprint.iacr.org/2023/433
41. Jao, D., De Feo, L.: Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In: Yang, B.Y. (ed.) Post-Quantum Cryptography - 4th International Workshop, PQCrypto 2011. pp. 19–34. Springer, Heidelberg (Nov / Dec 2011). https://doi.org/10.1007/978-3-642-25405-5_2
42. 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)
43. Lai, Y.F., Galbraith, S.D., Delpech de Saint Guilhem, C.: Compact, efficient and UC-secure isogeny-based oblivious transfer. In: Canteaut, A., Standaert, F.X. (eds.) EUROCRYPT 2021, Part I. LNCS, vol. 12696, pp. 213–241. Springer, Heidelberg (Oct 2021). https://doi.org/10.1007/978-3-030-77870-5_8
44. Maino, L., Martindale, C., Panny, L., Pope, G., Wesolowski, B.: A direct key recovery attack on SIDH. In: Hazay, C., Stam, M. (eds.) EUROCRYPT 2023, Part V. LNCS, vol. 14008, pp. 448–471. Springer, Heidelberg (Apr 2023). https://doi.org/10.1007/978-3-031-30589-4_16
45. Merz, S.P.: A Curved Path to Post-Quantum: Cryptanalysis and Design of Isogeny-based Cryptography. Ph.D. thesis, Royal Holloway, University of London (2023)
46. Petit, C., Smith, S.: An improvement to the quaternion analogue of the ‘-isogeny problem (2018), file:///C:/Users/HP/Downloads/08-50_3.pdf, file:///C:/Users/HP/Downloads/08-50_3.pdf
47. Petit, C.: Faster algorithms for isogeny problems using torsion point images. In: Takagi, T., Peyrin, T. (eds.) ASIACRYPT 2017, Part II. LNCS, vol. 10625, pp. 330–353. Springer, Heidelberg (Dec 2017). https://doi.org/10.1007/978-3-319-70697-9_12
48. de Quehen, V., Kutas, P., Leonardi, C., Martindale, C., Panny, L., Petit, C., Stange, K.E.: Improved torsion-point attacks on SIDH variants. In: Malkin, T., Peikert, C. (eds.) CRYPTO 2021, Part III. LNCS, vol. 12827, pp. 432–470. Springer, Heidelberg, Virtual Event (Aug 2021). https://doi.org/10.1007/978-3-030-84252-9_15
49. Robert, D.: Breaking SIDH in polynomial time. In: Hazay, C., Stam, M. (eds.) EUROCRYPT 2023, Part V. LNCS, vol. 14008, pp. 472–503. Springer, Heidelberg (Apr 2023). https://doi.org/10.1007/978-3-031-30589-4_17
50. Sterner, B.: Commitment schemes from supersingular elliptic curve isogeny graphs. Mathematical Cryptology **1**(2), 40–51 (Mar 2022), https://journals.flvc.org/mathcryptology/article/view/130656
51. van Oorschot, P.C., Wiener, M.J.: Parallel collision search with cryptanalytic applications. Journal of Cryptology **12**(1), 1–28 (Jan 1999). https://doi.org/10.1007/PL00003816
52. Vélu, J.: Isogénies entre courbes elliptiques. Comptes-Rendus de l’Académie des Sciences **273**, 238–241 (1971)
53. Voight, J.: Quaternion algebra. Graduate Texts in Mathematics, vol. 288, Springer international Publishing (2020)
54. Wesolowski, B.: Orientations and the supersingular endomorphism ring problem. In: Dunkelman, O., Dziembowski, S. (eds.) EUROCRYPT 2022, Part III. LNCS, vol. 13277, pp. 345–371. Springer, Heidelberg (May / Jun 2022). https://doi.org/10.1007/978-3-031-07082-2_13

55. Wesolowski, B.: The supersingular isogeny path and endomorphism ring problems are equivalent. In: 62nd FOCS. pp. 1100–1111. IEEE Computer Society Press (Feb 2022). https://doi.org/10.1109/FOCS52979.2021.00109