

The SQInstructor: a guide to SQIsign and the Deuring Correspondence with level structures

Giacomo Borin^{1,2}, Luca De Feo¹, Guido Lido³, and Sina Schaeffler^{1,4}

¹ IBM Research Europe, Switzerland

² University of Zurich, Switzerland

³ University of Roma Tor Vergata, Italy

⁴ ETH Zurich, Switzerland

Abstract. We explore the use of level structures to generalize the SQIsign signature scheme. We give a general framework where, given the public key and the commitment, the challenge is to exhibit an isogeny between them with an additional requirement, namely to map a chosen level structure to another. We then instantiate the framework using 1-dimensional and 2-dimensional isogenies. In doing that we provide a new explicit Deuring correspondence for supersingular elliptic curves with level structures and solve new constrained norm equations.

1 Introduction

Isogeny-based cryptography is a promising candidate for post-quantum cryptography, with several proposals for key exchange and digital signatures, but also for more advanced primitives such as threshold and ring signatures.

A mainstay of isogeny-based cryptography is SQIsign [25], which is so far the most compact signature scheme participating in NIST’s post-quantum standardization process [37]. At its heart, it is based on the *Deuring correspondence*, a mathematical and algorithmic equivalence between supersingular curves and orders of a quaternion algebra.

The original instantiation of SQIsign constructs signatures by solving some quadratic equations in the quaternion algebra, using an algorithm known as KLPT [32,26]. This approach gives very compact signatures, with a relatively simple verification procedure, but a quite involved and slow signing procedure. It also presents an intrinsic difficulty in proving EUF-CMA security, owing to the limitations of KLPT. A paradigm shift for SQIsign, first proposed in [22] and then improved [8,27,36], came with the introduction of *higher-dimensional (HD) isogenies*. Building upon a line of work started with the SIDH attacks [15,35,41], these techniques significantly sped up SQIsign and improved its provable security.

Author list in alphabetical order; see <https://ams.org/profession/leaders/CultureStatement04.pdf>.

Taking a step back, *level structures* are bases of torsion subgroups of elliptic curves, up to transformation by a well chosen group of matrices. They have been used to prove indistinguishability of certain distributions on supersingular isogeny graphs [7], and to classify hardness assumptions in isogeny-based cryptography [24]. However level structures are implicitly featured in many more isogeny-based protocols, for example in SIKE [31] or FESTA [10]. Even SQIsign itself can be understood in terms of level structures. Indeed, a *response* in the SQIsign interactive identification protocol is generally understood to be an isogeny connecting a *public key curve* to a *challenge curve*. The challenge curve is generated as the codomain of a *challenge isogeny*, which is itself defined in terms of its *kernel*, a form of level structure. Thus, an equivalent characterization of a SQIsign signature is as an isogeny (the composition of response and challenge isogeny) vanishing on a level structure (the kernel). This point of view is especially visible in the variant of SQIsign named SQIprime [27].

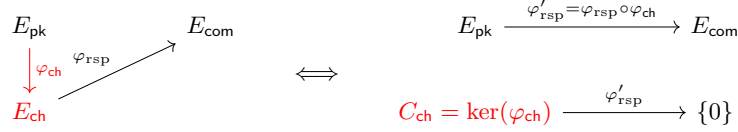


Fig. 1. SQIsign simplified (generation of key and of commitment is omitted)

With this point of view, it is very natural to consider signatures where the response is requested to send a certain cyclic subgroup (or a suitable level structure) to another one, instead of annihilating it. This is exactly the idea of our new proposal: SQInstructor is a general framework following this idea, with freedom to choose the kind of level structure and whether the response should be computed with one-dimensional or with HD techniques.

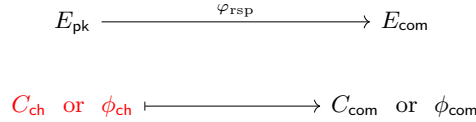


Fig. 2. SQInstructor simplified (generation of key and of commitment is omitted)

Contributions. In this work we instantiate and explore in detail the use of level structures for the SQInstructor protocol. Progressively in each section we:

- Generalize the well-known Deuring Correspondence to the setting of supersingular elliptic curves with level structure, with some concrete examples.

Remarkably, we show how to make this correspondence explicit, even for large non-smooth levels.

- We describe the new identification scheme SQInstructor in full generality, leaving open the choice of the level structure and isogeny representation for the specific instantiation of the protocol.
- Instantiating the framework using 1-dimensional isogenies, *a la* [25] requires solving specific *constrained* norm equations in the quaternion algebra $\mathcal{B}_{p,\infty}$. We show how to modify and combine previous algorithms in the literature to efficiently solve these equations in practice. We believe this is of independent interest. We also give a proof-of-concept implementation of these algorithms.
- We instantiate the framework using 2-dimensional isogenies, prove its security under assumptions similar to those of SQIsign, and give an optimized implementation based on [1].

Related work. Arpin [4] initiated the study of supersingular isogeny graphs with Borel level structure and generalized the Deuring correspondence to them. Here we extend the correspondence to even more general level structures, and explain for the first time how to build SQIsign-like identification protocols from it.

In [24], level structures were used to classify SIDH-like hardness assumptions and prove reductions between them, showing in particular that the SIDH attacks [15,35,41] apply to a broader class of problems than initially thought. Although we use level structures in this work, we only do so constructively and we never rely on the kind of assumptions studied in [24]. The security of SQInstructor rests on the same foundations as SQIsign itself.

Basso, De Feo, Patranabis, Radulescu and Wesolowski [9] introduce an abstract framework for SQIsign-like schemes called *forensic categories*. Among the proposed instantiations of the framework, one is based on level structures and yields an identification protocol equivalent to SQInstructor’s⁵ Their work is complementary to ours: whereas they focus on protocols and show that one can construct ring signatures and chameleon hashes from any forensic category, we focus on algorithms, carefully generalizing the Deuring correspondence and explaining how to implement SQInstructor’s 1- and 2-dimensional variants.

Acknowledgments. We thank Andrea Basso, Sikhar Patranabis, Ilinca Radulescu and Benjamin Wesolowski for the useful discussions, and Antonin Leroux for pointers to KLPT variants.

The third author is supported by the MIUR Excellence Department Project MatMod@TOV awarded to the Department of Mathematics, University of Rome Tor Vergata, by the PRIN PNRR 2022 “Mathematical Primitives for Post Quantum Digital Signatures” and by GNSAGA - INdAM. All other authors are supported by SNSF Consolidator Grant CryptonIs 213766.

⁵ Precisely, equivalent to the 1-dimensional variant of Section 5.

2 The Deuring Correspondence in Cryptography

We recall here some basic facts about the Deuring correspondence and its applications to cryptography, in particular to SQIsign. We assume some familiarity with elliptic curves, isogenies and quaternion algebras. For more details, we refer to [42,44,23,12].

Throughout this document we fix a prime p and we write $\mathbb{F}_p$ for the finite field with p elements, $\mathbb{F}_{p^2}$ for a field extension of degree 2, and $\overline{\mathbb{F}}_p$ for their algebraic closure. Finally, we write $\mathcal{B}_{p,\infty}$ for the quaternion algebra ramified at p and at infinity.

An equivalence of categories. If E, E' are elliptic curves, we write $\text{Hom}(E, E')$ for the group of homomorphisms $E \rightarrow E'$, and $\text{End}(E) := \text{Hom}(E, E)$. As a $\mathbb{Z}$ -module, $\text{Hom}(E, E')$ has finite rank, and the usual degree map is a positive definite quadratic form on it. In short, $\text{Hom}(E, E')$ is a Euclidean lattice. On top of that, composition of morphisms makes $\text{End}(E')$ a ring and $\text{Hom}(E, E')$ a left $\text{End}(E')$ -module.

Deuring proved that if E, E' are supersingular curves in characteristic p , then $\text{Hom}(E, E')$ has rank 4 and $\text{End}(E')$ is isomorphic to a maximal order in $\mathcal{B}_{p,\infty}$. But his correspondence goes even deeper: it shows that isomorphism classes of supersingular elliptic curves, up to Galois conjugation in $\mathbb{F}_{p^2}/\mathbb{F}_p$, are in one-to-one correspondence with isomorphism types of maximal orders of $\mathcal{B}_{p,\infty}$ (both sets are finite), and that the integral left ideals of $\text{End}(E)$ are in one-to-one correspondence with the isogenies of E , up to post-composition with isomorphisms. In modern terms, fixing a curve E_0 and an order $\mathcal{O}_0 \simeq \text{End}(E_0)$, the functor $\text{Hom}(-, E_0)$ defines an equivalence of categories between supersingular elliptic curves with isogenies and invertible left $\mathcal{O}_0$ -modules with non-zero homomorphisms.

Theorem 1. *Let E_0 be a supersingular curve and let $\rho : E_0 \rightarrow E$ be an isogeny. Define the ideal*

$$I_\rho := I_{\rho,E} := \{\psi \circ \rho : \psi \in \text{Hom}(E, E_0)\} \subset \text{End}(E_0), \quad (1)$$

then $n(I_\rho) = \deg(\rho)$. Two isogenies ρ, ρ' define the same ideal if and only if $\rho' = \iota \circ \rho$ for some isomorphism ι . Any integral ideal of $\text{End}(E_0)$ arises this way.

In what follows, we shall write $I_\rho \star E_0$ for the isomorphism class of E , and sometimes abuse notation and simply write $E = I_\rho \star E_0$. Two ideals I, J yield the same class $I \star E_0 = J \star E_0$ if and only if they are in the same left ideal class, i.e., if and only if $I = J\alpha$ for some $\alpha \in \mathcal{B}_{p,\infty}$. Equivalently, we may write $[I]$ for the ideal class of I and $[I] \star E_0$ for the unique isomorphism class of $I \star E_0$.

An algorithmic tool. Deuring's correspondence also has an algorithmic content that isogeny-based cryptography has helped unearth. It can be summarized

by the mantra: *some problems are hard for curves, every problem becomes easy in the quaternions.*

Concretely, the foundations of isogeny-based cryptography rest on the famous *isogeny problem*:

Problem 2 (Supersingular Isogeny Problem). Given supersingular elliptic curves $E, E'/\mathbb{F}_{p^2}$, compute an isogeny between them.

This problem is assumed to be exponentially hard, even for quantum computers, when at least one of E or E' is chosen at random. But the analogous problem for quaternions, that is to compute a *connecting ideal* between two given maximal orders of $\mathcal{B}_{p,\infty}$, is solved by basic integer linear algebra. In fact, Kohel, Lauter, Petit and Tignol [32] showed that even a more restricted variant of the problem, where the connecting ideal is requested to have prime-power norm, can be solved in polynomial time. Their algorithm has become a staple of isogeny-based cryptography, under the name of KLPT.

This disparity between curves and quaternions suggests a strategy to solve the isogeny problem: because curves are in (almost) one-to-one correspondence with maximal order types, if we could effectively evaluate this correspondence, we could translate isogeny problems to quaternion problems, solve them and bring the solution back to the curves. The intuition checks out and leads to the inevitable conclusion that computing endomorphism rings of supersingular elliptic curves is generically hard. The problem below is indeed proven polynomial-time equivalent to the isogeny problem for a random input curve, assuming GRH [45].

Problem 3 (Supersingular Endomorphism Ring Problem). Given a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$, find a basis for $\text{End}(E)$.

On the other hand, the “converse” problem is now known to be easy: given a maximal order $\mathcal{O}$ of $\mathcal{B}_{p,\infty}$, a supersingular curve such that $\text{End}(E) \simeq \mathcal{O}$ may be computed as follows:

1. Start with a pair $(E_0, \mathcal{O}_0)$ such that $\text{End}(E_0) \simeq \mathcal{O}_0$;⁶
2. Use KLPT to compute a connecting ideal I between $\mathcal{O}_0$ and $\mathcal{O}$ of norm ℓ^n for some small prime ℓ ;
3. Use an *ideal-to-isogeny* algorithm [28] to compute $E = I \star E_0$ by evaluating an isogeny of degree ℓ^n . Then $\text{End}(E) \simeq \mathcal{O}$.

Or at least this is how one would have solved the problem before 2022. The discovery of efficient attacks on SIKE [15,35,41] brought several innovations in isogeny-based cryptography, including more efficient ideal-to-isogeny algorithms [39,8,36,13]. These leverage *higher dimensional isogenies* to bypass the constraint of small-prime-power isogenies and thus dispense with KLPT entirely. There also exist *isogeny-to-ideal* algorithms, though they are currently more limited in scope (see [17]). We will not discuss them as they are not necessary for our purpose.

⁶ For any p , there exists a polynomial-time algorithm to produce a supersingular curve together with its endomorphism ring. Note this does not contradict the fact that computing endomorphism rings of random curves is hard.

From the correspondence to cryptography. Summarizing, it is easy to construct supersingular curves knowing their endomorphism rings, but once we throw away this information it is hard to recover it. This defines at the very least a one-way function, but hopefully something more. The first to observe that one could use the knowledge of the endomorphism ring as a “trapdoor” in a signature scheme were Galbraith, Petit and Silva (GPS) [29], but it is only with SQIsign [25] that the Deuring correspondence truly showed its full potential.

Both protocols define public parameters $(E_0, \mathcal{O}_0)$ with $\mathcal{O}_0 \simeq \text{End}(E_0)$. Both generate the secret key as a random ideal $I_{\text{sk}} \subset \mathcal{O}_0$, and define the public key as $E_{\text{pk}} := I_{\text{sk}} \star E_0$. Both are based on sigma-protocols proving knowledge of $\text{End}(E_{\text{pk}})$, but while GPS resembles the classic GMW protocol for graph isomorphism [30], SQIsign uses a radically different strategy achieving exponentially low soundness error. Seen from afar, SQIsign’s interactive protocol proceeds as follows:

1. The prover generates a random ideal $I_{\text{com}} \subset \mathcal{O}_0$, computes $E_{\text{com}} := I_{\text{com}} \star E_0$ and sends E_{com} to the verifier;
2. The verifier responds with a challenge $P_{\text{ch}} \in E_{\text{pk}}[N]$, a point of fixed (and smooth) order N on E_{pk} ;
3. The prover uses its knowledge of $\text{Hom}(E_{\text{pk}}, E_{\text{com}}) \simeq \overline{I_{\text{sk}}} I_{\text{com}}$ to produce an isogeny $\varphi_{\text{rsp}} : E_{\text{pk}} \rightarrow E_{\text{com}}$ such that $\varphi_{\text{rsp}}(P_{\text{ch}}) = 0$, sends φ_{rsp} to the verifier.
4. The verifier checks that φ_{rsp} matches all constraints.

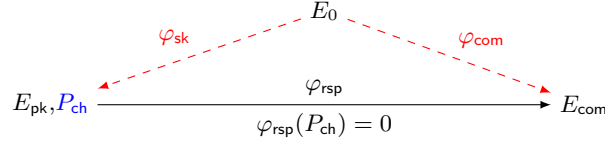


Fig. 3. SQIsign identification protocol. Secrets dashed in red. Challenge in blue.

The key difference between GPS and SQIsign lies in Step 2. There are $\approx N^2$ choices for P_{ch} , though linearly equivalent points are effectively the same challenge, so the number of distinct challenges is rather $\approx N$. Because the protocol is proven 2-special sound, it has soundness error $\approx 1/N$, as opposed to $1/2$ for GPS. If N is exponentially large, it thus suffices to run a single iteration of the identification protocol to achieve the desired level of security.

At first sight, using torsion points as challenges may seem a hack with little relation to the Deuring correspondence. Looking closer we notice that the set $\Lambda \subset \text{Hom}(E_{\text{pk}}, E_{\text{com}})$ of isogenies vanishing on P_{ch} forms a sublattice. Precisely, letting $\varphi_{\text{ch}} : E_{\text{pk}} \rightarrow E_{\text{ch}}$ be the isogeny such that $\ker \varphi_{\text{ch}} = \langle P_{\text{ch}} \rangle$, we have

$$\Lambda = \{ \psi \circ \varphi_{\text{ch}} : \psi \in \text{Hom}(E_{\text{ch}}, E_{\text{com}}) \}. \quad (2)$$

Some readers will find our explanation unnecessarily contrived: we may as well have said that φ_{ch} is the challenge sent by the verifier, and that the response

is computed from $\text{Hom}(E_{\text{ch}}, E_{\text{com}})$. However this point of view, which is the traditional way of presenting SQIsign, misses two important points: First, if φ_{ch} is the challenge, we need an isogeny-to-ideal algorithm, somewhat complicating the protocol. This was already observed in [27]. Second, there are potentially other choices of sublattices $\Lambda \subset \text{Hom}(E_{\text{pk}}, E_{\text{com}})$ that lead to interesting variants of SQIsign. This is the topic of the present work.

Roadmap. We start by characterizing which restrictions on $\text{Hom}(E, E')$ lead to a generalized Deuring correspondence. It is tempting to impose that a point $P \in E[N]$ is mapped to some other point $P \in E'[N]$, but this restriction does not define a sublattice of $\text{Hom}(E, E')$. We will see instead in the next section that the appropriate concept is that of mapping elliptic curves with *level structures*, extending previous work of Arpin on *Borel level structures* [5].

The rest of the paper will be devoted to adapting SQIsign and its building blocks to the new framework. In Section 4 we present SQInstructor, a general template for instantiating signature schemes from our generalized Deuring correspondence, and analyze its security properties insofar as they are independent of the choice of level structure and isogeny-to-ideal algorithm. In Section 5 we show that the KLPT algorithm can be generalized to find connecting ideals with restrictions defined by level structures. This lets us instantiate protocols using exclusively isogenies of elliptic curves (aka, one-dimensional isogenies), in the style of pre-SIDH-attacks SQIsign. Although modern SQIsign has moved away from one-dimensional isogenies for efficiency, these algorithms are still very much relevant for SQIsign-like ring signatures [14] and chameleon hashes [9]. Finally, in Section 6 we analyze in detail a modern instantiation of SQInstructor, using higher dimensional isogenies, and compare it to the latest version of the NIST candidate SQIsign.

3 Level structures and the Deuring Correspondence

We start by studying how isogenies map torsion subgroups of elliptic curve, then enlarge the perspective to isogenies mapping level structures, and finally generalize the Deuring correspondence to them.

3.1 From ideals to matrices via isogenies

Fix a positive integer N , let $\mathbb{Z}/N\mathbb{Z} := \mathbb{Z}/N\mathbb{Z}$, with group of units $(\mathbb{Z}/N\mathbb{Z})^*$. For E an elliptic curve defined over a field of characteristic not dividing N , a basis of the N -torsion group $E[N]$ is any ordered pair of points $\mathcal{B} = (P, Q)$ that generate $E[N]$. Then the ring $M_2(\mathbb{Z}/N\mathbb{Z})$ of 2×2 matrices modulo N acts on pairs of elements of $E[N]$ as follows

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{pmatrix} P \\ Q \end{pmatrix} = \begin{pmatrix} aP+bQ \\ cP+dQ \end{pmatrix}. \quad (3)$$

If for every elliptic curve E we make an arbitrary choice of a basis of $E[N]$, we can associate to any isogeny a matrix as follows.

Definition 4. Given a morphism of elliptic curves $\varphi: E \rightarrow E'$ and bases (P, Q) and (P', Q') of $E[N]$ and $E'[N]$, the matrix representation of φ on the N -torsion is the matrix $M_\varphi \in M_2(\mathbb{Z}/N)$ such that⁷

$$\begin{pmatrix} \varphi(P) \\ \varphi(Q) \end{pmatrix} = M_\varphi \cdot \begin{pmatrix} P' \\ Q' \end{pmatrix}. \quad (4)$$

The map $\varphi \mapsto M_\varphi$ defines a homomorphism of abelian groups, and in the case of supersingular elliptic curves it is surjective.

Lemma 5. Let N be a positive integer, let E, E' be supersingular elliptic curves in characteristic $p \nmid N$. Then the natural map

$$\text{Hom}(E, E') \longrightarrow \text{Hom}(E[N], E'[N]) \quad (5)$$

is surjective. In other words if we choose bases $(P, Q), (P', Q')$ of $E[N], E'[N]$ the map $\varphi \mapsto M_\varphi$ is surjective.

Proof. The kernel of the map (5) is the set of morphisms $\varphi: E \rightarrow E'$ such that $E[N] \subset \ker \varphi$, i.e. the maps $\varphi \in N\text{Hom}(E, E')$ by [42, Chapter III, Corollary 4.11]. After quotienting by the kernel, the map (5) becomes an injection

$$\frac{\text{Hom}(E, E')}{N\text{Hom}(E, E')} \hookrightarrow \text{Hom}(E[N], E'[N]) \cong M_2(\mathbb{Z}/N).$$

But for supersingular curves $\text{Hom}(E, E')$ is a rank 4 lattice, hence all the above groups have order equal to N^4 and the map is surjective. The last part of the statement is simply an explicit choice for the map following from having chosen bases of $E[N]$ and $E'[N]$. $\square$

This homomorphism enjoys several other properties:

- It is contravariant with respect to composition: given $\varphi: E \rightarrow E'$ and $\psi: E' \rightarrow E''$ we have $M_{\psi \circ \varphi} = M_\varphi \cdot M_\psi$.
- If the bases have the same Weil pairing $e(P, Q) = e(P', Q')$, then $\det M_\varphi = \deg \varphi \pmod{N}$; in particular this is the case if φ is an endomorphism.
- If $\widehat{\varphi}$ is the dual of φ , then $M_{\widehat{\varphi}} \cdot M_\varphi = \deg(\varphi) \cdot \text{Id}$; in particular, if $\deg \varphi = \det M_\varphi \pmod{N}$, then $M_{\widehat{\varphi}} = M_\varphi^\dagger$, the adjoint of M_φ .

We would like to extend this mapping to the ideals defined in Theorem 1, however we must be careful because ideals only correspond to isogenies up to isomorphism, thus even after fixing (P, Q) and (P', Q') the action of an ideal is only defined up to automorphisms of E' . Keeping this ambiguity in mind, we associate to an integral ideal one among the possible corresponding isogenies. Having made this choice for one ideal is enough to fix the choice for all equivalent ideals. Indeed looking at Eq. (1), if $I = I_\varphi$ is associated to $\varphi: E \rightarrow E'$ then we have maps

$$\begin{aligned} \text{Hom}(E, E') &\xleftarrow{\xi_I} I = I_\varphi \xrightarrow{\chi_I} \{\text{ideals equivalent to } I\} \\ \xi_I(\alpha) = \frac{1}{\deg \varphi} \varphi \circ \widehat{\alpha} &\longleftrightarrow \alpha \longmapsto \chi_I(\alpha) = \frac{I\widehat{\alpha}}{\mathfrak{n}(I)}. \end{aligned} \quad (6)$$

⁷ To simplify notation we omit the dependence on N and the bases (P, Q) and (P', Q') .

It is easy to check that $\xi_I(\alpha)$ is one of the (not so many) isogenies associated to $\chi_I(\alpha)$. Then, with a small abuse of notation, we extend the correspondence to matrices: given an integral ideal $J = \chi_I(\alpha)$ equivalent to I , we associate to it

$$\mathbf{M}_J := \mathbf{M}_{\xi_I(\alpha)} = \frac{\mathbf{M}_\alpha^\dagger \mathbf{M}_\varphi}{\deg \varphi}. \quad (7)$$

Notice moreover that the map χ_I is defined also when I is any fractional ideal and α is any quaternion. We summarize this in Algorithm 1, which solves the special case where we look for an equivalent ideal mapping (P, Q) to (P', Q') .

Algorithm 1 `InStructIdeal`

Input: Supersingular curves E, E' with bases $\langle P, Q \rangle = E[N]$ and $\langle P', Q' \rangle = E'[N]$;
Input: A basis $\langle \alpha_1, \dots, \alpha_4 \rangle$ of $\mathcal{O}(E)$ and the matrices $\mathbf{M}_{\alpha_1}, \dots, \mathbf{M}_{\alpha_4}$ wrt (P, Q) ;
Input: An ideal I_ζ associated to an isogeny $\zeta : E \rightarrow E'$ of degree coprime to N ;
Input: The matrix $\mathbf{M}_\zeta$ wrt (P, Q) and (P', Q') ;
Output: $I_\rho \sim I_\zeta$ such that $M_{I_\rho} = \text{Id}$.
1: Let $\langle \beta_1, \dots, \beta_4 \rangle$ be a basis of I_ζ , compute $\mathbf{M}_{\beta_1}, \dots, \mathbf{M}_{\beta_4}$ by linearity;
2: Find by linear algebra $n_1, \dots, n_4 \in \mathbb{Z}/N$ s.t. $n_1 \mathbf{M}_{\beta_1} + \dots + n_4 \mathbf{M}_{\beta_4} = \frac{n(I_\zeta)}{\det \mathbf{M}_\zeta} \mathbf{M}_\zeta$;
3: Set $\alpha = n_1 \beta_1 + \dots + n_4 \beta_4$;
4: **return** $I_\rho \leftarrow \chi_{I_\zeta}(\alpha)$.

Remark 6. Algorithm 1 requires as input a basis of $\langle \alpha_1, \dots, \alpha_4 \rangle$ for which we know the corresponding $\mathbf{M}_{\alpha_i}$. If N is smooth, then the α_i can be arbitrary, as long as they can be evaluated: the matrices are then computed through a generalized discrete logarithm.

When N contains a large prime factor, instead, we construct the basis along with (P, Q) . For special orders, such as $\mathcal{O}(E_0)$, we look for two endomorphisms α, β such that

1. $1, \alpha, \beta, \beta\alpha$ generate $\text{End}(E_0)/N\text{End}(E_0)$ as a $\mathbb{Z}/N$ -module,
2. we know $P \in E_0[N]$, an eigenvector of α with non-zero eigenvalue.
3. $\langle P, \beta(P) \rangle$ form a basis of $E_0[N]$.

Then the matrices $\mathbf{M}_\alpha, \mathbf{M}_\beta, \mathbf{M}_{\beta\alpha}$ on the basis $(P, \beta(P))$ follow by direct computation. When $E_0 : y^2 = x^3 + x$, we can take $\beta = \iota = \sqrt{-1}$ and $\alpha = \pi + n\iota$, with π the Frobenius endomorphism and n integer such that $(-p - n^2)$ is a quadratic residue modulo N , so that $\sqrt{-p - n^2} \pmod{N}$ is an eigenvalue of α .

For other orders, the information can be transported via an isogeny from E_0 , as detailed in Remark 15.

3.2 Level Structures

Restricting the action of Eq. (3) to the group $\text{GL}_2(\mathbb{Z}/N)$ of invertible matrices, we get an action of $\text{GL}_2(\mathbb{Z}/N)$ on the set of bases of $E[N]$. Given a subgroup Γ

of $\mathrm{GL}_2(\mathbb{Z}/N)$ a Γ -level structure, or simply Γ -structure on an elliptic curve E is a basis for $E[N]$ up to change of basis by matrices in Γ : given a basis (P, Q) of $E[N]$, the Γ -level structure containing it is

$$\Gamma \cdot \begin{pmatrix} P \\ Q \end{pmatrix} = \{ M \cdot \begin{pmatrix} P \\ Q \end{pmatrix} \mid M \in \Gamma \} . \quad (8)$$

The integer N is referred to as the *level*.

For example, the bases of the $E[N]$ are $\{\mathrm{Id}\}$ -structures, we call these *full-level structures*. In this work we focus on the following level structures:

- *Borel level structures* are the level structures relative to the Borel subgroup

$$\Gamma_0 = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \mid a \cdot d \in (\mathbb{Z}/N)^*, b \in \mathbb{Z}/N \right\} . \quad (9)$$

Borel structures of level N on E are in bijection with cyclic subgroups $C \subset E$ of order N : a Borel structure $\Gamma_0 \cdot \begin{pmatrix} P \\ Q \end{pmatrix}$ corresponds to $C = \langle Q \rangle$ since $\Gamma_0 \cdot \begin{pmatrix} P \\ Q \end{pmatrix}$ is exactly the set of bases (P', Q') with $Q' \in C$.

- *Split Cartan level structures*, i.e. diagonal level structures, relative to

$$\Gamma = \left\{ \begin{bmatrix} \lambda & 0 \\ 0 & \mu \end{bmatrix} \mid \lambda, \mu \in (\mathbb{Z}/N)^* \right\} .$$

They correspond to ordered pairs of cyclic subgroups whose direct sum is $E[N]$; indeed $\Gamma \cdot \begin{pmatrix} P \\ Q \end{pmatrix}$ is the set of bases (P', Q') with $Q' \in \langle Q \rangle$ and $P' \in \langle P \rangle$.

- *Scalar level structures*, i.e. Z -level structures, with

$$Z = \left\{ \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix} \mid \lambda \in (\mathbb{Z}/N)^* \right\} .$$

If $\alpha: E \rightarrow E'$ is an isogeny of degree coprime to N and $S = \Gamma \cdot \begin{pmatrix} P \\ Q \end{pmatrix}$ is a Γ -structure, we define

$$\alpha(S) = \Gamma \cdot \begin{pmatrix} \alpha(P) \\ \alpha(Q) \end{pmatrix} , \quad (10)$$

which is a well defined Γ -structure, in particular the above definition does not depend on the choice of $\begin{pmatrix} P \\ Q \end{pmatrix} \in S$.

The assumption $\gcd(N, \deg \alpha) = 1$ is necessary and sufficient to ensure that $(\alpha(P), \alpha(Q))$ is a basis of $E'[N]$, however it will be convenient to extend definitions to isogenies of degree not coprime to N . We let $\langle \Gamma \rangle \subset \mathrm{M}_2(\mathbb{Z}/N)$ be the set of all $\mathbb{Z}/N$ -linear combinations of elements in Γ , and we define the set of all linear combinations of pairs of points in $S = \Gamma \cdot \begin{pmatrix} P \\ Q \end{pmatrix}$ as

$$\langle S \rangle = \langle \Gamma \rangle \cdot \begin{pmatrix} P \\ Q \end{pmatrix} = \{ \gamma \cdot \begin{pmatrix} P \\ Q \end{pmatrix} \mid \gamma \in \langle \Gamma \rangle \} \subset E[N] \times E[N] , \quad (11)$$

which, again, does not depend on the choice of $\begin{pmatrix} P \\ Q \end{pmatrix} \in S$.

Definition 7. Let N be a positive integer and Γ be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N)$.

1. A (supersingular) elliptic curve with Γ -level structure is a pair $\mathbb{E} = (E, S)$ where E is a (supersingular) elliptic curve defined in characteristic not dividing N and S is a Γ -level structure on E .

2. Given two elliptic curves with Γ -level structures (E, S) and (E', S') , the set of homomorphisms between them is

$$\mathrm{Hom}((E, S), (E', S')) = \{\alpha: E \rightarrow E' : \alpha(S) \subseteq \langle S' \rangle\}. \quad (12)$$

We use the notation $\alpha: (E, S) \rightarrow (E', S')$ for such homomorphisms. Moreover α is an isomorphism between (E, S) and (E', S') if it has degree 1.

3. The endomorphism ring of an elliptic curve with Γ -level structure (E, S) is

$$\mathcal{O}(E, S) = \mathrm{End}(E, S) := \mathrm{Hom}((E, S), (E, S)) = \{\alpha \in \mathrm{End}(E) \mid \alpha(S) \subseteq \langle S \rangle\}.$$

Connecting level structures to the matrix representation of Definition 4, $\varphi \in \mathrm{Hom}((E, S), (E', S'))$ if and only if $M_\varphi \in \langle \Gamma \rangle$ for an arbitrary choice of representatives of S, S' , and $\varphi(S) = S'$ if and only if $M_\varphi \in \Gamma$.

Remark 8. From the characterization in terms of representation matrices, we notice that $\mathrm{Hom}((E, S), (E', S'))$ only depends on $\langle \Gamma \rangle$, in particular Γ and $\langle \Gamma \rangle \cap \mathrm{GL}_2(\mathbb{Z}/N)$ give the same Hom . This justifies the following definition.

Definition 9. $\Gamma \subset \mathrm{GL}_2(\mathbb{Z}/N)$ is additively stable if $\Gamma = \mathrm{GL}_2(\mathbb{Z}/N) \cap \langle \Gamma \rangle$.

The scalar, Borel and Cartan subgroups are all additively stable, but the trivial group or Γ_1 (see [24, Section 5.4] for a definition) are not. Moreover if Γ is additively stable, an isogeny $\varphi \in \mathrm{Hom}((E, S), (E', S'))$ has degree coprime to N if and only if it satisfies $\varphi(S) = S'$, which is stronger than $\varphi(S) \subseteq \langle S' \rangle$.

Lemma 5 implies that, given $\mathbb{E} = (E', S')$, $\mathbb{E}' = (E', S')$ supersingular elliptic curves with Γ -structure, $\mathrm{Hom}(\mathbb{E}, \mathbb{E}')$ is not empty. It is, in fact, a sublattice inheriting the usual scalar product, norm and length from $\mathrm{Hom}(E, E')$, namely

$$\langle \alpha, \beta \rangle = \frac{1}{2} \mathrm{tr}(\hat{\alpha} \circ \beta), \quad n(\alpha) = \deg(\alpha), \quad |\alpha| = \sqrt{\deg \alpha}. \quad (13)$$

Corollary 10. Let p be a prime, N be a positive integer not divisible by p and Γ a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N)$. Let $c_\Gamma = [M_2(\mathbb{Z}/N) : \langle \Gamma \rangle]$. Let $\mathbb{E}$ and $\mathbb{E}'$ be supersingular elliptic curves with Γ -structure in characteristic p .

1. $\mathrm{Hom}(\mathbb{E}, \mathbb{E}')$ is a (non-empty) 4-dimensional sublattice of $\mathrm{Hom}(E, E')$ of index equal to c_Γ and covolume $\frac{p}{4} \cdot c_\Gamma$.
2. If $\varphi \in \mathrm{Hom}(\mathbb{E}, \mathbb{E}')$ then $\hat{\varphi} \in \mathrm{Hom}(\mathbb{E}', \mathbb{E})$. Also, if Γ contains the group of scalar matrices, $\varphi(S) = S'$ if and only if $\hat{\varphi}(S') = S$.
3. For each positive integer M , the lattice $\mathrm{Hom}(\mathbb{E}, \mathbb{E}')$ contains an element of degree prime to M .
4. The set $\mathcal{O}(\mathbb{E})$ is a subring of $\mathrm{End}(E)$ of finite index c_Γ closed under dual; in particular it is an order.
5. There is always an isogeny $\varphi \in \mathrm{Hom}(\mathbb{E}, \mathbb{E}')$ of degree less than or equal to $2\sqrt{2pc_\Gamma}/\pi$.

Proof. The lattice $\mathrm{Hom}(\mathbb{E}, \mathbb{E}')$ is the kernel of the surjective map $\mathrm{Hom}(E, E') \rightarrow M_2(\mathbb{Z}/N)/\langle \Gamma \rangle$, thus it is a sublattice of $\mathrm{Hom}(E, E')$ of finite index c_Γ . Statement 1 follows from $\mathrm{Hom}(E, E')$ having covolume $\frac{p}{4}$. Statements 2 and 3 follow from Lemma 5 and Remark 8. Statement 4 is then immediate. The last statement follows from Minkowski's theorem. $\square$

3.3 Generalising the Deuring correspondence

We now extend the Deuring Correspondence to the context of supersingular elliptic curves with level structures. This also generalizes work of Sarah Arpin done in [4] for Borel level structures.

Given a supersingular elliptic curve with Γ -structure $\mathbb{E}$ the natural analogue of the maximal order $\mathcal{O} = \text{End}(E)$ is the subring $\mathcal{O}(\mathbb{E}) = \text{End}(\mathbb{E})$ in Definition 7, that is again an order in $\mathcal{B}_{p,\infty}$ by Corollary 10.

Remark 11. In general, when considering non-trivial level structures, there is not a bijection between supersingular elliptic curves with Γ -level structure and orders in $\mathcal{B}_{p,\infty}$. In fact, if there exists a matrix $M \notin \Gamma$ in the normalizer of Γ in $\text{GL}_2(\mathbb{Z}/N)$, i.e. $M^{-1}\Gamma M = \Gamma$, then it is immediate to check that $\mathcal{O}(E, S) = \mathcal{O}(E, MS)$ even if usually⁸ (E, S) and (E, MS) are not isomorphic.

The relevant ideals, in the context of supersingular elliptic curves with level structure are the following.

Definition 12. Let $\mathbb{E}, \mathbb{E}'$ be as in Corollary 10. Given $0 \neq \rho \in \text{Hom}(\mathbb{E}, \mathbb{E}')$, let

$$I_\rho := I_{\rho, \mathbb{E}'} := \{\psi \circ \rho : \psi \in \text{Hom}(\mathbb{E}', \mathbb{E})\} \subset \mathcal{O}(\mathbb{E}) . \quad (14)$$

Since $\text{Hom}(\mathbb{E}', \mathbb{E})$ is a left $\mathcal{O}(\mathbb{E})$ -module by postcomposition, then $I_{\rho, \mathbb{E}'}$ is a left ideal of $\mathcal{O}(\mathbb{E})$. Not all $\mathcal{O}(\mathbb{E})$ -ideals can be obtained as in Definition 12, only locally principal ones, i.e. ideals $I \subset \mathcal{O}(\mathbb{E})$ such that, for all primes $\ell \in \mathbb{Z}$ the ideal $I \otimes \mathbb{Z}_\ell$ of $\mathcal{O}(\mathbb{E}) \otimes \mathbb{Z}_\ell$ is generated by one element (a heuristic explanation is that $\mathcal{O}(\mathbb{E}) \otimes \mathbb{Z}_\ell$ and $\mathcal{O}(\mathbb{E}') \otimes \mathbb{Z}_\ell$ are isomorphic, and we can interpret ρ as a local generator, for the rigorous proof see Theorem 13). For example if Γ is the group of scalar matrices, then $N\text{End}(E)$ is non-principal as $\mathcal{O}(\mathbb{E})$ -ideal for $N > 1$, and it is not of the form (14).

If we change ρ with $\rho' : \mathbb{E} \rightarrow \mathbb{E}'$, the ideal changes to an equivalent one:

$$I_{\rho', \mathbb{E}'} = I_{\rho, \mathbb{E}'} \cdot \frac{\hat{\rho} \circ \rho'}{\deg \rho} . \quad (15)$$

The converse is not true in general: there may be equivalent ideals corresponding to different codomains $\mathbb{E}'$ (see Remark 8), unless Γ is additively stable, in which case we write $[I_{\mathbb{E}'}]$ for the ideal class of $I_{\rho, \mathbb{E}'}$.

Up to these two observations, the Deuring correspondence generalises, as summarized in Table 1.

Theorem 13. Let $p, N, \Gamma, \mathbb{E}, \mathbb{E}'$ be as in Corollary 10. For each $\rho : \mathbb{E} \rightarrow \mathbb{E}'$ the ideal $I_{\rho, \mathbb{E}'}$ is locally principal, with norm

$$n(I_{\rho, \mathbb{E}'}) := \gcd(\{\deg(\alpha) \mid \alpha \in I_{\rho, \mathbb{E}'}\}) = \sqrt{[\mathcal{O}(\mathbb{E}) : I_{\rho, \mathbb{E}'}]} = \deg(\rho) .$$

Moreover, if we denote by $\bar{\cdot}$ the conjugation in $\mathcal{B}_{p,\infty}$ and we identify $\mathcal{O}(\mathbb{E}')$ with

$$\frac{1}{\deg \rho} \hat{\rho} \circ \mathcal{O}(\mathbb{E}') \circ \rho \subset \mathcal{O}(\mathbb{E}) \otimes \mathbb{Q} \cong \mathcal{B}_{p,\infty} ,$$

⁸ e.g. if $j(E) \neq 0, 1728$ and $M \neq -\text{Id}$

then $I_{\widehat{\rho}, \mathbb{E}} = \overline{I_{\rho, \mathbb{E}}}$. Under the same identification, if $\tau: \mathbb{E}' \rightarrow \mathbb{E}''$ is another non-zero morphism, then $I_{\tau \circ \rho, \mathbb{E}''} = I_{\rho, \mathbb{E}'} \cdot I_{\tau, \mathbb{E}''}$.

Proof. Local principality is invariant if we replace $I_{\rho, \mathbb{E}'}$ with an equivalent ideal. In particular, using (15) we can change ρ to another element of $\text{Hom}(\mathbb{E}, \mathbb{E}')$ and, using Corollary 10, suppose that $\deg(\rho)$ is coprime to N . In particular if ℓ divides $\deg \rho$, then it does not divide the index $[\text{End}(E) : \mathcal{O}(\mathbb{E})]$, nor $[\text{Hom}(E, E') : \text{Hom}(\mathbb{E}, \mathbb{E}')]$, hence $\mathcal{O}(\mathbb{E}) \otimes \mathbb{Z}_\ell$ is equal to the maximal order $\text{End}(E) \otimes \mathbb{Z}_\ell$ and

$$I_{\rho, \mathbb{E}'} \otimes \mathbb{Z}_\ell = \left(\widehat{\text{Hom}(\mathbb{E}, \mathbb{E}')} \circ \rho \right) \otimes \mathbb{Z}_\ell = \left(\widehat{\text{Hom}(E, E')} \circ \rho \right) \otimes \mathbb{Z}_\ell \quad (16)$$

which is principal since it is the local version of the ideal $\widehat{\text{Hom}(E, E')} \circ \rho$ given by the classical Deuring correspondence. For the primes ℓ that do not divide $\deg \rho$, by the last part of Corollary 10 we can choose an element α of $\text{Hom}(\mathbb{E}, \mathbb{E}')$ of degree coprime to ℓ , so that $\hat{\alpha}\rho \in I_{\rho, \mathbb{E}'}$ also has degree prime to ℓ , implying that $I_{\rho, \mathbb{E}'} \otimes \mathbb{Z}_\ell = \mathcal{O}(\mathbb{E}) \otimes \mathbb{Z}_\ell$, which is principal.

By definition $\mathfrak{n}(I_{\rho, \mathbb{E}'})$ is the gcd of $\deg(\rho) \deg(\alpha)$ for all α in $\text{Hom}(\mathbb{E}, \mathbb{E}')$, which is equal to $\deg(\rho)$ by Corollary 10, Item 3.

To compute the index of $I_{\rho, \mathbb{E}'}$ we can change the ideal to an equivalent one using (15) and suppose that $\deg \rho$ is coprime to N (to see how the index changes, recall that for $\alpha \in \mathcal{O}(\mathbb{E})$, multiplication by α has determinant $\deg(\alpha)^2$, hence αI has index $\deg(\alpha)^2$ inside I). Then by the same arguments used to prove local principality we see that all the primes ℓ not dividing $\deg \rho$ do not divide the index $[\mathcal{O}(\mathbb{E}) : I_{\rho, \mathbb{E}'}]$, while the primes ℓ dividing $\deg \rho$ divide the index with the right multiplicity, by (16) and the classical case.

The characterization of $I_{\widehat{\rho}}$ is a direct application of Definition 12, using that taking the dual in $\text{End}(E)$ corresponds to conjugation in $\mathcal{B}_{p, \infty} \cong \text{End}(\mathbb{E}) \otimes \mathbb{Q}$. For the last statement, the inclusion $I_{\rho, \mathbb{E}'} \cdot I_{\tau, \mathbb{E}''} \subset I_{\tau \circ \rho, \mathbb{E}''}$ can be checked directly, and then it is enough to prove that both sides have the same index in $\text{End}(\mathbb{E})$. This is true since $I_{\rho, \mathbb{E}'}, I_{\tau, \mathbb{E}''}$ are locally principal, hence arguing locally, in our situation the index is multiplicative. $\square$

A useful consequence of Theorem 13 is that, when $\rho: \mathbb{E} \rightarrow \mathbb{E}'$ is an isogeny of degree coprime to the level N , then we have

$$I_{\rho, \mathbb{E}'} = I_\rho \cap \mathcal{O}(\mathbb{E}) , \quad (17)$$

where I_ρ is the ideal associated to ρ without considering level structures, as in Eq. (1). Indeed one has $I_{\rho, \mathbb{E}} \subset I_\rho \cap \mathcal{O}(\mathbb{E}')$ by definition. To get the equality we compare indices: the index $[\mathcal{O}(E) : \mathcal{O}(\mathbb{E})] = [\mathbf{M}_2(\mathbb{Z}/N) : \langle \Gamma \rangle]$ is a divisor of N^4 , hence it is coprime to $\deg \rho$ and in particular by Theorem 13 both sides in (17) have index $[\mathbf{M}_2(\mathbb{Z}/N) : \langle \Gamma \rangle] \cdot \deg \rho$ in $\mathcal{O}(E)$.

In the following theorem we state the other direction of the Deuring correspondence, i.e. from ideals to elliptic curves with level structure. We give the proof in Appendix C.1, since the statement is not needed in our applications.

Theorem 14. *Let $p, N, \Gamma, \mathbb{E}, \mathbb{E}'$ be as in Corollary 10. Then each locally-principal ideal of $\mathcal{O}(\mathbb{E})$ is of the form $I_{\rho', \mathbb{E}'}$ for some $\mathbb{E}'$ and ρ' .*

Moreover, if we suppose that Γ is additively stable, then two ideals $I_{\rho', \mathbb{E}'}, I_{\rho'', \mathbb{E}''}$ are equivalent if and only if $\mathbb{E}', \mathbb{E}''$ are isomorphic.

Curves side	Quaternion side	Reference
$\varphi : \mathbb{E} \rightarrow \mathbb{E}'$	left locally-principal ideal $I_{\varphi, \mathbb{E}'}$ of $\mathcal{O}(\mathbb{E})$	Theorems 13, 14
$\varphi : \mathbb{E} \rightarrow \mathbb{E}', \psi : \mathbb{E} \rightarrow \mathbb{E}'$	Equivalent ideals $I_{\varphi, \mathbb{E}'} \sim I_{\psi, \mathbb{E}'}$	Eq. (15)
$\mathbb{E}'$ supersingular elliptic curves with level structure up to isomorphism	$\text{Cl}(\mathcal{O}(\mathbb{E})) = \{\text{locally principal ideal}\}/\text{equivalence}$	Theorem 14
$\theta \in \mathcal{O}(\mathbb{E})$, up to units on the left	Principal ideal $\mathcal{O}(\mathbb{E}) \cdot \theta$	Definition 12
$\widehat{\varphi}$	$\overline{I_{\varphi}}$	Theorem 13
$\deg \varphi$	$\mathfrak{n}(I_{\varphi, \mathbb{E}'})$	Theorem 13
$\tau \circ \rho : \mathbb{E} \rightarrow \mathbb{E}' \rightarrow \mathbb{E}''$	$I_{\tau \circ \rho} = I_{\rho} \cdot I_{\tau}$	Theorem 13
Supersingular j -invariants $j(E)$ in $\mathbb{F}_{p^2}$ up to Galois conjugacy	Maximal orders in $B_{p, \infty}$ $\mathcal{O} \cong \text{End}(E)$ up to isomorphism	

Table 1. Generalization of the Deuring correspondence (see [26]) for supersingular elliptic curves with additively stable Γ -structure. The last line, in grey, is stated without level structures since it does not fully generalize

3.4 $\mathcal{O}(E, S)$ for concrete choices of level structures

We describe the rings of endomorphisms $\mathcal{O}(E, S)$ and their properties for Borel, scalar and split Cartan level structures. A summary is given in Table 2. Let $\mathcal{O}_E = \text{End}(E)$ be the endomorphism ring of the supersingular elliptic curve E .

Borel Level Structures. Thanks to [4] we know that for Borel level structures the set $\mathcal{O}(E, S)$ is an Eichler order in the quaternion algebra $\mathcal{B}_{p, \infty}$. As proven in [25], if I_S is the ideal associated to the isogeny with kernel given by S , then $\mathcal{O}(E, S) = \mathbb{Z} + I_S$. For Borel level structures, if $N > 2$, $\langle \Gamma \rangle$ is equal to the set of upper triangular matrices, hence $[M_2(\mathbb{Z}/N) : \langle \Gamma \rangle] = N$ and the covolume of $\text{Hom}((E, S), (E', S'))$ is $\frac{1}{4}pN$.

Scalar level structures. Given E, S with $S \ni (P_S, Q_S)$ we have $\mathcal{O}(E, S) = \mathbb{Z} + N\mathcal{O}_E$, where $\mathcal{O}_E$ is the endomorphism ring of the curve E . In fact, whenever $\alpha \in \mathcal{O}(E, S)$ we have that $\alpha(P_S) = \lambda P_S$ and $\alpha(Q_S) = \lambda Q_S$ for some $\lambda \in \mathbb{Z}/N$, that implies that $\alpha - [\lambda]$ maps both P_S, Q_S to 0_E , so $\alpha - [\lambda] \in N\mathcal{O}_E$. We used that for scalar structures $\langle \Gamma \rangle$ is the set of all scalar matrices. In particular $[M_2(\mathbb{Z}/N) : \langle \Gamma \rangle] = N^3$ and the covolume of $\text{Hom}((E, S), (E', S'))$ is $\frac{1}{4}pN^3$.

Split Cartan level structures. Let $S = \Gamma \cdot (P_S, Q_S)$ be a split Cartan structure on E and suppose $N > 2$ (otherwise split Cartan is the same as scalar). Then, for any choice of an endomorphism $\gamma \in \mathcal{O}_E$ such that⁹ $\gamma(P_S) = \lambda P_S$ and $\gamma(Q_S) = \mu Q_S$ with $\lambda \neq \mu$ in $(\mathbb{Z}/N)^*$, we have $\mathcal{O}(E, S) = \mathbb{Z}[\gamma] + N\mathcal{O}_E$. Indeed $M_\gamma = \begin{bmatrix} \lambda & 0 \\ 0 & \mu \end{bmatrix}$, hence $\mathbb{Z}/N[M_\gamma]$ is equal to $\langle \Gamma \rangle = \{\begin{bmatrix} * & 0 \\ 0 & * \end{bmatrix}\}$. In particular we have $[M_2(\mathbb{Z}/N) : \langle \Gamma \rangle] = N^2$ and the covolume of $\text{Hom}((E, S), (E', S'))$ is $\frac{1}{4}pN^2$.

Level Structure	Trivial	Borel	Split Cartan	Scalar
Γ	$\text{GL}_2(\mathbb{Z}/N)$	$\begin{bmatrix} * & * \\ 0 & * \end{bmatrix}$	$\begin{bmatrix} * & 0 \\ 0 & * \end{bmatrix}$	$\begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix}$
$\mathcal{O}(E, S)$	$\mathcal{O}_E$	$\mathbb{Z} + I_S$	$\mathbb{Z}[\gamma] + N\mathcal{O}_E$	$\mathbb{Z} + N\mathcal{O}_E$
Covolume	$\frac{p}{4}$	$\frac{p}{4} \cdot N$	$\frac{p}{4} \cdot N^2$	$\frac{p}{4} \cdot N^3$

Table 2. Structure and covolume of the order $\mathcal{O}(E, S)$ for different level structures.

4 SQInstructor's identification protocols

We now describe a paradigm for creating SQIsign-like interactive identification protocols. The general idea is simple and resembles the description of SQIsign we gave in Section 2, however it has several moving pieces and instantiations may differ a lot. In the next sections we will take a closer look at two instantiations: one using KLPT and 1-dimensional isogenies, the other using 2-dimensional isogenies.

Regardless of the details, the security of all instantiations is comparable to that of SQIsign. We analyze in this section soundness, which is proven similarly for all instantiations, while we defer zero-knowledge of each variant to the respective section.

4.1 The Protocol

As usual, we choose a prime p and a supersingular elliptic curve $E_0/\mathbb{F}_{p^2}$ of known endomorphism ring. In practice we may take $p \equiv 3 \pmod{4}$ and $E_0 : y^2 = x^3 + x$. Additionally we fix a level N coprime to p and an additively stable subgroup Γ of $\text{GL}_2(\mathbb{Z}/N)$.

The protocol being a sigma-protocol, we describe its phases one by one.

Key generation. Like in SQIsign, the secret key is a left ideal $I_{\text{sk}} \subset \mathcal{O}(E_0)$, corresponding to an isogeny $\varphi_{\text{sk}} : E_0 \rightarrow E_{\text{pk}}$. Then an arbitrary Γ -structure S_{pk} is chosen on E_{pk} . The public key is $\mathbb{E}_{\text{pk}} := (E_{\text{pk}}, S_{\text{pk}})$.

The exact way in which I_{sk} is sampled is not crucial, as long as recovering it from E_{pk} is hard. Using modern techniques [1] it can be taken uniformly at

⁹ In other words we want $\gamma|_{E[N]}$ to diagonalize in basis (P_S, Q_S) .

random among the ideals of a fixed prime degree $> p^2$, ensuring E_{pk} is statistically close to being uniformly distributed. For convenience, we assume $n(I_{\text{sk}})$ is coprime to N .

Depending on the instantiation, S_{pk} may be chosen at key generation time, or it may be deterministically computed from E_{pk} using a public algorithm and thus take no space in the public key.

Commitment is similar to key generation: a secret ideal I_{com} is sampled and the associated isogeny $\varphi_{\text{com}} : E_0 \rightarrow E_{\text{com}}$ evaluated. The curve E_{com} is sent to the verifier as commitment. The same sampling algorithm used for I_{sk} may be used here, in particular we assume $n(I_{\text{com}})$ is coprime to N .

Challenge. The verifier picks a uniformly random Γ -structure S_{com} on E_{com} and sends it to the prover. Let $\mathbb{E}_{\text{com}} = (E_{\text{com}}, S_{\text{com}})$.

The response is an isogeny $\varphi_{\text{rsp}} \in \text{Hom}(\mathbb{E}_{\text{pk}}, \mathbb{E}_{\text{com}})$ such that $\varphi_{\text{rsp}}(S_{\text{pk}}) = S_{\text{com}}$.

This is where we encounter the biggest variability: we may opt to sample responses of smooth degree, so that they can be encoded as chains of 1-dimensional isogenies like in earlier versions of SQIsign [16], or we may let them have arbitrary degree and encode them as higher-dimensional isogeny chains [1]. The latter choice leads to more performant implementations, on par with the version of SQIsign currently submitted to NIST, as we will show in Section 6. But the former is still of interest as it offers the only known way to instantiate advanced primitives such as ring signatures [14] or chameleon hashes [9]. We analyze this alternative in Section 5.

Irrespective of this choice, the first step is to compute $\text{Hom}(\mathbb{E}_{\text{pk}}, \mathbb{E}_{\text{com}})$. We will detail this step in Section 4.3.

Verification. The verifier checks that φ_{rsp} is indeed a valid isogeny $E_{\text{pk}} \rightarrow E_{\text{com}}$ and that $\varphi_{\text{rsp}}(S_{\text{pk}}) = S_{\text{com}}$. The protocol is summarized in Figure 4.

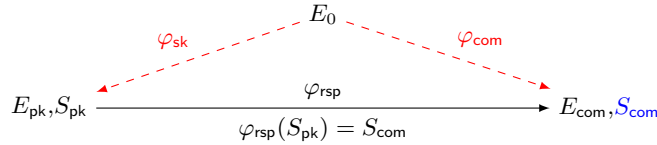


Fig. 4. SQInstructor identification protocol. Secrets dashed in red. Challenge in blue.

4.2 Encoding and sampling level structures

The group Γ being a fixed parameter, a level structure S can simply be encoded by taking an arbitrary representative basis (P_S, Q_S) . A random level structure

is then drawn by sampling a random basis of $E[N]$. Some level structures have more compact representations: for example a Borel level structure is equivalent to a cyclic group of order N , it may thus be encoded by a single point.

If (P, Q) is some basis of $E[N]$ known to both prover and verifier, for example because it is computed deterministically from E using a public algorithm, such as [1, Algorithm 2.1], then an alternative is to represent (P_S, Q_S) by the matrix $M_S \in \text{GL}_2(\mathbb{Z}/N)$ such that $(P_S, Q_S) = M_S \cdot (P, Q)$. While transmitting (P_S, Q_S) requires $4 \log(q)$ bits for a suitable $q = p^r$, the matrix M_S only takes $4 \log(N)$ bits, which is less since $N^2 = O(q)$ by Hasse inequality and, later, by our choice of parameters. Because we are free to act by Γ , we may even reduce M_S to some standard form requiring only $\approx 4 \log(N) - \log(|\Gamma|)$ bits. Sampling a random level structure is then equivalent to sampling a random element in $\Gamma \backslash \text{GL}_2(\mathbb{Z}/N)$.

4.3 Computing $\text{Hom}(\mathbb{E}_{\text{pk}}, \mathbb{E}_{\text{com}})$

The first step in computing the response is computing the module $\text{Hom}(\mathbb{E}_{\text{pk}}, \mathbb{E}_{\text{com}})$. Thanks to Theorem 13, this is isomorphic to an ideal $I_{\rho, \mathbb{E}_{\text{com}}} \subset \mathcal{O}(\mathbb{E}_{\text{pk}})$ for some $\rho : \mathbb{E}_{\text{pk}} \rightarrow \mathbb{E}_{\text{com}}$. We already know an isogeny $\varphi_{\text{com}} \circ \widehat{\varphi}_{\text{sk}} : E_{\text{pk}} \rightarrow E_{\text{com}}$, we may thus use Algorithm [InStructIdeal](#) to find $I_{\rho, \mathbb{E}_{\text{com}}}$.

Algorithm 2 [ResponseIdeal](#)

Input: Curves $E_0, E_{\text{pk}}, E_{\text{com}}$, with N -torsion bases $(P_0, Q_0), (P_{\text{pk}}, Q_{\text{pk}}), (P_{\text{com}}, Q_{\text{com}})$;
Input: A basis $\langle \omega_1, \dots, \omega_4 \rangle$ of $\mathcal{O}(E_0)$ and the matrices $M_{\omega_1}, \dots, M_{\omega_4}$ wrt (P_0, Q_0) ;
Input: Ideals I_{sk} and I_{com} of norm coprime to N s.t. $E_{\text{pk}} = I_{\text{sk}} \star E_0$ and $E_{\text{com}} = I_{\text{com}} \star E_0$;
Output: Ideal $I_{\rho} \subset \mathcal{O}(E_{\text{pk}})$ such that $\rho(P_{\text{pk}}) = P_{\text{com}}$ and $\rho(Q_{\text{pk}}) = Q_{\text{com}}$.
1: Let M_{sk} be the matrix of I_{sk} in (P_0, Q_0) and $(P_{\text{pk}}, Q_{\text{pk}})$;
2: Let M_{com} be the matrix of I_{com} in (P_0, Q_0) and $(P_{\text{com}}, Q_{\text{com}})$;
3: Let $\langle \beta_1, \dots, \beta_4 \rangle$ be a basis of the right order of I_{sk} ;
4: **for** $1 \leq i \leq 4$ **do**
5: $\alpha_i \leftarrow \varphi_{\text{sk}} \beta_i \widehat{\varphi}_{\text{sk}} / \deg \varphi_{\text{sk}}$,
6: $M_{\alpha_i} \leftarrow M_{\text{sk}}^{-1} (c_1 M_{\omega_1} + \dots + c_4 M_{\omega_4}) M_{\text{sk}}$, where $\beta_i = c_1 \omega_1 + \dots + c_4 \omega_4$;
7: $I_{\zeta} \leftarrow \overline{I_{\text{sk}}} \cdot I_{\text{com}}$;
8: $M_{\zeta} \leftarrow \deg \varphi_{\text{sk}} \cdot M_{\text{sk}}^{-1} \cdot M_{\text{com}}$;
9: **return** $I_{\rho} \leftarrow \text{InStructIdeal}((E_{\text{pk}}, E_{\text{com}}), (\alpha_i)_i, (M_{\alpha_i})_i, I_{\zeta}, M_{\zeta})$.

With the notation above, and letting $(P_{\text{pk}}, Q_{\text{pk}})$ and $(P_{\text{com}}, Q_{\text{com}})$ be arbitrary representatives of S_{pk} and S_{com} , the procedure is summarized in Algorithm 2. To understand why it produces the desired output, observe that $\mathcal{O}(E_{\text{pk}})$ is identified to the right order of I_{sk} via

$$\iota_{\text{pk}} : \mathcal{O}(E_{\text{pk}}) \rightarrow \mathcal{O}(E_0) \otimes \mathbb{Q} \\ \alpha \mapsto \frac{1}{\deg \varphi_{\text{sk}}} \widehat{\varphi}_{\text{sk}} \alpha \varphi_{\text{sk}}.$$

Thus if $\beta_i = \iota_{\text{pk}}(\alpha_i)$, then Lines 5–6 recover α_i and its matrix M_{α_i} in the basis $(P_{\text{pk}}, Q_{\text{pk}})$. Note that M_{sk} and the denominators of the c_i 's are invertible modulo N thanks to the assumption $\gcd(N, \deg \varphi_{\text{sk}}) = 1$.

Then, at Lines 7–8, I_ζ is the ideal corresponding to $\varphi_{\text{com}} \circ \widehat{\varphi_{\text{sk}}}$ and M_ζ its associated matrix in $(P_{\text{pk}}, Q_{\text{pk}})$ and $(P_{\text{com}}, Q_{\text{com}})$. Hence `InStructIdeal` returns an ideal $I_\rho \sim I_\zeta$ mapping $(P_{\text{pk}}, Q_{\text{pk}})$ to $(P_{\text{com}}, Q_{\text{com}})$ (and thus S_{pk} to S_{com}).

Finally, to represent $\text{Hom}(\mathbb{E}_{\text{pk}}, \mathbb{E}_{\text{com}})$, we first compute $\mathcal{O}(\mathbb{E}_{\text{pk}})$ using Table 2, and then we obtain $I_{\rho, \mathbb{E}_{\text{com}}} = I_\rho \cap \mathcal{O}(\mathbb{E}_{\text{pk}})$ thanks to Eq. (17).

Pay attention to the fact that the isogeny ρ associated to I_ρ is not the φ_{rsp} we are looking for, but only one in the same $\text{Hom}(\mathbb{E}_{\text{pk}}, \mathbb{E}_{\text{com}})$. Indeed, having been computed by linear algebra, we cannot argue that ρ hides $\widehat{\varphi_{\text{sk}}} \circ \varphi_{\text{com}}$, nor do we control its degree. Picking a suitable equivalent ideal to $I_{\rho, \mathbb{E}_{\text{com}}}$ is the topic of Sections 5 and 6.

Remark 15. In the discussion above it was crucial that we could compute M_{com} with respect to (P_0, Q_0) and $(P_{\text{com}}, Q_{\text{com}})$ (and similarly for M_{sk}). When discrete logarithms modulo N can be efficiently computed, this can be done simply by evaluating φ_{com} on (P_0, Q_0) and then computing the discrete logarithm of $(\varphi_{\text{com}}(P_0), \varphi_{\text{com}}(Q_0))$ in base (a representative of) S_{com} .

When discrete logarithms cannot be computed, our options are more limited. A workaround is for the prover to compute $(\varphi_{\text{com}}(P_0), \varphi_{\text{com}}(Q_0))$, mask it as

$$(P'_{\text{com}}, Q'_{\text{com}}) := M \cdot (\varphi_{\text{com}}(P_0), \varphi_{\text{com}}(Q_0))$$

via a random change of basis M , and commit to $E_{\text{com}}, (P'_{\text{com}}, Q'_{\text{com}})$. Then the challenge S_{com} can be submitted as a matrix $M' \in \Gamma \setminus \text{GL}_2(\mathbb{Z}/N)$, so that $S_{\text{com}} = M' \cdot (P'_{\text{com}}, Q'_{\text{com}})$, and the prover is able to compute M_{com} . This slightly increases the protocol's bandwidth, since the curve needs to be sent together with a basis of its N -torsion, but has a negligible impact on performance.

4.4 Security

We conclude this section with an analysis of the security of the identification protocol, insofar as the arguments apply to any instantiation.

Special soundness is proven analogously to SQIsign: we prove that two responses with distinct challenges for the same commitment compose to a non-scalar endomorphism. Actually, we can prove the endomorphism provides a witness for the stronger relation

$$\mathcal{R}_{\Gamma\text{-OneEnd}} := \{(\mathbb{E}, \omega) \mid \omega \in \text{End}(E) \setminus \mathcal{O}(\mathbb{E})\}, \quad (18)$$

for $\mathbb{E}$ a supersingular elliptic curve with Γ -level structure. Since we assume Γ contains the scalar matrices, ω is not a scalar endomorphism. So, by [40], $\mathcal{R}_{\Gamma\text{-OneEnd}}$ is a hard relation equivalent to the endomorphism ring problem.

Theorem 16. *The protocol in Section 4.1 is 2-special sound for $\mathcal{R}_{\Gamma\text{-OneEnd}}$. The knowledge error is*

$$\varepsilon = [\text{GL}_2(\mathbb{Z}/N) : \Gamma]^{-1}. \quad (19)$$

If an adversary breaks soundness with probability w and expected running time r for a uniform public key E_{pk} , then there is an algorithm computing a witness for $\mathcal{R}_{\Gamma\text{-OneEnd}}$ with expected running time $O(r/(w - \varepsilon))$.

Proof. Consider two valid transcripts $(E_{\text{com}}, S_{\text{com}}, \varphi_{\text{rsp}})$ and $(E_{\text{com}}, S'_{\text{com}}, \varphi'_{\text{rsp}})$ with $S_{\text{com}} \neq S'_{\text{com}}$. By definition $\varphi_{\text{rsp}}(S_{\text{pk}}) = S_{\text{com}}$ and $\varphi'_{\text{rsp}}(S_{\text{pk}}) = S'_{\text{com}}$. Let $\beta = \widehat{\varphi_{\text{rsp}}} \circ \varphi'_{\text{rsp}}$ and assume $\beta \in \mathcal{O}(\mathbb{E}_{\text{pk}})$, then

$$S_{\text{pk}} = \beta(S_{\text{pk}}) = \widehat{\varphi_{\text{rsp}}} \circ \varphi'_{\text{rsp}}(S_{\text{pk}}) = \widehat{\varphi_{\text{rsp}}}(S'_{\text{com}}) .$$

Since Γ is additively stable, it is closed under scalar multiplication, thus by Item 2 from Corollary 10 we have $\varphi_{\text{rsp}}(S_{\text{pk}}) = S'_{\text{com}} \neq S_{\text{com}}$, a contradiction. So β is a witness for $\mathcal{R}_{\Gamma\text{-OneEnd}}(E_{\text{pk}})$. We conclude that the protocol is 2-special sound. To compute the knowledge error we just need to count the number of cosets of Γ in $\text{GL}_2(\mathbb{Z}/N)$, that is the index $[\text{GL}_2(\mathbb{Z}/N) : \Gamma] = \#\text{GL}_2(\mathbb{Z}/N)/\#\Gamma$.

The second part of the theorem follows by standard techniques, see for example [21, Theorem 1 and Definition 2]. $\square$

Zero Knowledge. To prove zero-knowledge we would need to exhibit a simulator that on input E_{pk} produces a random isogeny $\varphi'_{\text{rsp}} : E_{\text{pk}} \rightarrow E'_{\text{com}}$ and computes $S'_{\text{com}} := \varphi'_{\text{rsp}}(S_{\text{pk}})$, so that $(E'_{\text{com}}, S'_{\text{com}}, \varphi'_{\text{rsp}})$ is distributed identically to a valid transcript.

However the existence of such a simulator depends on how the response is computed. Like in SQIsign, if we use a KLPT-style algorithm to compute a 1-dimensional response, then the distribution of φ_{rsp} is very poorly understood, and the only thing we can do is argue computational zero-knowledge. We briefly discuss this in Section 5.2.

If instead we use a higher-dimensional method to produce the response, we are faced with the obstacle that no polynomial time algorithm is known to compute a large arbitrary degree isogeny from E_{pk} without knowing its endomorphism ring. The workaround used in SQIsign is to prove security in a model where the simulator has access to an oracle producing such isogenies [1], or at least where it is provided non-interactively with a polynomially sized *hint* string [2]. We adapt these proof techniques to SQInstructor in Section 6.3 and appendix D.

Whatever the case is, if we take Zero-Knowledge for granted, then we can apply the Fiat-Shamir transform to the protocol to obtain a signature scheme as secure as SQIsign: its EUF-CMA security reduces to the hardness of $\mathcal{R}_{\Gamma\text{-OneEnd}}$, and thus to Problem 3 via [40].

Parameter sizes The best classical attacks against Problem 3 having complexity $\tilde{O}(\sqrt{p})$, the bit-size of p should be taken to be twice the security parameter λ . The primes defined in SQIsign v1 [16] or v2 [1] are valid choices for a 1-dimensional or a higher-dimensional implementation, respectively.

The level N may then be taken according to the available torsion in $E_0(\mathbb{F}_{p^2})$, i.e., according to the prime factors of $p \pm 1$. For a 1-dimensional implementation this may be a product of some mid-sized factors of $p^2 - 1$, or a power of a small prime not dividing the degree of the response. For a higher-dimensional implementation it appears to be most efficient to take a power of 2.

Finally the size of N will be determined by the size of the challenge space: which we just saw it is $[\text{GL}_2(\mathbb{Z}/N) : \Gamma]$. We want this quantity to be $\approx 2^\lambda$. Recall

that $\#\mathrm{GL}_2(\mathbb{Z}/N) = N^4 \prod_{p|N} (1 - \frac{1}{p^2})(1 - \frac{1}{p})$, and that $\#\Gamma = N\phi(N)^2$, $\phi(N)^2$, $\phi(N)$ for Borel, split-Cartan and scalar level structures respectively. Thus we need $\log(N) \approx \lambda, \frac{\lambda}{2}, \frac{\lambda}{3}$ respectively.

5 KLPT for level structures

We now come to the problem of finding an element of $\mathrm{Hom}(\mathbb{E}, \mathbb{E}')$ of smooth norm. Here we focus solely on extending to the SQInstructor framework the KLPT algorithm [32], which computes a connecting ideal of smooth norm given $\mathcal{O}(E)$ and $\mathcal{O}(E')$. Then, standard techniques [16] let us translate this ideal into a 1-dimensional isogeny, to be used, e.g., as response φ_{rsp} in the identification protocol.

These algorithms lead to larger degree isogenies and less efficient implementations than what is achievable through higher-dimensional techniques, but, unlike those, produce outputs that can be efficiently simulated (under an *ad hoc* computational assumption). This feature makes 1-dimensional techniques unavoidable in the context of advanced protocols such as ring signatures [14] and chameleon hashes [9].

Notation. We call integral ideals of $\mathcal{B}_{p,\infty}$ ideals for short. For I a fractional ideal, $\mathcal{O}_L(I)$ is its left order and $\mathcal{O}_R(I)$ its right one. Two ideals I, J are compatible if $\mathcal{O}_L(J) = \mathcal{O}_R(I)$. For compatible ideals I, J , the pullback of J through I is $[I]^*J = IJ + \mathfrak{n}(J)\mathcal{O}_L(I)$. For I, J left ideals of a maximal order $\mathcal{O}$, the push-forward of J through I is $[I]_*J = \frac{1}{\mathfrak{n}(I)}\bar{I}(I \cap J)$. Similar to [25, Section 2.4], $\mathcal{O}_0 = \mathcal{O}(E_0)$ is a special maximal order.

Solving norm equations with level structure. In the following, we are given a left $\mathcal{O}(\mathbb{E})$ -ideal Λ defined as in Eq. (14), and we want to compute an equivalent ideal of smooth norm. Recall that, in quaternion terms, Λ is the intersection of an $\mathcal{O}(E)$ -ideal with the suborder $\mathcal{O}(\mathbb{E})$, as summarized in Table 2. Thus, for $\mathcal{O}$ a maximal order and $\mathcal{O}_N$ a suborder associated to a level structure, we say that an $\mathcal{O}$ -ideal J is *equivalent in $\mathcal{O}_N$* or *is equivalent respecting the level structure associated to $\mathcal{O}_N$* to an input $\mathcal{O}$ -ideal I if J is such that $J = I \frac{\bar{\alpha}}{\mathfrak{n}(I)}$ with α in $I \cap \mathcal{O}_N$. This also implies that $J \cap \mathcal{O}_N$ and $I \cap \mathcal{O}_N$ are equivalent $\mathcal{O}_N$ -ideals. We therefore need to solve norm equations *with level structure* or *in $\mathcal{O}_N$* , which means finding an ideal equivalent to the input in $\mathcal{O}_N$ and of smooth norm.

Prior work. The papers on 1-dimensional SQIsign [25, 26] propose the algorithms **GenericKLPT** and **SigningKLPT**, which transform a quaternion ideal of a maximal order into an equivalent ideal of smooth or even power-of-two norm. The difference between the two algorithms is that **SigningKLPT** outputs an ideal following a distribution which is assumed to be computationally indistinguishable from uniformly random ideals of the same norm and equivalence class. **GenericKLPT** is a simpler version than **SigningKLPT**, which leaves out some rerandomization

procedures to focus solely on smooth-norm ideals in the correct equivalence class. It is therefore suitable to first adapt **GenericKLPT**, then the rerandomization.

In his PhD thesis [33], Leroux analyses these KLPT versions and creates more variants. **GenericKLPT** consists in some equivalence-taking to get prime norm inputs, a pullback to $\mathcal{O}_0$ of the input ideal, and an algorithm for resolution in a special order $\mathcal{O}_0$. This last algorithm is called **IdealEichlerNorm** [33, Algorithm 10] and solves (in $\mathcal{O}_0$) a norm equation in the intersection of an ideal I and an Eichler suborder $\mathbb{Z} + I_c$, where I_c is a primitive ideal of a maximal order. While Leroux often assumes I_c to be of prime norm, he insists this is not a requirement, but a low number of distinct prime factors is better for performance. Leroux also describes a similar algorithm solving (in $\mathcal{O}_0$) a norm equation in the intersection of an ideal I and a suborder $\mathbb{Z} + NI_c$ for some integer N , called **IdealSuborderEichlerNorm** [33, Algorithm 14]. A copy of the pseudocode for both of these algorithms is given in Appendix A. In the remainder of this section, we use this **IdealSuborderEichlerNorm** and an input treatment derived from **SigningKLPT** to create an algorithm for smooth-norm equivalence with level structure.

Plan of the section. We focus on the scalar level structure because solving this case allows us to solve the problem also for other level structures (see Section 5.3). For simplicity, we restrict the discussion here to input ideals I such that $\mathfrak{n}(I)$ is a square modulo N . An explanation of this choice and a generalization to the non-square case can be found in Appendix B.

In the following, we show how **IdealSuborderEichlerNorm** [33, Algorithm 14] can be used to solve norm equations associated to scalar level structures. Then, we adapt the initialization steps of **GenericKLPT** to the scalar case, and evaluate the output length of our KLPT variant. Next, we show how to adapt the rerandomization step of **SigningKLPT** to take equivalences respecting a level structure. Pseudocode for the resulting **ScalarSigningKLPT** algorithm can be found in Algorithm 3. Finally, we explain how to solve the non-scalar case, including a more efficient implementation for the Borel case using **IdealEichlerNorm**. We also present our proof-of-concept implementation. For the sake of conciseness we refer to Appendix C.2 for the proofs of the lemmas and propositions stated in this section.

5.1 The use of **IdealSuborderEichlerNorm** in **ScalarSigningKLPT**

We search a β in $A = I \cap (\mathbb{Z} + N\mathcal{O})$ of the correct norm, then return $J = I \frac{\bar{\beta}}{\mathfrak{n}(I)}$. However, all KLPT-related algorithms solve norm equations only in special orders like $\mathcal{O}_0$ or suborders of those. Following prior work such as [25], we therefore search for β in the intersection $I \cap (\mathbb{Z} + N\mathcal{O}) \cap \mathcal{O}_0$.

Let us show that **IdealSuborderEichlerNorm** can be applied to this problem. Denote I_c a primitive ideal connecting $\mathcal{O}_0$ to $\mathcal{O}$. Then the Eichler order $\mathcal{O} \cap \mathcal{O}_0$ equals $\mathbb{Z} + I_c$. Thanks to Lemma 17, this means that we search in I intersected with $\mathbb{Z} + NI_c$. Furthermore, since $\mathbb{Z} + NI_c$ is an order is contained in $\mathbb{Z} + I_c$, the intersection of $\mathbb{Z} + NI_c$ with I is equal to its intersection with the pullback

$[I_c]^*I$. Since $[I_c]^*I$ is a left $\mathcal{O}_0$ -ideal, searching in its intersection with $\mathbb{Z} + NI_c$ is exactly the problem solved by [IdealSuborderEichlerNorm](#).

Lemma 17. *For I a primitive right ideal of a maximal order $\mathcal{O}$ in $\mathcal{B}_{p,\infty}$. Then $(\mathbb{Z} + I) \cap (\mathbb{Z} + N\mathcal{O}) = (\mathbb{Z} + NI)$ for $N \in \mathbb{Z}$ coprime to $\mathfrak{n}(I)$.*

Creating inputs to [IdealSuborderEichlerNorm](#) We now show how to transform the input ideal I (left ideal of a maximal order $\mathcal{O}$) into a suitable input for [IdealSuborderEichlerNorm](#). We leave the rerandomization step to Section 5.2. To ensure efficiency, we need to transform the connecting ideal I_c from $\mathcal{O}$ to $\mathcal{O}_0$ so that it is of prime norm. Also, the input ideal I must be pulled back to $\mathcal{O}_0$ through the transformed I_c (so that we work at $\mathcal{O}_0$) and replaced by a prime-norm equivalent (again for efficiency). Finally, none of these steps should change the equivalence class of I in the order $\mathbb{Z} + N\mathcal{O}$.

For the connecting ideal I_c , we use [EquivalentPrimeIdeal](#) (as in [25]) to find an equivalent $I'_c = I_c \frac{\alpha_c}{\mathfrak{n}(I_c)}$ of prime norm N_c . Conjugating I and $\mathcal{O}$ with $\frac{\bar{\alpha}_c}{\mathfrak{n}(I_c)}$ is an isomorphism, and therefore does not modify any problem input.

Then, since N_c is a large prime, I is (with overwhelming probability) of norm coprime to N_c and can be pulled back through I'_c . This results in a left $\mathcal{O}_0$ -ideal I_1 of norm equal to $\mathfrak{n}(I)$. To get a prime-norm equivalent without modifying its equivalence class with respect to $\mathbb{Z} + N\mathcal{O}_0$, one uses an element δ in $I_1 \cap (\mathbb{Z} + N\mathcal{O}_0)$ with $\frac{\mathfrak{n}(\delta)}{\mathfrak{n}(I_1)}$ prime. Therefore $I_0 = I_1 \frac{\delta}{\mathfrak{n}(I_1)}$ is a prime-norm input ideal which is in the same class with respect to $\mathbb{Z} + N\mathcal{O}_0$ as I is with respect to $\mathbb{Z} + N\mathcal{O}$, as explained in the preceding paragraph. This results in Algorithm 3. We set the input exponent e according to the following proposition (proven in Appendix C.2).

Proposition 18. *There is a variant of [ScalarSigningKLPT](#) which produces output for $\ell^e > p^{9/2}N^{10}\epsilon$ with ϵ polylogarithmic in (pN) , under plausible assumptions.*

Algorithm 3 [ScalarSigningKLPT](#) $_{\ell^e}(I, N)$

Input: N prime or power of prime of known factorization, I left ideal of a maximal order $\mathcal{O}$ in $\mathcal{B}_{p,\infty}$ such that $\mathfrak{n}(I) \bmod N$ is a square, ℓ small prime and $e \in \mathbb{Z}$ even such that ℓ^e large enough (See Proposition 18).

Output: $J \sim I$ such that $J = \chi_I(\beta)$ with $\beta \in (\mathbb{Z} + N\mathcal{O}) \cap I$ and $\mathfrak{n}(J) \mid \ell^e$

- 1: $\alpha, I'_c \leftarrow \text{EquivalentPrimeIdeal}(I_c)$; $I_1 \leftarrow \frac{1}{\alpha}I\alpha$; // $I'_c = \chi_{I_c}(\alpha)$
 - 2: $\alpha_I, I_2 \leftarrow \text{InitialRerandomization}(I_1, \mathbb{Z} + N(\frac{1}{\alpha}I\alpha), I'_c)$ // See Section 5.2
 - 3: Let $\delta \in [I'_c]^*I_2 \cap (\mathbb{Z} + N\mathcal{O}_0)$ random s.t. $I_0 = \chi_{[I'_c]^*I_2}(\delta)$ is of prime norm N
 - 4: $\beta \leftarrow \text{IdealSuborderEichlerNorm}_{\ell^e}(N, I'_c, I_0)$
 - 5: $J_0 \leftarrow \chi_{I_0}(\beta)$ and $J_a \leftarrow [I'_c]^*J_0$ and $J \leftarrow \alpha J_a \frac{1}{\alpha}$
 - 6: **return** J
-

5.2 Rerandomization to improve the output distribution

The difference between [GenericKLPT](#) and [SigningKLPT](#) is that the latter ensures that restricting the search space from I to $I \cap (\mathbb{Z} + I_c)$ does not bias the output [25,33]. This is done by replacing the input ideal I — before computing the pullback through I_c — by an equivalent ideal which is in a uniformly random equivalence class when taking equivalences in $(\mathbb{Z} + I_c)$ [33, Lemma 5.3.1]. In the following, the set of ideal classes for a (non necessarily maximal) quaternion order $\mathcal{O}$ is denoted $\text{Cl}(\mathcal{O})$, as in [33, Section 2.3].

For rerandomization in [ScalarSigningKLPT](#), we adapt [33, Algorithm 34], but we need to prove that the equivalence for I is taken in the order $\mathcal{O}_N$ translating the level structure constraint. This means in $\mathbb{Z} + N\mathcal{O}$ for the scalar case. As shown in Lemma 19, it is possible to modify the rerandomization in [SQIsign](#) so that the equivalence is taken in $I \cap \mathcal{O}_N$ as done in Algorithm 4. With this choice of equivalence, [33, Proposition 2.3.12] applies, so that the class in $\text{Cl}(\mathcal{O}_0 \cap \mathcal{O})$ of the output of this rerandomization only depends on the class of I in $\text{Cl}(\mathcal{O}_N)$. More details on this can be found in Appendix C.3.

Lemma 19. *For I a left ideal of a maximal order $\mathcal{O}$ and $N, N_c, \mathfrak{n}(I)$ coprime, there exist $\omega \in \mathbb{Z} + N\mathcal{O}$ such that N_c is inert in $\mathbb{Z}[\omega]$ and $\gamma \in I \cap \mathbb{Z} + N\mathcal{O}$ such that γ is not in $N_c\mathcal{O}_R(I)$.*

Algorithm 4 [InitialRerandomization](#)($I, \mathcal{O}_N, I_c$)

Input: I ideal of a maximal order $\mathcal{O}$ in $B_{p,\infty}$, $\mathcal{O}_N$ suborder of $\mathcal{O} = \mathcal{O}_L(I)$ of level N and superorder of $\mathbb{Z} + N\mathcal{O}$, N prime or power of prime of known factorization

Output: $I' \sim I$ such that $I' = \chi_I(\beta)$ with $\beta \in \mathcal{O}_N \cap I$ and the class of I' uniformly random in $\text{Cl}(\mathbb{Z} + I_c)$

- 1: Get $\omega \in \mathcal{O}_N$ s.t. N_c is inert in $\mathbb{Z}[\omega]$;
 - 2: Get $\gamma \in I \cap \mathcal{O}_N$ s.t. γ is not in $N_c\mathcal{O}_R(I)$; // We assume N_c coprime to $N\mathfrak{n}(I)$ as N_c is a large prime
 - 3: Let $D \leftarrow_{\$} [0, N_c]$, let $C \leftarrow 1$; **if** $D = N$ **then** $C, D \leftarrow 0, 1$;
 - 4: Let $\beta \leftarrow (C + D\omega)\gamma$;
 - 5: **return** $\beta, \chi_I(\beta)$;
-

Output distribution. As for [SQIsign](#) [25,26], the above arguments should not be taken as a proof that the output distribution is indistinguishable from random ideals of required norm and equivalence class, but better proofs are not common for 1-dimensional [SQIsign](#) variants. [SQIsign](#)'s authors mostly assume that the output distribution of [IdealEichlerNorm](#) is computationally indistinguishable from random ideals satisfying the same constraints as its output¹⁰. Despite these similarities, the arguments on the distribution of outputs of [SigningKLPT](#) do not

¹⁰ A small bias was noticed in [26], and fixed with small changes to two subroutines, [IdealSuborderEichlerNorm](#) already has these changes.

immediately generalize to Algorithm 3. This is because the algorithms [IdealSuborderEichlerNorm](#) and [IdealEichlerNorm](#) are despite all similarities distinct, so the security of 1-dimensional SQInstructor relies again on an *ad hoc* assumption on the output distribution of [ScalarSigningKLPT](#). We claim however that this new assumption is just as plausible as the assumption that [SigningKLPT](#) is undistinguishable from uniformly random isogenies.

5.3 Adapting from the scalar to other level structures

The above [ScalarSigningKLPT](#) can be adapted to a norm equation solving algorithm with other level structures, as long as the corresponding orders contain $\mathbb{Z} + N\mathcal{O}$. Let I the input ideal, a left ideal of a maximal order $\mathcal{O}$ in $B_{p,\infty}$, and $\mathcal{O}_N$ order translating the level structure constraint, with $\mathbb{Z} + N\mathcal{O} \subset \mathcal{O}_N \subset \mathcal{O}$. One must take special care so that the rerandomized ideal has square norm modulo N (see Appendix B). Then the only modification compared to [ScalarSigningKLPT](#) is that [InitialRerandomization](#) is called with the order $\mathcal{O}_N$ instead of $\mathbb{Z} + N\mathcal{O}$. This works because all later steps in [ScalarSigningKLPT](#) take an ideal in the same class of $\text{Cl}(\mathbb{Z} + N\mathcal{O})$ as the output of the rerandomization. Since $\mathcal{O}_N$ contains $\mathbb{Z} + N\mathcal{O}$, ideals which are equivalent for $\mathbb{Z} + N\mathcal{O}$ are also equivalent for $\mathcal{O}_N$. The output distribution of this adaptation only depends on the class of the I in $\text{Cl}(\mathcal{O}_N)$, again by [33, Lemma 2.3.12], and depends on the one of [IdealSuborderEichlerNorm](#) just as for [ScalarSigningKLPT](#). The required output size is the same as for [ScalarSigningKLPT](#) at the same level N , given by Proposition 18.

More efficient variant for Borel level structure. For Borel level structures, there is an even more efficient approach, which allows shorter output sizes. This [BorelSigningKLPT](#) consists in exactly the same rerandomization (again with $\mathcal{O}_N = \mathbb{Z} + I_N$, and no constraints on the quadratic residuosity of the output norm) and input preparation, except that I_0 is just taken equal to $[I_c]^* I_1$, since [IdealEichlerNorm](#) as stated in [33, Algorithm 10] does not require a prime-norm input. Then, the call to [IdealSuborderEichlerNorm](#) is replaced by a call to [IdealEichlerNorm](#) with inputs $I'_c I'_N, I_0$, where I'_N is I_N conjugated by $\frac{\bar{\alpha}_c}{n(I_c)}$ (so the product is compatible). The correctness of this algorithm can be seen from Lemma 20, which clarifies that searching an element in $\mathbb{Z} + I'_N \cap \mathbb{Z} + I'_c$ is the same as searching it in $\mathbb{Z} + I'_c I'_N$, which is the problem [IdealEichlerNorm](#) solves.

Lemma 20. *For I, J two primitive compatible ideals of $B_{p,\infty}$ (that is $\mathcal{O}_R(I) = \mathcal{O}_L(J)$) of coprime norms, $(\mathbb{Z} + I) \cap (\mathbb{Z} + J) = (\mathbb{Z} + IJ)$.*

[BorelSigningKLPT](#) has a shorter output size and its output distribution is more directly linked to [SigningKLPT](#). The output size is due to [IdealEichlerNorm](#) which produces outputs of size $p^3(NN_c)^3$ if the Eichler order $\mathbb{Z} + I'_c I_N$ is used. The output distribution is similar to the one of [SigningKLPT](#) since [IdealEichlerNorm](#) is used in both. The only difference between these distributions is that rerandomization in [BorelSigningKLPT](#) is only done up to equivalence with respect to $(\mathbb{Z} + I'_N)$.

Proposition 21. *There is a variant of **BorelSigningKLPT** which produces output for $\ell^e > p^{9/2}N^3\epsilon$ with ϵ polylogarithmic in (pN) , under plausible assumptions.*

Proof-of-concept implementation. We implemented the KLPT variants for scalar and the optimized version for Borel level structures¹¹ based on the LearningToSQI [20] SageMath [43] implementation of SQIsign. It is a proof-of-concept implementation and has severe limitations. In particular, it is quite slow. In addition, we did not implement the rerandomization from Algorithm 4 for Borel level structures, which means the output distribution is biased in that case. Finally, we only support N to be a power of an odd prime, and ℓ to be 2, and the special order to be $\mathcal{O}_0$ (this means that the implementation does not adjust the order in case of larger lattice minima, but fails instead).

Instantiation of SQInstructor with 1-dimensional isogenies Thanks to the previous algorithms we can finally instantiate the SQInstructor signature scheme using a 1-dimensional representation of the response isogeny. For efficiency, we use a Borel level structure. First, we need a prime p so that ideals of norm ℓ^e can be translated to isogenies efficiently and the N -torsion is accessible¹² for some prime (or prime-power) N of bitsize λ . Therefore we consider $\ell = 2$ and $p = f2^e - 1$ such that $p - 1$ has a prime factor N roughly of size λ . For translating ideals of norm a power of ℓ we can then use the algorithms from [34, Appendix A] or those from [38].¹³ A simple search targeting NIST I security gives $p = 369 \cdot 2^{252} - 1$, where $p - 1$ has a factor N of size 126 bits. With these choices, using **BorelSigningKLPT** we obtain a response isogeny of degree 2^e for $e = 9/2 \log(p) + 3 \log(N) + \log(\log(pN)) \approx 1920$. This gives a public key size of 186 bytes, composed by E_{pk}, P_{pk}, Q_{pk} ¹⁴ and a signature size of 300 bytes, composed by $\gamma \in \Gamma$, M_{ch} (compressed to $2 \log(N)$ bits) and φ_{rsp} (compressed to e bits using techniques from [25,19]).

6 A state-of-the-art SQInstructor signature

In this section we instantiate the SQInstructor signature protocol using the same state-of-the-art techniques in [1], in particular 2-dimensional isogeny representations. We carefully analyze the Zero-Knowledge property of the identification scheme and prove EUF-CMA of the signature scheme. Finally, we implement our signature by forking the reference SQIsign implementation available at

¹¹ github.com/SQInstructors/SQInstructor

¹² that means the N -torsion is defined over $\mathbb{F}_{p^4}$

¹³ Both of these algorithms rely on higher dimensional isogenies to avoid requirements on the smoothness of $p + 1$, but they are meant to be used only in the signing phase, without modification of the 1-dimensional verification procedure. They don't affect the simulatability of the transcripts.

¹⁴ we can define the points over the twist to have the represented by $\mathbb{F}_{p^2}$ coefficients

<https://github.com/SQISign/the-sqisign> and benchmark it, demonstrating comparable performance.¹⁵

6.1 The protocol in detail

Parameters. We take a prime $p = f2^e - 1$ such that f is a small odd cofactor, and a starting curve $E_0 : y^2 = x^3 + x / \mathbb{F}_{p^2}$. Any of the primes specified in [1] works. We take the level to be $N = 2^{e_{\text{tor}}}$ for some $e_{\text{tor}} \leq e$, owing to the fact that $E_0[2^e]$ is $\mathbb{F}_{p^2}$ -rational. To simplify the exposition we focus on Z -level structures, where $Z = \{ \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix} \mid \lambda \text{ odd} \} \subset \text{GL}_2(\mathbb{Z}/N)$ is the subgroup of scalar matrices, thus, following the analysis of Section 4.4, we take $e_{\text{tor}} \approx \frac{\lambda}{3} \approx \frac{e}{6}$.

Representing level structures. For compactness, we represent level structures on a curve E as matrices in $\text{GL}_2(\mathbb{Z}/N)/Z$, with respect to a fixed public basis (P_E, Q_E) of $E[N]$. Such bases can be computed using [1, Algorithms 2.1-3] and then multiplying by $2^{e-e_{\text{tor}}}$.

Letting $\mathcal{O}_0$ be the maximal order with basis $(1, i, (i+j)/2, (1+k)/2)$, isomorphic to $\mathcal{O}(E_0)$ via $i \mapsto \iota$ and $j \mapsto \pi$, we precompute the matrices $(M_0^{(1)}, \dots, M_0^{(4)})$ of the action of the order's basis on (P_{E_0}, Q_{E_0}) as described in Remark 6.

Key Generation and commitment are similar to SQISign [1, Algorithm 4.1]: we generate secret ideals $I_{\text{sk}}, I_{\text{com}} \subset \mathcal{O}_0$ of prime norm $\approx p^2$ and we evaluate the corresponding isogenies $\varphi_{\text{sk}}, \varphi_{\text{com}}$ to obtain the public key / commitment curves $E_{\text{pk}}, E_{\text{com}}$. The level structure S_{pk} is then simply $Z \cdot (P_{\text{pk}}, Q_{\text{pk}})$, with $(P_{\text{pk}}, Q_{\text{pk}}) = (P_{E_{\text{pk}}}, Q_{E_{\text{pk}}})$ the fixed level structure associated to E_{pk} . Additionally we compute and store the action matrices $M_{\text{sk}}, M'_{\text{com}}$ associated to $\varphi_{\text{sk}}, \varphi_{\text{com}}$ with respect to (P_{E_0}, Q_{E_0}) , $(P_{\text{pk}}, Q_{\text{pk}})$ and $(P'_{\text{com}}, Q'_{\text{com}}) = (P_{E_{\text{com}}}, Q_{E_{\text{com}}})$.

The challenge is expressed as a matrix $M_{\text{ch}} \in \text{GL}_2(\mathbb{Z}/N)/Z$ with respect to the public basis $(P'_{\text{com}}, Q'_{\text{com}})$, i.e.

$$S_{\text{com}} = Z \cdot (P_{\text{com}}, Q_{\text{com}}) := Z M_{\text{ch}} \cdot (P'_{\text{com}}, Q'_{\text{com}}) . \quad (20)$$

In the non-interactive signature, M_{ch} is computed as $H(j(E_{\text{pk}}), j(E_{\text{com}}), \text{msg})$, where $H : \mathbb{F}_{p^2} \times \mathbb{F}_{p^2} \times \{0, 1\}^* \rightarrow \text{GL}_2(\mathbb{Z}/N)/Z$ is a preimage-resistant hash function.

The response is then computed follows. We start by calling Algorithm [Response-Ideal](#) on I_{sk} and I_{com} to obtain an ideal $I_{\rho} \subset \mathcal{O}(E_{\text{pk}})$ such that $\rho(P_{\text{pk}}) = P_{\text{com}}$ and $\rho(Q_{\text{pk}}) = Q_{\text{com}}$. Note that $M_{\text{com}} = M'_{\text{com}} M_{\text{ch}}^{-1}$ at Line 2.

Then, writing $\mathbb{E}_{\text{pk}} = (E_{\text{pk}}, S_{\text{pk}})$ and $\mathbb{E}_{\text{com}} = (E_{\text{com}}, S_{\text{com}})$, we let $I_{\rho, \mathbb{E}_{\text{com}}} = I_{\rho} \cap \mathcal{O}(\mathbb{E}_{\text{pk}})$. Next, we randomize $I_{\rho, \mathbb{E}_{\text{com}}}$ by taking a random equivalent $\mathcal{O}(\mathbb{E}_{\text{pk}})$ -ideal of bounded norm. For this, we take a uniformly random $\alpha \in I_{\rho, \mathbb{E}_{\text{com}}}$ of

¹⁵ To gain even more performance, we could use the recent technique Qlapoti [13], which applies equally well to SQISign and SQInstructor. We refrain from doing so to make the comparison with SQISign's reference code simpler.

odd norm $n(\alpha) < B_{\text{rsp}} \cdot n(I_{\rho, \mathbb{E}_{\text{com}}})$. An algorithm to sample α is described in [1, Algorithm 3.7]. If no such α is found, we restart the signing procedure by sampling a new commitment. The parameter B_{rsp} and the restart probability will be discussed in Section 6.2.

Then, we set $I_\alpha := \chi_{I_\rho}(\alpha)$ (see Eq. (6)) and we compute a response isogeny φ_{rsp} such that $I_{\varphi_{\text{rsp}}} = I_\alpha$. By Eq. (7), the matrix $M_{\varphi_{\text{rsp}}}$ wrt $(P_{\text{pk}}, Q_{\text{pk}})$ and $(P_{\text{com}}, Q_{\text{com}})$ is $\frac{1}{\deg \rho} M_\alpha^\dagger = \gamma \text{Id}$, where $\gamma = \frac{1}{n(I_\rho)} \cdot \frac{\text{tr}(\alpha)}{2}$. Finally we construct a 2-dimensional isogeny representation of φ_{rsp} , like in [1, Section 4.4.3]. For this, we construct an auxiliary isogeny $\varphi_{\text{aux}} : E_{\text{com}} \rightarrow E_{\text{aux}}$ such that $\deg(\varphi_{\text{rsp}}) + \deg(\varphi_{\text{aux}}) = 2^a < 2^e$ and we construct the Kani diamond on φ_{rsp} and φ_{aux} , as in Figure 5, defining a $(2^a, 2^a)$ -isogeny $\Phi : E_{\text{pk}} \times E_{\text{aux}} \rightarrow E_{\text{com}} \times E'_{\text{aux}}$.

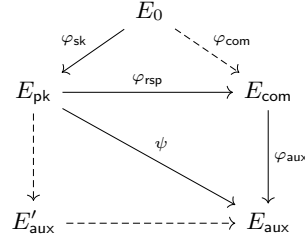


Fig. 5. Protocol diagram for the HD version of the protocol.

The signature then contains the following data:

- The degree $\deg(\varphi_{\text{rsp}})$ of the response,
- The auxiliary curve E_{aux} ,
- The kernel of the $(2^a, 2^a)$ -isogeny Φ , encoded with respect to public bases of $E_{\text{pk}}[2^e]$ and $E_{\text{aux}}[2^e]$,
- The challenge matrix M_{ch} ,
- Optionally: the scalar $\gamma = \frac{\text{tr}(\alpha)}{2n(I_\rho)}$.

Verification recomputes the $(2^a, 2^a)$ -isogeny Φ from its kernel and evaluates it to recover E_{com} and φ_{rsp} , checks that $M_{\text{ch}} = \text{H}(j(E_{\text{pk}}), j(E_{\text{com}}), \text{msg})$ and that

$$\varphi_{\text{rsp}} \begin{pmatrix} P_{E_{\text{pk}}} \\ Q_{E_{\text{pk}}} \end{pmatrix} = \gamma M_{\text{ch}} \begin{pmatrix} P_{E_{\text{com}}} \\ Q_{E_{\text{com}}} \end{pmatrix}.$$

If γ is not included in the signature, the verifier can recompute it via a generalized discrete-logarithm.

6.2 Lattice shapes and response degree

The response computation described above may fail and restart the signature when no $\alpha \in I_{\rho, \mathbb{E}_{\text{com}}}$ of odd norm $n(\alpha) < B_{\text{rsp}} \cdot n(I_{\rho, \mathbb{E}_{\text{com}}})$ is found. Though

we set this failure probability to be so low as to be practically irrelevant, it is not practically negligible and it thus affects the distribution of responses and consequently the Zero-Knowledge property. We note that SQIsign also has failure cases that force it to restart, as analyzed in [1,13], and those failure cases also affect SQInstructor, however this failure event is specific to the design described here, thus we analyze it exclusively.

Because $I_{\rho, \mathbb{E}_{\text{com}}}$ is isometric to $\text{Hom}(\mathbb{E}_{\text{pk}}, \mathbb{E}_{\text{com}})$ up to a multiplicative factor $\deg \rho$, the probability of failing to find α is the same as the probability of failing to find an isogeny of odd degree $< B_{\text{rsp}}$ in $\text{Hom}(\mathbb{E}_{\text{pk}}, \mathbb{E}_{\text{com}})$. Let $(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ be the Minkowski-reduced basis of $\text{Hom}(\mathbb{E}_{\text{pk}}, \mathbb{E}_{\text{com}})$ and $(\lambda_1, \lambda_2, \lambda_3, \lambda_4)$ be the norms of the α_i 's, i.e. the squares of the successive minima¹⁶. It is not possible that all the minima are even, otherwise all the elements of the lattice would be even, contradicting Lemma 5. Thus, the probability of not finding an odd norm vector in the intersection with the ball of radius B_{rsp} is lower-bounded by $\Pr(\lambda_4 > B_{\text{rsp}})$. We estimate this probability via a quantitative analysis of the distribution of the minima, for which we provide experiments¹⁷. We also refer to [1, Section 9.3.2] for a similar analysis. Recall that:

1. **InStructIdeal** returns a left $\mathcal{O}$ -ideal I_ρ where $\mathcal{O} = \mathcal{O}(E_{\text{pk}})$.
2. $I_{\rho, \mathbb{E}_{\text{com}}} = I_\rho \cap (\mathbb{Z} + N\mathcal{O})$.
3. $\mathcal{O}$ is statistically close to the uniform distribution over the set of maximal orders of $B_{p, \infty}$ (Table 1), by the choice of $\deg(\varphi_{\text{sk}})$.
4. if C is $\text{Cov}(\text{Hom}(\mathbb{E}_{\text{pk}}, \mathbb{E}_{\text{com}})) = [M_2(\mathbb{Z}/N) : \langle \Gamma \rangle] \cdot \frac{1}{4}p$, for scalar level structures $C = \frac{p}{4}N^3$, then by Minkowski's second theorem we have
$$\frac{1}{55}C^2 \leq \frac{2^4}{9\pi^4}C^2 \leq \prod_{i=1}^4 \lambda_i < \frac{2^{10}}{\pi^4}C^2 < 11C^2.$$

In our experiments, we observe an inverse linear correlation between the first and the last minima, that means we can approximate $\lambda_1 \lambda_4 \approx k_1 C$ for a constant k_1 . Our experiments suggest $k_1 \approx 0.314$. We thus focus on the cumulative distribution of λ_1 , i.e. $\Pr(\lambda_1 \leq x)$, that is the probability that the shortest vector of $\text{Hom}(\mathbb{E}, \mathbb{E}')$ has norm at most x .

Following the same estimates as in [1], we know that there are $\psi(x) = x \prod_{l|x} (1 + \frac{1}{l})$ primitive left $\mathcal{O}(\mathbb{E})$ -ideals (i.e. cyclic isogenies mapping curves with level structure) of norm x , that means that the number of primitive ideals of odd norm at most x is $\sum_{2r+1 \leq x} \psi(2r+1)$, which asymptotically lies between $\frac{1}{4}x^2$ and x^2 . To count also minimal isogenies $\varphi: \mathbb{E}_{\text{pk}} \rightarrow \mathbb{E}'$ of even degree, (here minimal just means that it is not a multiple of another isogeny $\mathbb{E}_{\text{com}} \rightarrow \mathbb{E}'$) we notice that such maps, since they map scalar structures to multiples of scalar structures, at the level of elliptic curves (without level structures) are of the form $\varphi = 2^\delta \varphi'$ with $\delta \leq e_{\text{tor}}$ and φ' a cyclic, odd-degree isogeny. Moreover if we choose φ' , then E' is determined and the level structure is determined up to $2^{3\delta}$ choices (or $\frac{3}{4}2^{3\delta}$ if $\delta = e_{\text{tor}}$). Then, fixing $\deg \varphi = 2^{2\delta} \deg \varphi' = 2^{3\delta}(2r+1)$, then the number of such ϕ is (up to a small constant in the case $\delta = e_{\text{tor}}$) $2^{3\delta} \psi(2r+1)$. Summing over possible δ and $2r+1$ such that $4^\delta(2r+1) \leq x$, we see that the possible

¹⁶ recall that we are using the norm specified in Eq. (13)

¹⁷ github.com/SQInstructors/SQInstructor

minimal isogenies $\mathbb{E}_{\text{com}} \rightarrow \mathbb{E}'$ of degree at most x is equal to αx^2 for some α bounded from below by $\frac{1}{4}$ and also bounded from above by some constant (in particular $\alpha \leq 2$ if x/N^2 is large enough).

The total number of ideal classes, or equivalently the number of possible choices for $\mathbb{E}' = \mathbb{E}_{\text{com}}$ up to isomorphism, is approximately $\frac{p}{12}N^3 = \frac{C}{3}$ for scalar level structures. Thus, if all ideal classes are equally likely and it never happens that two ideals of norm at most x are in the same class, for $x \gg N^2$ we have

$$\Pr(\lambda_1 \leq x) = k_2 \left(\frac{\sqrt{C}}{x} \right)^2, \text{ for } k_2 \in \left[\frac{3}{2}, 6 \right]. \quad (21)$$

Thus, combining the last estimate with our correlation hypothesis, we have that

$$\Pr(\lambda_4 > x) = \Pr\left(\lambda_1 \leq \frac{k_1 C}{x}\right) \approx k_3 \left(\frac{\sqrt{C}}{x} \right)^2 \text{ for } k_3 = k_1^2 k_2. \quad (22)$$

Our experiments corroborate this estimate, for $k_3 \approx 0.553794$. Thus, we can conclude that via fixing $B_{\text{rsp}} = \kappa\sqrt{C} = \kappa\sqrt{p}N^{3/2}$ we can bound the restart probability by $\frac{k_3}{\kappa^2}$. Thus, we have three possible strategies. The aggressive one is to fix κ to a small $O(1)$ constant, having a restart probability of $O(1)$, getting a more efficient signature. The conservative one is to fix $\kappa = \sqrt[4]{p}$, getting a negligible restart probability in λ . The intermediate one is to aim to a restart probability of 2^{-64} , in line with [1] and NIST's recommendations that the adversary has access to no more than 2^{64} signing queries [37], thus we fix $\kappa = 2^{32}$, implying

$$B_{\text{rsp}} = 2^{32}\sqrt{p}N^{3/2}, \quad (23)$$

that implies, recalling the definition of N , that $\log(B_{\text{rsp}}) = 32 + \frac{1}{2}(\log(p) + \lambda)$.

6.3 EUF-CMA Security

We are finally ready to discuss the EUF-CMA security of our SQInstructor signature. From now we denote by $\Sigma_{\text{SQInstructor}}$ the identification protocol from Section 4.1. As noted repeatedly, see [22,8,1,6], we cannot sample efficient representations of large degree isogenies without relying on the knowledge of the endomorphism ring of the starting curve. This means that the straightforward simulator for the SQIsign protocol described above cannot be instantiated in polynomial time.

To overcome this problem in [22], and following works on SQIsign variants [8,27], the authors introduced the notion of *isogeny oracles*: oracles that on input a supersingular elliptic curve and some parameters, return an efficient representation of a large degree isogeny from the curve following a given distribution.

Remark 22. In a follow-up the authors of [2] provide a different security proof for the SQIsign signature scheme, avoiding the use of isogeny oracles, but instead

introduce the notion of *hint-assisted* zero knowledge, where the simulator is given hints sampled from an isogeny distribution. A similar proof can be adapted to our protocol, but is very technical and would take all our available space. We focus here on the more intuitive, yet rigorous proof based on oracles, and give the hint-assisted proof in Appendix D for completeness.

As for [8], we consider two variants of the oracle:

Definition 23. A Γ -uniform target oracle (Γ -UTO) for $\Gamma \leq \text{GL}_2(\mathbb{Z}/N)$ is an oracle taking as input a supersingular elliptic curve with Γ -level structure $\mathbb{E}$ defined over $\mathbb{F}_{p^2}$ and an integer B_{rsp} and outputs a random isogeny $\phi : \mathbb{E} \rightarrow \mathbb{E}'$ (in efficient representation) such that:

1. $\mathbb{E}'$ is distributed sampled from the uniform distribution on the set of supersingular elliptic curves over $\mathbb{F}_{p^2}$ with level structure so that there exists an odd-norm isogeny in $\text{Hom}(\mathbb{E}, \mathbb{E}')$ of degree $\leq B_{\text{rsp}}$;
2. The conditional distribution of ϕ given $\mathbb{E}'$ is uniform over isogenies $\phi : \mathbb{E} \rightarrow \mathbb{E}'$ of odd degree $\leq B_{\text{rsp}}$

Definition 24 (Definition 23 [8]). A fixed degree isogeny oracle (FIDIO) is an oracle taking as input a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$ and an integer N , and outputs a uniformly random isogeny $\phi : E \rightarrow E'$ (in efficient representation) with domain E and degree N .

Using these oracles, we can enunciate and prove the following theorem:

Theorem 25. The $\Sigma_{\text{SQInstructor}}$ identification protocol is statistically non-aborting honest-verifier zero-knowledge in the Γ -UTO and FIDIO model. In other words, there exists a polynomial time simulator Sim with access to a Γ -UTO and a FIDIO that produces random transcripts which are statistically indistinguishable from honest non-aborting transcripts.

Proof. Let E_{pk} be a random supersingular elliptic curve over $\mathbb{F}_{p^2}$ and $P_{\text{pk}}, Q_{\text{pk}}$ be a random basis of the N -torsion. We consider the following simulator Sim that using the Γ -UTO and FIDIO returns a transcript $(\text{com}, \text{ch}, \text{rsp})$:

1. Sim sets $S_{\text{pk}} \leftarrow Z \cdot \begin{pmatrix} P_{\text{pk}} \\ Q_{\text{pk}} \end{pmatrix}$, then calls the Γ -UTO with input $(E_{\text{pk}}, S_{\text{pk}})$ and B_{rsp} to get the isogeny $\varphi_{\text{rsp}} : (E_{\text{pk}}, S_{\text{pk}}) \rightarrow (E_{\text{com}}, S_{\text{com}})$;
2. Sim computes the matrix $M_{\text{ch}} \leftarrow \text{GL}_2(\mathbb{Z}/N)/Z$ such that $S_{\text{com}} = ZM \cdot (P_{E_{\text{com}}}, Q_{E_{\text{com}}})$ and sets $\text{ch} := M_{\text{ch}}$;
3. Sim sets $\text{com} := (j(E_{\text{com}}))$;
4. Let $d = \deg(\varphi_{\text{rsp}})$, $a = \lceil \log(d) \rceil$, Sim calls the FIDIO with input $E_{\text{com}}, 2^a - d$ to get $\varphi_{\text{aux}} : E_{\text{com}} \rightarrow E_{\text{aux}}$;
5. Let $\psi = \varphi_{\text{aux}} \circ \varphi_{\text{rsp}}$, Sim sets $(P_{\text{aux}}, Q_{\text{aux}}) = ([d^{-1}] \psi(P_{\text{pk}}), [d^{-1}] \psi(Q_{\text{pk}}))$;
6. Sim sets $\text{rsp} := (a, E_{\text{aux}}, P_{\text{aux}}, Q_{\text{aux}})$;

It is clear from the definition of the oracles and the steps that the response consists of a valid isogeny representation distributed as in the honest transcript that can be used to re-compute $\varphi_{\text{rsp}} : E_{\text{pk}} \rightarrow E_{\text{com}}$. Finally, note that the Γ -UTO

only returns isogenies for curves with level structure that admit odd degree isogenies from the input curve with level structure, that is the same condition required for the honest transcript to not restart. $\square$

Since the commitment set, i.e. the set of supersingular elliptic curves with torsion points, is a superset of SQIsign commitment set – just supersingular elliptic curves – the min-entropy of the commitment in SQInstructor is also negligible in the security parameter by [2, Lemma 4.1]. This, in combination with from Theorem 25, Theorem 16, immediately implies the EUF-CMA security of SQInstructor in the $\mathcal{F}$ -UTO, FIDIO and random oracle models. More precisely: if the signature restarting probability is negligible in the security parameter this is an immediate implication of [3, Lemma 3.5]. If not, assuming that the signing procedure is repeated enough times to ensure negligible failure probability, the EUF-CMA security follows from [11, Theorem 1].

6.4 Implementation and benchmarks

We implemented the protocol described in this section by forking SQIsign’s reference implementation. The bound B_{rsp} was set according to the “intermediate” choice of Eq. (23). We compare the performances of SQInstructor and SQIsign in Table 3. We observe very similar performances across the board, with a slight increase in signature size and verification time, both attributable to the longer $(2, 2)$ -isogeny chain in SQInstructor. We remark that both SQInstructor and SQIsign’s signatures could be slightly compressed, however we deem this optimization minor.

Scheme	Security	(Mcycles)		Verify	(bytes)	
		KeyGen	Sign		pk	sig
SQInstructor	NIST I	33.5	78.9	6.0	65	174
	NIST III	102.9	240.1	20.8	97	272
	NIST V	166.2	420.2	39.0	129	355
SQIsign	NIST I	32.1	76.8	4.3	65	148
	NIST III	101.3	237.7	14.4	97	224
	NIST V	166.9	398.6	27.7	129	292

Table 3. Comparison between SQInstructor and SQIsign. Timings are the median of 100 runs on a laptop CPU AMD Ryzen 7000.

References

1. Aardal, M.A., Adj, G., Aranha, D.F., Basso, A., Canales Martínez, I.A., Chávez-Saab, J., Santos, M.C., Dartois, P., De Feo, L., Duparc, M., Eriksen, J.K., Fouotsa, T.B., Filho, D.L.G., 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 (2024), available at <https://csrc.nist.gov/Projects/pqc-dig-sig/round-2-additional-signatures>
2. Aardal, M.A., Basso, A., De Feo, L., Patranabis, S., Wesolowski, B.: A complete security proof of SQIsign. In: Kalai, Y.T., Kamara, S.F. (eds.) CRYPTO 2025, Part VI. LNCS, vol. 16005, pp. 190–222. Springer, Cham (Aug 2025). https://doi.org/10.1007/978-3-032-01887-8_7
 3. 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, Berlin, Heidelberg (Apr / May 2002). https://doi.org/10.1007/3-540-46035-7_28
 4. Arpin, S.: Adding level structure to supersingular elliptic curve isogeny graphs. Journal de théorie des nombres de Bordeaux (2022), <https://api.semanticscholar.org/CorpusID:247292410>
 5. Arpin, S., Castryck, W., Eriksen, J.K., Lorenzon, G., Vercauteren, F.: Generalized class group actions on oriented elliptic curves with level structure. In: International Workshop on the Arithmetic of Finite Fields. pp. 171–190. Springer (2024)
 6. 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.) PKC 2025, Part III. LNCS, vol. 15676, pp. 300–332. Springer, Cham (May 2025). https://doi.org/10.1007/978-3-031-91826-1_10
 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, Cham (Apr 2023). https://doi.org/10.1007/978-3-031-30617-4_14
 8. Basso, A., Dartois, P., De Feo, L., Leroux, A., Maino, L., Pope, G., Robert, D., Wesolowski, B.: SQIsign2D-West - the fast, the small, and the safer. In: Chung, K.M., Sasaki, Y. (eds.) ASIACRYPT 2024, Part III. LNCS, vol. 15486, pp. 339–370. Springer, Singapore (Dec 2024). https://doi.org/10.1007/978-981-96-0891-1_11
 9. Basso, A., De Feo, L., Patranabis, S., Radulescu, I., Wesolowski, B.: Forensic categories: a framework for SQIsign-like primitives. Private communication (2026)
 10. Basso, A., Maino, L., Pope, G.: FESTA: Fast encryption from supersingular torsion attacks. In: Guo, J., Steinfeld, R. (eds.) ASIACRYPT 2023, Part VII. LNCS, vol. 14444, pp. 98–126. Springer, Singapore (Dec 2023). https://doi.org/10.1007/978-981-99-8739-9_4
 11. Bert, P., Roux-Langlois, A.: From identification using rejection sampling to signatures via the Fiat-Shamir transform: Application to the BLISS signature. In: Inomata, A., Yasuda, K. (eds.) IWSEC 18. LNCS, vol. 11049, pp. 297–312. Springer, Cham (Sep 2018). https://doi.org/10.1007/978-3-319-97916-8_19
 12. Boneh, D., Shoup, V.: A graduate course in applied cryptography. Draft 0.5 p. 14 (2020)
 13. Borin, G., Corte-Real Santos, M., Eriksen, J., Invernizzi, R., Mula, M., Schaeffler, S., Vercauteren, F.: Qlapoti: Simple and efficient translation of quaternion ideals to isogenies. In: Hanaoka, G., Yang, B. (eds.) Advances in Cryptology -

- ASIACRYPT 2025 - 31st International Conference on the Theory and Application of Cryptology and Information Security, Melbourne, VIC, Australia, December 8–12, 2025, Proceedings, Part IV. Lecture Notes in Computer Science, vol. 16248, pp. 174–205. Springer (2025). https://doi.org/10.1007/978-981-95-5113-2_6, https://doi.org/10.1007/978-981-95-5113-2_6
14. Borin, G., Lai, Y.F., Leroux, A.: Erebor and durian: Full anonymous ring signatures from quaternions and isogenies. *CiC* 1(4), 4 (2024). <https://doi.org/10.62056/ava3zivvrzn>
 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, Cham (Apr 2023). https://doi.org/10.1007/978-3-031-30589-4_15
 16. Chavez-Saab, J., Santos, M.C., De Feo, L., Eriksen, J.K., Hess, B., Kohel, D., Leroux, A., Longa, P., Meyer, M., Panny, L., Patranabis, S., Petit, C., Rodríguez Henríquez, F., Schaeffler, S., Wesolowski, B.: SQIsign. Tech. rep., National Institute of Standards and Technology (2023), available at <https://csrc.nist.gov/Projects/pqc-dig-sig/round-1-additional-signatures>
 17. 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. In: Guo, J., Steinfeld, R. (eds.) ASIACRYPT 2023, Part III. LNCS, vol. 14440, pp. 99–130. Springer, Singapore (Dec 2023). https://doi.org/10.1007/978-981-99-8727-6_4
 18. Codogni, G., Lido, G.: Spectral theory of isogeny graphs (2025), <https://arxiv.org/abs/2308.13913>
 19. Corte-Real Santos, M., Eriksen, J.K., Meyer, M., Reijnders, K.: AprèsSQI: Extra fast verification for SQIsign using extension-field signing. In: Joye, M., Leander, G. (eds.) EUROCRYPT 2024, Part I. LNCS, vol. 14651, pp. 63–93. Springer, Cham (May 2024). https://doi.org/10.1007/978-3-031-58716-0_3
 20. Corte-Real Santos, M., Pope, G.: Learning to sqi. <https://learningtosqi.github.io/> (2022), last accessed June 11, 2023
 21. Damgård: On σ -protocols. <http://www.cs.au.dk/%7eivan/Sigma.pdf> (2010)
 22. Dartois, P., Leroux, A., Robert, D., Wesolowski, B.: SQIsignHD: New dimensions in cryptography. In: Joye, M., Leander, G. (eds.) EUROCRYPT 2024, Part I. LNCS, vol. 14651, pp. 3–32. Springer, Cham (May 2024). https://doi.org/10.1007/978-3-031-58716-0_1
 23. De Feo, L.: Mathematics of isogeny based cryptography. arXiv preprint arXiv:1711.04062 (2017)
 24. De Feo, L., Fouotsa, T.B., Panny, L.: Isogeny problems with level structure. In: Joye, M., Leander, G. (eds.) EUROCRYPT 2024, Part VII. LNCS, vol. 14657, pp. 181–204. Springer, Cham (May 2024). https://doi.org/10.1007/978-3-031-58754-2_7
 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, Cham (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, Cham (Apr 2023). https://doi.org/10.1007/978-3-031-30589-4_23
 27. Duparc, M., Fouotsa, T.B.: SQIPrime: A dimension 2 variant of SQIsignHD with non-smooth challenge isogenies. In: Chung, K.M., Sasaki, Y. (eds.) ASI-

- ACRYPT 2024, Part III. LNCS, vol. 15486, pp. 396–429. Springer, Singapore (Dec 2024). https://doi.org/10.1007/978-981-96-0891-1_13
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, Cham (Apr / May 2018). https://doi.org/10.1007/978-3-319-78372-7_11
 29. 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>
 30. Goldreich, O., Micali, S., Wigderson, A.: Proofs that yield nothing but their validity and a methodology of cryptographic protocol design (extended abstract). In: 27th FOCS. pp. 174–187. IEEE Computer Society Press (Oct 1986). <https://doi.org/10.1109/SFCS.1986.47>
 31. 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, Berlin, Heidelberg (Nov / Dec 2011). https://doi.org/10.1007/978-3-642-25405-5_2
 32. Kohel, D., Lauter, K., Petit, C., Tignol, J.P.: On the quaternion-isogeny path problem. *LMS Journal of Computation and Mathematics* **17**(A), 418–432 (2014)
 33. Leroux, A.: Quaternion algebras and isogeny-based cryptography. https://www.lix.polytechnique.fr/Labo/Antonin.LEROUX/manuscrit_these.pdf (2022), last accessed March 23, 2023
 34. Leroux, A.: Verifiable random function from the deuring correspondence and higher dimensional isogenies. In: Fehr, S., Fouque, P.A. (eds.) EUROCRYPT 2025, Part VII. LNCS, vol. 15607, pp. 167–194. Springer, Cham (May 2025). https://doi.org/10.1007/978-3-031-91098-2_7
 35. Maino, L., Martindale, C., Panny, L., Pope, G., Wesolowski, B.: A direct key recovery attack on SIDH. In: Hazay, C., Stam, M. (eds.) EUROCRYPT 2023, Part V. LNCS, vol. 14008, pp. 448–471. Springer, Cham (Apr 2023). https://doi.org/10.1007/978-3-031-30589-4_16
 36. Nakagawa, K., Onuki, H., Castryck, W., Chen, M., Invernizzi, R., Lorenzon, G., Vercauteren, F.: SQIsign2D-East: A new signature scheme using 2-dimensional isogenies. In: Chung, K.M., Sasaki, Y. (eds.) ASIACRYPT 2024, Part III. LNCS, vol. 15486, pp. 272–303. Springer, Singapore (Dec 2024). https://doi.org/10.1007/978-981-96-0891-1_9
 37. National Institute of Standards and Technology (NIST): Call for Additional Digital Signature Schemes for the Post-Quantum Cryptography Standardization Process (2022), <https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/call-for-proposals-dig-sig-sept-2022.pdf>
 38. Onuki, H., Nakagawa, K.: Ideal-to-isogeny algorithm using 2-dimensional isogenies and its application to SQIsign. In: Chung, K.M., Sasaki, Y. (eds.) ASIACRYPT 2024, Part III. LNCS, vol. 15486, pp. 243–271. Springer, Singapore (Dec 2024). https://doi.org/10.1007/978-981-96-0891-1_8
 39. 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>
 40. Page, A., Wesolowski, B.: The supersingular endomorphism ring and one endomorphism problems are equivalent. In: Joye, M., Leander, G. (eds.) EUROCRYPT 2024, Part VI. LNCS, vol. 14656, pp. 388–417. Springer, Cham (May 2024). https://doi.org/10.1007/978-3-031-58751-1_14

41. Robert, D.: Breaking SIDH in polynomial time. In: Hazay, C., Stam, M. (eds.) EUROCRYPT 2023, Part V. LNCS, vol. 14008, pp. 472–503. Springer, Cham (Apr 2023). https://doi.org/10.1007/978-3-031-30589-4_17
42. Silverman, J.H.: The arithmetic of elliptic curves, vol. 106. Springer (2009)
43. The Sage Developers: SageMath, the Sage Mathematics Software System (2025), <https://www.sagemath.org>, dOI 10.5281/zenodo.6259615
44. Voight, J.: Quaternion algebras. Springer Nature (2021)
45. 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>

A Pseudocode

A.1 Algorithms from other authors

To make our paper self contained, in this section we recall some known algorithms from the SQIsign literature, and more specifically from Leroux thesis [33]. In our algorithms from Section 5 we use the following:

- **EquivalentPrimeIdeal**, that on input a fractional ideal I returns the smallest left equivalent ideal I' of prime norm and $\alpha \in I$ such that $I' = \chi_I(\alpha)$. We refer to [33, Algorithm 6] for details;
- **FullRepresentInteger**, that on input an integer M returns a quaternion in $\mathcal{O}_0$ of norm M in $\mathcal{B}$ (if it exists). We refer to [33, Algorithm 4] for details;
- **FullStrongApproximation_N** ([33, Algorithm 5]), that on input an integer M and a pair $C, D \in \mathbb{Z}$ returns $\mu \in \mathcal{O}_0$ such that $n(\mu) = N$ and $2\mu = \lambda(jC + kD) + M\mu_1$ for some $\mu_1 \in \mathcal{O}_0$ and $\lambda \in \mathbb{Z}$.
- **IdealSuborderEichlerNorm** [33, Algorithm 14], that we recall in Algorithm 5, with notations slightly adapted to the use it has in Appendix B;
- **IdealEichlerNorm**, that we recall in Algorithm 6;
- **GenericKLPT** [33, Algorithm 33], which we include for comparison to our variants, with the original notations.
- **SigningKLPT** [33, Algorithm 11] which we include for comparison to our variants, with the original notations. It relies on **RandomEquivalentEichlerIdeal** for rerandomization, which is explained (without pseudocode) in Appendix C.3.

A.2 Pseudocode for **BorelSigningKLPT**

in Algorithm 7, we give full pseudocode for the more efficient KLPT variant for Borel level structure mentioned in Section 5.3.

B Generalization of **ScalarSigningKLPT** to inputs of non-square norm modulo N

In Section 5 we assumed the input to **ScalarSigningKLPT** to be an ideal I of norm a square modulo N . In this section, we first explain that equivalences in $\mathbb{Z} + N\mathcal{O}$

Algorithm 5 `IdealSuborderEichlerNorm` _{ℓ^e}

Input: An integer N , two left $\mathcal{O}_0$ -ideals I, J of inert prime norm N_I, N_J , with $\gcd(N, N_I, N_J) = 1$,

Output: $\beta \in \mathbb{Z} + DI \cap J$ of norm $N_J \ell^e$.

- 1: Select a random class $(C_2 : D_2) \in \mathbb{P}^1(\mathbb{Z}/D\mathbb{Z})$.
 - 2: Compute $\gamma = \text{FullStrongApproximation}_{N_J \ell^{e_1}}(N, C_2, D_2)$. If the computation fails go back to Step 1.
 - 3: Compute $(C_0 : D_0) = \text{EichlerModConstraint}(I, \gamma, 1)$.
 - 4: Compute $(C_3 : D_3) = \text{IdealModConstraint}(J, \gamma)$.
 - 5: Sample a random D'_2 in $\mathbb{Z}/N\mathbb{Z}$, compute $C'_2 = -D'_2 C_2 (D_2)^{-1} \pmod{N}$.
 - 6: Compute $C_1 = \text{CRT}_{N_I, N, N_J}(C_0, C'_2, C_3)$, $D_1 = \text{CRT}_{N_I, N, N_J}(D_0, D'_2, D_3)$.
 - 7: Compute $\mu = \text{FullStrongApproximation}_{N_J \ell^{e-e_1}/n(\gamma)}(N_I N N_J, C_1, D_1)$. If it fails, go back to step 1.
 - 8: return $\beta = \gamma \mu$.
-

Algorithm 6 `IdealEichlerNorm` _{$\mathcal{N}$} (I, J)

Input: Two left $\mathcal{O}_0$ -ideals I, J of inert prime norm N_I, N_J , with $\gcd(N_I, N_J) = 1$,

Output: $\beta \in (\mathbb{Z} + I) \cap J$ of norm in $n(J)\mathcal{N}$.

- 1: Compute $L = \text{EquivalentPrimeIdeal}(J)$, $L = \chi_J(\delta)$ for $\delta \in J$. Set $N = n(L)$.
 - 2: Compute $\gamma = \text{FullRepresentInteger}_{N_J \mathcal{N}}$.
 - 3: Compute $(C_0 : D_0) = \text{IdealModConstraint}(L, \gamma)$.
 - 4: Compute $(C_1 : D_1) = \text{EichlerModConstraint}(I, \gamma, \delta)$.
 - 5: Compute $C = \text{CRT}_{N_J, N_I}(C_0, C_1)$ and $D = \text{CRT}_{N_J, N_I}(D_0, D_1)$.
 - 6: Compute $\mu = \text{StrongApproximation}_{N_J \mathcal{N}/n(\gamma)}(N_I N_J, C, D)$.
 - 7: return $\beta = \gamma \mu \delta$.
-

Algorithm 7 `BorelSigningKLPT` _{ℓ^e} (I, I_N)

Input: I and I_N left ideals of the same maximal order N in $\mathcal{B}_{p, \infty}$, with $N \leftarrow n(I_N)$ prime or power of prime of known factorization and e such that ℓ^e large enough (See Proposition 21).

Output: $J \sim I$ such that $J = \chi_I(\beta)$ with $\beta \in (\mathbb{Z} + I_N) \cap I$ and $n(J) \mid 2^e$

- 1: $\alpha, I'_c \leftarrow \text{EquivalentPrimeIdeal}(I_c)$ // $I'_c = \chi_{I_c}(\alpha)$
 - 2: Let $I_1 \leftarrow \frac{1}{\alpha} I \alpha$
 - 3: Let $I'_N \leftarrow \frac{1}{\alpha} I_N \alpha$
 - 4: $\alpha_I, I_0 \leftarrow \text{InitialRerandomization}(I_1, \mathbb{Z} + I'_N, I'_c)$ // See Section 5.2
 - 5: $\beta \leftarrow \text{IdealEichlerNorm}_{\ell^e}(I'_c I'_N, I_0)$
 - 6: $J_0 \leftarrow \chi_{I_0}(\beta)$ and $J_a \leftarrow [I'_c]^* J_0$ and $J \leftarrow \alpha J_a \frac{1}{\alpha}$
 - 7: return J
-

Algorithm 8 `GenericKLPT` _{$\mathcal{N}$} $(\mathcal{O}_1, I)$

Input: $\mathcal{O}_1$ a maximal order and I left $\mathcal{O}_1$ -ideal

Output: $J \sim I$ of norm in $\mathcal{N}$

- 1: Compute $I_0 = I(\mathcal{O}_0, \mathcal{O}_1)$ $\triangleright I_0$ primitive connecting ideal of $\mathcal{O}_0$ and $\mathcal{O}_1$
 - 2: Compute $K = \text{RandomEquivalentPrimeIdeal}(I_0)$ and α such that $K = I_0 \alpha$
 - 3: Compute $I' = \alpha^{-1} I \alpha$ and $L = [K]^* I'$
 - 4: Compute $\mu = \text{IdealEichlerNorm}_{\mathcal{N}}(K, L)$
 - 5: Set $\beta = \alpha \mu \alpha^{-1}$
 - 6: return $\chi_I(\beta)$
-

Algorithm 9 `SigningKLPT`_{2^e}(I_τ, I)

Input: I_τ a primitive left $\mathcal{O}_0$ and right $\mathcal{O}_1$ -ideal of prime norm N_τ

Input: I a left $\mathcal{O}_1$ -ideal

Output: $J \sim I$ of norm 2^e

- 1: Compute $K = \text{RandomEquivalentEichlerIdeal}(I, N_\tau)$
 - 2: Compute $K' = [I_\tau]^* K$ and set $L = \text{EquivalentPrimeIdeal}(K')$, $L = \chi_{K'}(\delta)$ for $\delta \in K'$ with $N = n(L)$. Sample $e_0 \in e_0(N)$.
 - 3: Compute $\gamma = \text{FullRepresentInteger}_{ND2^{e_0}}$
 - 4: Compute $(C_0 : D_0) = \text{IdealModConstraint}(L, \gamma)$
 - 5: Compute $(C_1 : D_1) = \text{EichlerModConstraint}(I_\tau, \gamma, \delta)$
 - 6: Compute $C = \text{CRT}_{N_\tau, N}(C_0, C_1)$ and $D = \text{CRT}_{N_\tau, N}(D_0, D_1)$
 - 7: $e_0 \leftarrow v_2(n(\gamma))$ and $e_1 \leftarrow e - e_0$
 - 8: Compute $\mu = \text{FullStrongApproximation}_{2^{e_1}}(NN_\tau, C, D)$. If it fails, go back to step 3.
 - 9: Set $\beta = \gamma\mu$
 - 10: **return** $J = [I_\tau]_* \chi_L(\beta)$
-

preserve the square or non-square character of ideal norms modulo N (or to say it short, the squarity of ideals). It is therefore clear that the input to `ScalarSigningKLPT` has the same squarity than the input to `IdealSuborderEichlerNorm` in this algorithm. Next, we analyze why these algorithms only work for ideals with square norm modulo N (which we'll call square ideals for short). Finally, we explain in which cases and how it is possible to adjust inputs to `ScalarSigningKLPT` so that it can also be used for non-square input ideals.

For conciseness, we use the word "squarity" for integers to designate the character of being or not being a square modulo N . For quaternion ideals, their squarity means the squarity of their norms. Similarly, if an ideal is said square, we mean that its norm is a square modulo N .

B.1 Equivalence-taking in $\mathbb{Z} + N\mathcal{O}$ preserves squares

For $\mathcal{O}$ a maximal ideal in $\mathcal{B}_{p, \infty}$, taking equivalences in $\mathbb{Z} + N\mathcal{O}$ cannot alter the squarity of an $\mathcal{O}$ -ideal, so that the classes in $\text{Cl}(\mathbb{Z} + N\mathcal{O})$ have either only or no element whose norm is a square modulo N . This fact can be understood in two ways, the elementary and the matrix way.

Lemma 26. *Let $\mathcal{O}$ a maximal order in $\mathcal{B}_{p, \infty}$ and I a left $\mathcal{O}$ -ideal. Let N be a positive integer coprime to $n(I)$. Let $\alpha \in I \cap (\mathbb{Z} + N\mathcal{O})$ of norm coprime to N and $J = I \frac{\alpha}{n(I)}$. Then either both $n(I)$ and $n(J)$ are squares modulo N , or none of them is a square modulo N .*

Proof. Since $\alpha \in I \cap (\mathbb{Z} + N\mathcal{O})$, $\alpha = nIn + N\beta$ for some $n \in \mathbb{Z}$ and $\beta \in \mathcal{O}$ with $\text{tr}(\beta) = 0$. Therefore $n(\alpha) = n(I)^2 n^2 + N^2 n(\beta)$. Since $\alpha \in I$, $n(I) \mid n(\alpha)$ so $n(I)$ also divides $n(\beta)$. As N and $n(I)$ are coprime, there exists $m \in \mathbb{Z}$ such that $n(\alpha) = n(I)^2 n^2 + N^2 mn(I)$. Therefore we obtain $n(J) = n(\alpha)n(I) = n(I)n^2 + N^2 m$, which gives $n(J) = n(I)n^2 \pmod{N}$. n^2 is an integer square and

therefore a square modulo N . As a consequence, $\mathfrak{n}(J)$ and $\mathfrak{n}(I)$ are either both squares or both non-squares modulo N . $\square$

Proof. This can also be seen by the matrices from Lemma 5. Compute M_I and M_J the matrices associated to (the isogenies associated to) the ideal I and J from Lemma 26. We know that these matrices are the same up to multiplication by a scalar matrix, since the ideals are equivalent in $(\mathbb{Z} + N\mathcal{O})$. Scalar matrices have square degree, so the determinants of M_I and M_J are either both squares or both non-squares modulo N . These determinants are, modulo N , equal to the norms of I and J . $\square$

Lemma 26 gives a first idea of why we stated **ScalarSigningKLPT** for square input ideals only. It makes clear that any algorithm taking equivalences in $\mathbb{Z} + N\mathcal{O}$ like **ScalarSigningKLPT** has the inherent limitation that it cannot create an output ideal whose norm has a different squarity than the input. Given that our **ScalarSigningKLPT** has a square target norm (the exponent e is even), it can obviously only treat square inputs.

B.2 Details of **IdealSuborderEichlerNorm** applying only to squares

Knowing that equivalences respecting $\mathbb{Z} + N\mathcal{O}$ preserve squarity, it seems natural to use the exact same algorithm **ScalarSigningKLPT**, but with a non-square output norm, and a non-square input ideal. However, this approach fails due to inherent limitations of its **IdealSuborderEichlerNorm** subroutine, whose pseudocode can be found in Algorithm 5 or in Leroux' thesis [33, Algorithm 14]. More precisely, with the notations from the pseudocode of Algorithm 5 and the notation $\mu_0 = j(C_1i + D_1)$, one notices the following points which show that the output norm ℓ^e must be a square modulo N :

- For λ to exist, we need ℓ^e and $\mathfrak{n}(\mu_0)$ of same squarity
- ℓ^e has the same squarity as the product $\mathfrak{n}(\gamma)\mathfrak{n}(\mu_0)$
- $\mathfrak{n}(\gamma)$ and $\mathfrak{n}(\mu_0)$ have the same squarity, so their product is a square modulo N

In consequence, the output of **IdealSuborderEichlerNorm** has square norm modulo N . Since **ScalarSigningKLPT** takes all equivalences to the input in $\mathbb{Z} + N\mathcal{O}$, Lemma 26 means that the input ideal to **ScalarSigningKLPT** must have square norm modulo N .

B.3 Workaround for non-squares when a solution exists

Despite this obstacle, suitable input transformations allow to use **ScalarSigningKLPT** for non-square input ideals, as long as the output is expected to be a power of a non-square. Denote ℓ^e the required output norm with ℓ not a square modulo N and e odd, and I an input ideal of norm not a square modulo N . Denote $\mathcal{O}$ the left order of I . Then we can use a random right $\mathcal{O}$ -ideal I_r of non-square norm ℓ to create an alternative input $I_r I$ which has square norm modulo

N . We can then call **ScalarSigningKLPT** on $I_r I$, with output norm ℓ^{e-1} which is square modulo N as required. Finally the obtained output J of **ScalarSigningKLPT** is multiplied by $\bar{I}_r$ to get the ideal $\bar{I}_r J$ of norm ℓ^e which is equivalent to I in $\mathbb{Z} + N\mathcal{O}$. Algorithm 10 is obtained by applying these step to all non-square input ideals (and output norms).

Algorithm 10 **GeneralizedScalarSigningKLPT** $_{\ell^e}(I, N)$

Input: N prime or power of prime of known factorization, I left ideal of a maximal order $\mathcal{O}$ in $B_{p,\infty}$ such that $\ell^e \mathfrak{n}(I) \bmod N$ is a square, $e \in \mathbb{Z}$ even such that ℓ^e large enough while ℓ is a small prime (See Proposition 18).
Output: $J \sim I$ such that $J = \chi_I(\beta)$ with $\beta \in (\mathbb{Z} + N\mathcal{O}) \cap I$ and $\mathfrak{n}(J) \mid 2^e$
1: **if** $\mathfrak{n}(I)$ is a square modulo N **then**
2: $J \leftarrow \text{ScalarSigningKLPT}_{\ell^e}(I, N)$
3: **else**
4: Let I_r a uniformly random right $\mathcal{O}$ -ideal of norm ℓ non such that $I_r I$ is primitive
5: $J_r \leftarrow \text{ScalarSigningKLPT}_{\ell^{e-1}}(I_r I, N)$
6: $J \leftarrow \bar{I}_r J_r$
7: **if** J not primitive **then**
8: Restart
9: **return** J

Using this additional input treatment, **GeneralizedScalarSigningKLPT** can solve all solvable squarity combinations for smooth norms. The cases where the in- and output norms have different squarity don't have a solution, since ideals of such norms cannot be equivalent in $\mathbb{Z} + N\mathcal{O}$ as seen in Lemma 26.

C Proofs

In this appendix we collect the detailed proofs of the statements that we omitted in the main body of the paper. For the sake of readability we restate the statements before their proofs.

C.1 Proofs from Section 3

Theorem 14. *Let $p, N, \Gamma, \mathbb{E}, \mathbb{E}'$ be as in Corollary 10. Then each locally-principal ideal of $\mathcal{O}(\mathbb{E})$ is of the form $I_{\rho', \mathbb{E}'}$ for some $\mathbb{E}'$ and ρ' .*

Moreover, if we suppose that Γ is additively stable, then two ideals $I_{\rho', \mathbb{E}'}, I_{\rho'', \mathbb{E}''}$ are equivalent if and only if $\mathbb{E}', \mathbb{E}''$ are isomorphic.

Proof. For the first part we start by proving that if I is an ideal equivalent to a certain $I_{\rho, \mathbb{E}'}$, then $I = I_{\rho', \mathbb{E}'}$ for some $\rho' \in \text{Hom}(\mathbb{E}, \mathbb{E}')$. By hypothesis we know that $I = I_{\rho, \mathbb{E}'} \cdot \frac{\alpha}{Q}$ for some $\alpha \in \mathcal{O}(\mathbb{E})$ and some positive integer Q , hence by (15) it is enough finding a ρ' in $\mathcal{O}(\mathbb{E})$ such that $\frac{\alpha}{Q} = \frac{\hat{\rho} \circ \rho'}{\deg(\rho)}$ or equivalently $\frac{\rho \circ \alpha}{Q} = \rho'$. In other words this is equivalent to proving that $\rho \circ \alpha$ lies in the sublattice

$Q \cdot \text{Hom}(\mathbb{E}, \mathbb{E}')$ of $\text{Hom}(\mathbb{E}, \mathbb{E}')$. To prove this pick an element $\phi \in \text{Hom}(\mathbb{E}, \mathbb{E}')$ of degree coprime to Q . Then by definition $\hat{\phi}\rho$ is an element of $I_{\rho, \mathbb{E}'}$ hence $\frac{1}{Q}\hat{\phi}\rho\alpha$ is an element of $I \subset \mathcal{O}(\mathbb{E})$ (we are supposing I is a proper ideal, not only a fractional ideal) hence we can find an element $\beta \in \mathcal{O}(\mathbb{E})$ such that

$$\deg(\phi) \cdot \rho\alpha = Q\phi \cdot \frac{1}{Q}\hat{\phi}\rho\alpha = Q\phi\beta \in Q \cdot \text{Hom}(\mathbb{E}, \mathbb{E}')$$

and since multiplication by $\deg \phi$ is invertible in $\text{Hom}(\mathbb{E}, \mathbb{E}')/Q\text{Hom}(\mathbb{E}, \mathbb{E}')$ we deduce that also $\rho\alpha$ lies in $Q\text{Hom}(\mathbb{E}, \mathbb{E}')$.

Now let I be any (non-zero) locally principal ideal of $\mathcal{O}(\mathbb{E})$, for which we want to prove that it is of the form $I_{\rho', \mathbb{E}'}$. First of all we prove that I is equivalent to some ideal whose index in $\mathcal{O}(\mathbb{E})$ is coprime to Np . Indeed I is a lattice isomorphic to $\mathbb{Z}^4$ and by the chinese remainder theorem, for each exponent e the natural map

$$I \longrightarrow \prod_{\ell | Np} \frac{I}{\ell^e I}$$

is surjective, hence a fortiori, if we denote $(I \bmod Q)$ the image of I in $\mathcal{O}(\mathbb{E})/Q\mathcal{O}(\mathbb{E})$, the following map is surjective

$$I \longrightarrow \prod_{\ell | Np} (I \bmod \ell^e) .$$

In other words the map

$$I \longrightarrow \prod_{\ell | Np} (I \otimes \mathbb{Z}_\ell) ,$$

has dense image. If we now fix a generator α_ℓ of $I \otimes \mathbb{Z}_\ell$ for each ℓ dividing Np , then we for each precision e we can find an element α of I which is congruent to α_ℓ , modulo ℓ^e for all $\ell \mid Np$. Taking e large enough this implies that α differs multiplicatively from α_ℓ by a unit of $\mathcal{O}(\mathbb{E}) \otimes \mathbb{Z}_\ell$ (indeed set $U \subset \mathcal{O}(\mathbb{E}) \otimes \mathbb{Z}_\ell$ of elements congruent to 1 modulo ℓ is an open containing units, and for e large enough α lies in the neighborhood $U\alpha_\ell$ of α_ℓ) implying that α generates $I \otimes \mathbb{Z}_\ell$ for all $\ell \mid Np$. Now take such an α and write $\deg(\alpha) = Q_1 Q_2$, with Q_1 only multiple of primes dividing Np and Q_2 coprime to Np : then the ideal $I \cdot \frac{\hat{\alpha}}{Q_1}$ is equivalent to I and has index in $\mathcal{O}(\mathbb{E})$ coprime to Np .

By what we have seen before, to prove that I is of the form $I_{\rho', \mathbb{E}'}$ we can change I to an equivalent one, hence we can suppose that $[\mathcal{O}(\mathbb{E}) : I]$ is coprime to Np . Then we claim that

$$\ker(I) = \cap_{\alpha \in I} \ker \alpha .$$

is a subgroup of E of order $\sqrt{[\mathcal{O}(\mathbb{E}) : I]}$: indeed it is enough to prove that for all primes ℓ , the $\ker(I) \cap E[\ell^\infty]$ has order equal to the ℓ part of $\sqrt{[\mathcal{O}(\mathbb{E}) : I]}$, namely order equal to $\sqrt{[\mathcal{O}(\mathbb{E}) \otimes \mathbb{Z}_\ell : I \otimes \mathbb{Z}_\ell]}$; this is clear for the ℓ 's that do not divide the index of I and for the primes dividing such an index, which are coprime to pN it is a consequence of the following isomorphism

$$\mathcal{O}(\mathbb{E}) \otimes \mathbb{Z}_\ell = \text{End}(E) \otimes \mathbb{Z}_\ell \cong M_2(\mathbb{Z}_\ell)$$

which keeps track of the action of endomorphism on the ℓ^∞ -torsion of E (hence on the kernels of the endomorphisms when intersected with the ℓ^∞ -torsion) by taking basis $(\tilde{P}, \tilde{Q})$ of the Tate module $T_\ell E$ and sending an endomorphism α to the matrix $M \in M_2(\mathbb{Z}_\ell)$ such that $(\alpha(\tilde{P}), \alpha(\tilde{Q})) = M \cdot (\tilde{P}, \tilde{Q})$. Then we can consider the isogeny $\gamma: E \rightarrow E/\ker(I)$ and the Γ -structure $\gamma(S)$ on $E/\ker(I)$, which is well defines since γ has degree coprime to N : the ideal $I_{\gamma, (E/\ker(I), \gamma(S))}$ contains all elements of $\mathcal{O}(\mathbb{E})$ whose kernel contains $\ker(I) = \ker(\gamma)$ hence contains I and it is actually equal to I since by the previous computations has the same index in $\mathcal{O}(\mathbb{E})$.

Now the second part of the statement. One implication is clear using Eq. (15) and the fact that if $u: \mathbb{E}' \rightarrow \mathbb{E}'$ is an isomorphism, then $I_{u \circ \rho'} = \circ u \circ \rho' = \text{Hom}(\mathbb{E}', \mathbb{E}) \circ \rho' = I_{\rho'}$.

For the other implication, up to using Eq. (15), we can suppose that $I_{\rho', \mathbb{E}'} = I_{\rho'', \mathbb{E}''}$. First of all we notice that the kernel of ρ' can be extracted from the ideal: indeed by definition $\ker \rho'$ is contained in the intersection $\cap_{i \in I} \ker i$, and, to see that the two are equal, we choose elements $\phi_1, \phi_2 \in \text{Hom}(\mathbb{E}_A, \mathbb{E})$ such that $\deg(\rho')$ is coprime to $\deg(\phi_1)$ and both are coprime to $\deg(\phi_2)$, so that $i_1 = \hat{\phi}_1 \circ \rho'$ and $i_2 = \hat{\phi}_2 \circ \rho'$ are two elements in I such that $\ker i_1 \cap \ker i_2 = \ker \rho'$ (the existence of the isogenies ϕ_j is a consequence of Corollary 10).

Applying the same argument on ρ'' we deduce that $\ker \rho' = \ker \rho''$. In particular is E'' is the elliptic curve underlying $\mathbb{E}''$, there exists an isomorphism $u: E' \rightarrow E''$ such that $\rho'' = u\rho'$. It remains to prove that u is an isomorphism also when we take into account the level structure, i.e. that $u(S') = S''$ where we write $\mathbb{E}'' = (E'', S'')$. Applying Lemma 5, take ϕ_1 an element $\phi' \in \text{Hom}(\mathbb{E}, \mathbb{E}')$ sending exactly S to S' , hence having degree coprime to N . Since $I_{\rho', \mathbb{E}'} = I_{\rho'', \mathbb{E}''}$ we deduce that there exists $\phi'' \in \text{Hom}(\mathbb{E}, \mathbb{E}'')$ such that

$$\hat{\phi}' \circ \rho' = \hat{\phi}'' \circ \rho'' = \hat{\phi}'' \circ u\rho',$$

which implies, after taking the dual, that $\phi' = \hat{u}\phi''$, hence $\phi'' = u \circ \phi'$. Since the degree of ϕ' is coprime to N , the same is true for ϕ'' , hence the matrix $M_{\phi''}$ representing ϕ'' in basis $(P, Q) \in S$ and $(P'', Q'') \in S''$ is a matrix in $\text{GL}_2(\mathbb{Z}/N)$. Moreover, since ϕ'' lies in $\text{Hom}(\mathbb{E}, \mathbb{E}'')$, the same matrix lies in $\langle \Gamma \rangle$. Hence by our hypothesis we have that $M_{\phi''}$ lies in $\langle \Gamma \rangle \cap \text{GL}_2(\mathbb{Z}/N) = \Gamma$, hence

$$S'' = \phi''(S) = u \circ \phi'(S) = u(S'),$$

i.e. u is also an isomorphism between $\mathbb{E}'$ and $\mathbb{E}''$. □

C.2 Proofs from Section 5

Lemma 17. *For I a primitive right ideal of a maximal order $\mathcal{O}$ in $\mathcal{B}_{p, \infty}$. Then $(\mathbb{Z} + I) \cap (\mathbb{Z} + N\mathcal{O}) = (\mathbb{Z} + NI)$ for $N \in \mathbb{Z}$ coprime to $\mathfrak{n}(I)$.*

Proof (Proof of Lemma 17). Let's assume I is a right $\mathcal{O}$ -ideal.

1. Since I is a group and $N \in \mathbb{Z}$, $NI \subset I$. Since $I \cap \mathcal{O}_R(I) = \mathcal{O}$, $NI \subset NO$ so $(\mathbb{Z} + NI) \subset (\mathbb{Z} + I) \cap (\mathbb{Z} + NO)$.

2. Let $z \in (\mathbb{Z} + I) \cap (\mathbb{Z} + NO)$. Then there are integers λ, μ such that $x = z - \lambda \in I$ and $y = z - \mu \in NO$. Note $n_I = \min(I \cap \mathbb{Z})$ and observe that $N = \min(NO \cap \mathbb{Z})$. Since $\mathfrak{n}(I)$ divides n_I and $\gcd(\mathfrak{n}(I), N) = 1$, n_I and N are coprime. By applying the Chinese remainders theorem to (λ, n_I) and (μ, N) we get $\nu \in \mathbb{Z}$ such that $z - \nu \in NO \cap I$. This proves that $(\mathbb{Z} + I) \cap (\mathbb{Z} + NO) \subset (\mathbb{Z} + (NO \cap I))$.

3. Let us now show that $I \cap NO \subset NI$. Let $z \in I \cap NO$. Write $z = Nx$ with $x \in O$. Since $\gcd(N, \mathfrak{n}(I)) = 1$, there are integers λ, μ such that $\lambda N + \mu \mathfrak{n}(I) = 1$. Then $\lambda Nx + \mu \mathfrak{n}(I)x = x$. However, $\lambda Nx \in I$ since $Nx \in I$ and $\mu \mathfrak{n}(I)x \in I$ since $x \in O$ and $\mathfrak{n}(I) \in I \cap \mathbb{Z}$. Therefore $x \in I$ and $z = Nx \in NI$. This implies $NO \cap I \subset NI$.

4. With 2. and 3. we get $(\mathbb{Z} + I) \cap (\mathbb{Z} + NO) \subset (\mathbb{Z} + NI)$. Together with 1. this proves the result. $\square$

Proposition 18. *There is a variant of [ScalarSigningKLPT](#) which produces output for $\ell^e > p^{9/2} N^{10} \epsilon$ with ϵ polylogarithmic in (pN) , under plausible assumptions.*

Proof (Proof of Proposition 18). Following Leroux [33, Section 3.4], in order to produce output under plausible assumptions, [IdealSuborderEichlerNorm](#) requires to get e such that ℓ^e is larger than $p^2(N^2 N_c)^3 \mathfrak{n}(I)^2$ (multiplied additionally with some logarithmic factor).

Given how we compute I in Section 5.1, we have $\mathfrak{n}(I)$ smaller than $N^2 \lambda_4$ times some logarithmic factor, where λ_4 is the forth minimum of the pullback of the rerandomized input to $\mathcal{O}_0$.

Usually, this λ_4 is as large as $\sqrt{p}$. If it is larger, one can replace $\mathcal{O}_0$ by another special extremal order (and recompute a connecting ideal), which will result in different minima. Similarly, we can assume that N_c is of norm $\sqrt{p}$ up to logarithmic factors, and use another special extremal order otherwise.

The technique to use alternative special extremal orders when the forth minimum of the $\mathcal{O}_0$ -ideal is not small enough is used in the KLPT-based ideal-to-isogeny algorithm in the first round SQIsign NIST submission [16, Section 2.5.2.1]. In another context, a similar argument is used in the second-round SQIsign NIST submission [1, Section 3.2.5] and that variant is justified heuristically in [1, Section 9.3].

By substituting into $p^2(N^2 N_c)^3 \mathfrak{n}(I)^2$, we obtain $p^2 N^6 \sqrt{p}^3 N^4 \sqrt{p}^2$ which equals $p^{9/2} N^{10}$ and therefore proves the proposition. $\square$

Lemma 19. *For I a left ideal of a maximal order $\mathcal{O}$ and $N, N_c, \mathfrak{n}(I)$ coprime, there exist $\omega \in \mathbb{Z} + N\mathcal{O}$ such that N_c is inert in $\mathbb{Z}[\omega]$ and $\gamma \in I \cap \mathbb{Z} + N\mathcal{O}$ such that γ is not in $N_c \mathcal{O}_R(I)$.*

Proof (Proof of Lemma 19). 1. According to [33, Lemma 5.3.1], there is an $\omega_0 \in O$ such that N_c is inert in $\mathbb{Z}[\omega_0]$. Let $\omega = N\omega_0$. Then $\omega \in \mathbb{Z} + NO$ and N_c inert in $\mathbb{Z}[\omega]$.

2. For γ : Let $\gamma_0 \in I$ of norm coprime to N_c (exists since $\mathfrak{n}(I)$ coprime to N_c). Then $\gamma = N\gamma_0 \in I \cap \mathbb{Z} + NO$, and γ has norm $N^2 \mathfrak{n}(\gamma_0)$ not divisible by N_c , so that $\gamma \notin N_c \mathcal{O}_R(I)$. $\square$

Lemma 20. *For I, J two primitive compatible ideals of $B_{p,\infty}$ (that is $\mathcal{O}_R(I) = \mathcal{O}_L(J)$) of coprime norms, $(\mathbb{Z} + I) \cap (\mathbb{Z} + J) = (\mathbb{Z} + IJ)$.*

Proof (Proof of Lemma 20). I is included in $\mathcal{O}_R(I) = \mathcal{O}_L(J)$ and J in $\mathcal{O}_L(J) = \mathcal{O}_R(I)$, we have IJ included in both I and J , and therefore $(\mathbb{Z} + IJ) \subset (\mathbb{Z} + I) \cap (\mathbb{Z} + J)$.

For the converse, note that $\mathbb{Z} + K = \mathcal{O}_L(K) \cap \mathcal{O}_R(K)$ for K a primitive quaternion ideal of a maximal order $\mathcal{O}_L(K)$. Since we obviously have $(\mathcal{O}_L(I) \cap \mathcal{O}_R(I)) \cap (\mathcal{O}_L(J) \cap \mathcal{O}_R(J)) = \mathcal{O}_L(IJ) \cap \mathcal{O}_R(IJ) \cap \mathcal{O}_L(J) \subset \mathcal{O}_L(IJ) \cap \mathcal{O}_R(IJ)$, we obtain $(\mathbb{Z} + I) \cap (\mathbb{Z} + J) \subset \mathbb{Z} + IJ$.

In conclusion, $(\mathbb{Z} + IJ) = (\mathbb{Z} + I) \cap (\mathbb{Z} + J)$. $\square$

C.3 Details on adapting Leroux' justification of rerandomization for Section 5.2

In [33, Section 2.3], Leroux uses the following notations and notions:

Definition 27. *The ideal class set $Cl(\mathcal{O}_2)$ of an order $\mathcal{O}_2$ is the set of equivalence classes of its left ideals under the equivalence relation $K \sim J$ if and only if there is an invertible quaternion α such that $K = J\alpha$.*

Definition 28. *Let $\mathcal{O}_2$ a maximal order in the quaternion algebra, and $\mathcal{O}_\cap$ an Eichler order contained in $\mathcal{O}_2$. Let $I_\cap$ the unique primitive left $\mathcal{O}_2$ -ideal such that $\mathcal{O}_\cap = \mathbb{Z} + I_\cap$, and $N_\cap$ its norm.*

For K, J left $\mathcal{O}_2$ -ideals of norm coprime to N , say that $K \sim_{\mathcal{O}_\cap} J$ if and only if $(K \cap \mathcal{O}_\cap) \sim (J \cap \mathcal{O}_\cap)$ in the sense of equivalence as left $\mathcal{O}_\cap$ -ideals.

The ideal class set of $\mathcal{O}_2$ for $\mathcal{O}_\cap$ is denoted $Cl_{\mathcal{O}_\cap}(\mathcal{O}_2)$ and defined as the set of equivalence classes of the left ideals of $\mathcal{O}_2$ of norm coprime to $N_\cap$ for the equivalence relation $\sim_{\mathcal{O}_\cap}$.

With these notions, he states:

Proposition 29. [33, Proposition 2.3.12]

Let $\mathcal{O}_1$ a maximal order in the quaternion algebra, and $\mathcal{O}_E$ an Eichler sub-order of $\mathcal{O}_1$.

For C in $Cl(\mathcal{O}_1)$, take $L \in C$ and define $\mathcal{O}_C := \mathcal{O}_R(L)$.

If $\mathcal{O}_C^\times = \langle \pm 1 \rangle$, then for any $\gamma \in L \setminus N\mathcal{O}_C$ and quadratic order $s = \mathbb{Z}[\omega_s]$ of discriminant Δ_S inside $\mathcal{O}_1$ in which N is inert, the map:

$$\Theta : \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) \longrightarrow Cl_{\mathcal{O}_E}(C)$$

$$(A : B) \longmapsto \chi_L((C + \omega_s D)\gamma)$$

is a bijection. In particular, $|Cl_{\mathcal{O}_E}(C)| = N + 1$.

From this Proposition, Leroux then derives the randomization algorithm [33, Algorithm 34] used in SQIsign [25]. There, $(A : B)$ is uniformly randomly sampled in $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ and then used to map an ideal of a maximal order $\mathcal{O}_C$ (of norm coprime to N_E the norm of the unique primitive left $\mathcal{O}_2$ -ideal I_E with $\mathbb{Z} + I_E = \mathcal{O}_E$) to an equivalent ideal which is in a uniformly random equivalent class for equivalence in $\mathcal{O}_E$.

From this rerandomization in SQIsign, we can build the one for SQInstructor with 1-dimensional response representation. Recall our goal in Section 5.2:

1. Randomize a left ideal I of a maximal order $\mathcal{O}$ with respect to the Eichler order $\mathcal{O} \cap \mathcal{O}_0 = \mathbb{Z} + I_c$, where $\mathcal{O}_0$ is the usual maximal order and I_c the unique primitive ideal connecting $\mathcal{O}_0$ and $\mathcal{O}$.
2. In addition, take the equivalent of I in such a way that the equivalence preserves the class of I with respect to $\mathbb{Z} + N\mathcal{O}$.

The work of Leroux summarized above and Lemma 19 allow to achieve this:

Point 1. is exactly what [33, Algorithm 34] does using his proposition 2.3.12 explained above (with $\mathcal{O}$ corresponding to $\mathcal{O}_C$, $\mathcal{O}_0$ to $\mathcal{O}_1$, $\mathbb{Z} + I_c = \mathcal{O}_0 \cap \mathcal{O}$ to $\mathcal{O}_e$ and I is like L a representative of a class C).

Point 2. can be achieved by choosing γ and ω_S such that $(C + \omega_S D)\gamma \in (\mathbb{Z} + N\mathcal{O})$. This is possible thanks to Lemma 19.

The condition of coprimality of I to the norm of I_c is not a concern, since I_c is modified before the rerandomization so that its norm is a large prime, which is very unlikely to divide the norm of I .

D EUF-CMA Security for Section 6 protocol using non-interactive assumptions

In [2] the authors give a reduction of SQIsign EUF-CMA security to non-interactive assumptions. To do this they:

- introduce the notion of *hint-assisted* zero knowledge, where the simulator is given hints sampled from a distribution $\mathcal{H}_E$.
- consider two distributions and conjecture them to be undistinguishable. One is simulating the SQIsign distribution of the responses and challenges, while the other is sampling uniformly over the set of isogenies of degree $d(2^{e'} - d)$ and codomain E , for d in a fixed range, then pushing them via another uniform isogeny of smooth degree. We refer to [2, Problem 3] for the exact definition of the distributions and the aforementioned assumption.

Using this framework, SQIsign, as instantiated in [1], EUF-CMA security reduces to the aforementioned indistinguishability assumption and the following generalization of the one endomorphism problem used already in Section 4.4.

Problem 30 (*q -hint-OneEnd $_p$, Problem 4 [2]*). Given a curve E sampled from the stationary distribution on the set of supersingular elliptic curves over $\mathbb{F}_{p^2}$, and q hints $h_1, \dots, h_q \leftarrow \mathcal{H}_E^{\text{unif}}$, find an endomorphism in $\text{End}(E) \setminus \mathbb{Z}$ in efficient representation.

Here we define for SQInstructor also two distributions $\mathcal{H}_E^{\text{unif}}$ and $\mathcal{H}_E^{\text{sim}}$ as in Figure 6 and give the same result for SQInstructor.

Consider the following indistinguishability assumption between the two distributions:

Problem 31 (q -hint-dist). Let E be a curve obtained from the KeyGen of SQInstructor. Let $(h_1, \dots, h_q)$ be sampled with probability $\frac{1}{2}$ all from $\mathcal{H}_E^{\text{sim}}$ and with probability $\frac{1}{2}$ all from $\mathcal{H}_E^{\text{unif}}$. Given E and the tuple, distinguish between the two distributions.

For an algorithm $\mathcal{A}$ we denote its advantage on Problem 31 by

$$\text{Adv}^{q\text{-hint-dist}}(\mathcal{A}) = |\Pr[\mathcal{A}(E, x) = 1 | \mathcal{H}_E^{\text{sim}}] - \Pr[\mathcal{A}(E, x) = 1 | \mathcal{H}_E^{\text{unif}}]| . \quad (24)$$

Using the above hint definitions and the framework from [2] we can prove:

Theorem 32. *For any PPT adversary $\mathcal{A}$ against the EUF-CMA security of the signature scheme SQInstructor (Section 4.1), there exists polynomial time algorithms $\mathcal{B}, \mathcal{D}$ such that:*

$$\begin{aligned} \text{Adv}_{\text{SQInstructor}}^{\text{EUF-CMA}}(\mathcal{A}) \leq (q+1) \cdot \left(\text{Adv}^{s\text{-hint-OneEnd}_p}(\mathcal{B}) + \right. \\ \left. + \text{Adv}^{s\text{-hint-dist}}(\mathcal{D}) + 2^{-\lambda} + \frac{1}{2\sqrt{p}} \right) + (2q+s+2) \frac{s}{\sqrt{p}} , \end{aligned}$$

where q and s are bounds in the number of queries that $\mathcal{A}$ makes to the random oracle and the signing oracle respectively.

We give the formal proof for the case in which the restarting probability of the signature procedure is negligible and we leave a generalization for the general case as a future work. The proofs follows a similiar strategy to the one in [2], we given in Appendix D a detailed adaptation of the proof. We refer to [2] for a more in depth discussion on the security of Problem 30 and its relation to the Endomorphism Ring Problem (Problem 3). We discuss the indistinguishability assumption and its differences with the one from [2].

From now we denote by $\Sigma_{\text{SQInstructor}}$ the identification protocol in which the challenge is a random element of $\mathbf{M}_2(\mathbb{Z}/N)$ and $\text{SIG}[\Sigma_{\text{SQInstructor}}]$ the signature scheme obtained by applying the Fiat-Shamir transform to $\Sigma_{\text{SQInstructor}}$ and modelling the hash function as a random oracle. We denote by Σ_{SQI} the SQIsign identification protocol from [2].

For the sake of completeness we report here the hint-specific definitions from [2, Section 3] we need for our proof.

Definition 33. *Let R be a relation and $\Sigma = (P, V)$ a Σ -protocol for R .*

1. *A hint distribution $\mathcal{H}$ for R is a collection of distributions $\mathcal{H} = \{\mathcal{H}_x\}_{x \in R}$ with codomains efficiently representable in $|x|$. We call the pair $(R, \mathcal{H})$ a relation with hints.*

- $\mathcal{H}_E^{\text{unif}}$:
- 1: Sample $M \leftarrow \text{GL}_2(\mathbb{Z}/N)$;
 - 2: Sample an integer d from a weighted distribution on the odd integers $\leq B_{\text{rsp}}$ where each integer n , with prime factorization $n = \prod_{i=1}^t p_i^{e_i}$, has weight $\prod_{i=1}^t (p_i + 1)^{e_i}$.
 - 3: Sample an isogeny $\varphi_1 : E \rightarrow E_1$ uniformly among the (possibly non-cyclic) isogenies from E of degree d .
 - 4: Sample $\varphi_2 : E_1 \rightarrow E_2$ of degree $2^a - d$, for $a = \lceil \log(d) \rceil$.
 - 5: **return** $h = (M, \varphi_1, \varphi_2)$.
- $\mathcal{H}_E^{\text{sim}}$:
- 1: Sample $M \leftarrow \text{GL}_2(\mathbb{Z}/N)$ and set $\mathbb{E} = (E, S)$ for $S \leftarrow \Gamma \cdot M \cdot \begin{pmatrix} P_{\text{pk}} \\ Q_{\text{pk}} \end{pmatrix}$;
 - 2: Sample an isogeny $\varphi_1 : \mathbb{E} \rightarrow \mathbb{E}'$ such that:
 - a. $\mathbb{E}$ is distributed sampled from the stationary distribution on the set of supersingular elliptic curves over $\mathbb{F}_{p^2}$ with level structure so that there exists an odd-norm isogeny in $\text{Hom}(\mathbb{E}, \mathbb{E}')$;
 - b. The conditional distribution of φ_1 given $\mathbb{E}'$ is uniform over isogenies $\varphi_1 : \mathbb{E} \rightarrow \mathbb{E}'$ of odd degree $\leq B_{\text{rsp}}$.
 - 3: Sample $\varphi_2 : E \rightarrow E_2$ of degree $2^a - \deg(\varphi_1)$ for $a = \lceil \log(\deg(\varphi_1)) \rceil$;
 - 4: **return** $(M, \varphi_1, \varphi_2)$.

Fig. 6. The hint distribution $\mathcal{H}_E^{\text{unif}}$ and $\mathcal{H}_E^{\text{sim}}$. For the sake of simplicity we added the sampling of M in both the distributions, but it is only relevant for $\mathcal{H}_E^{\text{sim}}$.

2. We say that Σ is $\mathcal{H}$ -hint-assisted wHVZK if there exists a PPT algorithm, called the simulator Sim , such that for all $q = \text{poly}(\lambda)$ and all PPT algorithms $\mathcal{A}$ the advantage in distinguishing a distribution of q real transcripts of Σ and q simulated transcripts of Σ using q hints is negligible in λ . We refer to this advantage as $\text{Adv}_{\Sigma, \mathcal{H}_x, \text{Sim}}^{\text{hint-wHVZK}}(\mathcal{A}, q)$.
3. We say that $(R, \mathcal{H})$ is a hard relation with hints if, in the following game, it holds for all PPT algorithms $\mathcal{A}$ and all $q = \text{poly}(\lambda)$ that

$$\text{Adv}_{R, \mathcal{H}}^{\text{hintrel}}(\mathcal{A}, q) := \Pr \left[(x, w^*) \in R \mid \begin{array}{l} (x, w) \leftarrow \text{Gen}_R(1^\lambda), \\ h_1, \dots, h_q \leftarrow \mathcal{H}_x, \\ w^* \leftarrow \mathcal{A}(x, h_1, \dots, h_q) \end{array} \right] = \text{negl}(\lambda).$$

We then recall the main theorem from [2] that we use to prove Theorem 32.

Theorem 34 ([2], Theorem 1). *Let $(R, \mathcal{H})$ be a relation with hints. Let Σ be a Σ -protocol for the relation R that has challenge space $\mathcal{C}$ and is special-sound with respect to a soundness relation R . Additionally, let Sim be a $\mathcal{H}$ -hint-assisted simulator for Σ .*

For any PPT algorithm $\mathcal{A}$ against the EUF-CMA of $\text{SIG}[\Sigma]$, there exists a PPT algorithm $\mathcal{B}$ and an expected polynomial time algorithm $\mathcal{D}$ such that

$$\begin{aligned} \text{Adv}_{\text{SIG}[\Sigma \text{SQInstructor}]}^{\text{EUF-CMA}}(\mathcal{A}) &\leq (q + 1) \cdot \left(\text{Adv}_{R, \mathcal{H}}^{\text{hintrel}}(\mathcal{D}, s) + \text{Adv}_{\Sigma, \mathcal{H}_x, \text{Sim}}^{\text{hint-wHVZK}}(\mathcal{B}, s) + \frac{1}{|\mathcal{C}|} \right) \\ &\quad + (q + s + 1)s \cdot \text{MinEnt}(\Sigma), \quad (25) \end{aligned}$$

where q and s are upper-bounds on the number of queries that $\mathcal{A}$ makes to the random oracle and to the signing oracle, respectively, and $\text{MinEnt}(\Sigma)$ is the minimum entropy of the protocol Σ .

We can use the previous theorem to finally prove the EUF-CMA security of $\text{SIG}[\Sigma_{\text{SQInstructor}}]$.

Proof (Proof of Theorem 32). The proof is a straightforward adaption of the proof of [2, Theorem 3] in which we use a slightly different protocol and hint distribution. Let R_{OneEnd_p} be the relation Eq. (18), in which the instance is a supersingular elliptic curve and the witnesses are non-scalar endomorphisms. The steps of the proof consists in the following:

- Prove that $\Sigma_{\text{SQInstructor}}$ satisfies the hypothesis of Theorem 34, in particular that it has $\mathcal{H}_E^{\text{sim}}$ -hint-assisted wHVZK, thus reducing the security of $\text{SIG}[\Sigma_{\text{SQInstructor}}]$ to the relation with hints $(R_{\text{OneEnd}_p}, \mathcal{H}_E^{\text{sim}})$.
- As done in [2, Theorem 3], we finally reduce the security of $\text{SIG}[\Sigma_{\text{SQInstructor}}]$ to the security of Problem 31 and Problem 30 via a game-hopping argument.

First step. We check the hypothesis from Theorem 34. By Theorem 16 we know that $\Sigma_{\text{SQInstructor}}$ is special-sound with respect to R_{OneEnd_p} , also the challenge space is by definition of size $[\text{GL}_2(\mathbb{Z}/N) : \Gamma] \geq 2^\lambda$. Also, since the generation of the commitment curve E_{com} is the same as in the Σ_{SQI} protocol, by [2, Lemma 4.1] we have that $\text{MinEnt}\Sigma_{\text{SQInstructor}} \leq p^{-\frac{1}{2}}$. Finally, we need to prove that $\Sigma_{\text{SQInstructor}}$ has $\mathcal{H}_E^{\text{sim}}$ -hint-assisted wHVZK, for this we provide a simulator $\text{Sim}_{\Sigma_{\text{SQInstructor}}}$ in Algorithm 11 and prove that its output is undistinguishable from the real protocol. It is clear that the challenge matrix is uniform in both the real and the simulated protocol. Without considering the rejecting of commitment without short odd degree isogenies, by [2, Proposition 2.4], the distribution of $j(E_{\text{com}})$ are statistically close. The torsion points $P_{\text{com}}, Q_{\text{com}}$ are sampled uniformly in both cases (note that in the real case they are randomized via M_{com} and in the simulated one via the uniform matrix M), also we are rejecting in the both cases the same subset of level structures, i.e. the ones such that $\text{Hom}(\mathbb{E}, \mathbb{E}')$ has no odd degree isogeny. Thus, these distributions are still statistically close, with distance bounded by $s \frac{1}{\sqrt{p}}$. With respect to the response information we remark that it is equivalent to the information given by the response isogeny φ_{rsp} and the uniformly random auxiliary isogeny $\varphi'_{\text{aux}} : E_{\text{pk}} \rightarrow E'_{\text{aux}}$. Note that in both cases they are both sampled from the same distribution: for the former the odd degree isogenies in $\text{Hom}(\mathbb{E}, \mathbb{E}')$ while for the latter they are uniformly random between the isogenies of the same degree. We conclude that $\text{Adv}_{\Sigma_{\text{SQInstructor}}, \mathcal{H}_E^{\text{sim}}, \text{Sim}_{\Sigma_{\text{SQInstructor}}}}^{\text{hint-wHVZK}}(\mathcal{A}, q) \leq s \frac{1}{\sqrt{p}}$ and we can apply Theorem 34.

Second step. As a consequence of the first step and by Theorem 34, we have that for any PPT algorithm $\mathcal{A}$ against the EUF-CMA of $\text{SIG}[\Sigma_{\text{SQInstructor}}]$, there

Algorithm 11 Simulator $\text{Sim}_{\Sigma_{\text{SQInstructor}}}$ for $\Sigma_{\text{SQInstructor}}$

Input: The public parameters for $\Sigma_{\text{SQInstructor}}$, the curve E_{pk} and a hint $h = (M, \varphi_{\text{rsp}}, \varphi'_{\text{aux}}) \in \mathcal{H}_{E_{\text{pk}}}^{\text{sim}}$ with $\varphi_{\text{rsp}} : E_{\text{pk}} \rightarrow E_{\text{com}}$ and $\varphi_{\text{aux}} : E_{\text{com}} \rightarrow E_{\text{aux}}$.

Output: Transcript of $\Sigma_{\text{SQInstructor}}$.

- 1: $P_{\text{pk}}, Q_{\text{pk}}$ a deterministic basis of $E_{\text{pk}}[N]$;
 - 2: sample $\gamma \leftarrow \Gamma$;
 - 3: $\begin{pmatrix} P_{\text{com}} \\ Q_{\text{com}} \end{pmatrix} \leftarrow (\gamma \cdot M) \cdot \varphi_{\text{rsp}} \begin{pmatrix} P_{\text{pk}} \\ Q_{\text{pk}} \end{pmatrix}$;
 - 4: $\text{com} := (j(E_{\text{com}}), P_{\text{com}}, Q_{\text{com}})$ and $\text{ch} := M$.
 - 5: $d \leftarrow \deg(\varphi_{\text{rsp}})$, $a \leftarrow \lceil \log(d) \rceil$;
 - 6: $\varphi \leftarrow [\varphi_{\text{rsp}}]_* (\varphi'_{\text{aux}}) \circ \varphi_{\text{rsp}} : E_{\text{pk}} \rightarrow E_{\text{aux}}$;
 - 7: $(P_{\text{aux}}, Q_{\text{aux}}) \leftarrow ([d^{-1}] \varphi(P_{\text{pk}}), [d^{-1}] \varphi(Q_{\text{pk}}))$;
 - 8: $\text{rsp} := (a, E_{\text{aux}}, P_{\text{aux}}, Q_{\text{aux}})$;
 - 9: **return** $(\text{com}, \text{ch}, \text{rsp})$.
-

exists an expected polynomial time algorithm $\mathcal{E}$ such that

$$\begin{aligned} \text{Adv}_{\text{SIG}[\Sigma_{\text{SQInstructor}}]}^{\text{EUF-CMA}}(\mathcal{A}) &\leq (q+1) \cdot \text{Adv}_{R_{\text{OneEnd}_p}}^{\text{hintrel}, \mathcal{H}_E^{\text{sim}}}(\mathcal{E}, s) + \\ &\quad + (2q + s + 2) \frac{s}{\sqrt{p}} + \frac{q+1}{2^\lambda}. \end{aligned}$$

We can then repeat the same game-hopping argument from [2, Theorem 3] to conclude the proof. For this we construct $\mathcal{B}$ from $\mathcal{E}$ by simulating the hints from $\mathcal{H}_E^{\text{sim}}$ with $\mathcal{H}_E^{\text{unif}}$ instead. Any difference in the success probability between $\mathcal{B}$ and $\mathcal{E}$ is bounded by the advantage in solving Problem 31 with s queries. Thus we imply

$$\begin{aligned} \text{Adv}_{R_{\text{OneEnd}_p}}^{\text{hintrel}, \mathcal{H}_E^{\text{sim}}}(\mathcal{E}, s) &\leq \text{Adv}^{s\text{-hint-dist}}(\mathcal{A}) + \text{Adv}_{R_{\text{OneEnd}_p}}^{\text{hintrel}, \mathcal{H}_E^{\text{unif}}}(\mathcal{B}, s) \\ &\leq \text{Adv}^{s\text{-hint-dist}}(\mathcal{A}) + \text{Adv}^{s\text{-hint-OneEnd}_p}(\mathcal{B}) + \frac{1}{2\sqrt{p}}. \end{aligned}$$

The last inequality is due to the fact that for **hint-OneEnd_p** Problem we are considering a curve sampled from the stationary distribution instead so we need to account for the statistical distance between the two distributions, as done also in the proof of [2, Theorem 3]. $\square$

Hardness of distinguishing the hint distributions. As in [2], we argue that Problem 31 is computationally hard. Both the hint distributions, $\mathcal{H}_E^{\text{sim}}$ and $\mathcal{H}_E^{\text{unif}}$, provide a matrix M and two isogenies φ_1, φ_2 such that their degree sum to a power of 2. Actually both M and φ_2 are sampled uniformly in both the two distributions, so the only difference lie in the sampling of φ_1 . The distribution of φ_1 in both cases depends on the bound D_{rsp} , and for a large enough bound, the statistical distance between the two curves with level structure is negligible since we consider a level structure containing the scalar matrices [18]. Moreover, note that the set of curves with level structure $\mathbb{E}'$ excluded from $\mathcal{H}_E^{\text{sim}}$ is the same of the codomains of φ_1 in $\mathcal{H}_E^{\text{unif}}$ since for them we have by definition the existence of an odd degree isogeny from $\mathbb{E}$ to $\mathbb{E}'$.

*Remark 35 (Differences q -**hint-dist** in [2]).* In [2, Problem 3] the authors consider an hint distribution statistically close to the real one and the pushforward of hints sampled from a uniform hint distribution $\mathcal{H}_E^{\text{unif}}$ through cyclic powersmooth degree isogenies. Since for our protocol there is no challenge isogeny involved, only a level structure, there is no third curve involved and we can directly consider the uniform distribution $\mathcal{H}_{E_{\text{pk}}}^{\text{unif}}$ to sample the hints. Also, we argue that the use of a level structure does not fundamentally change the hardness of distinguishing the two distributions, as discussed in Section 3.2 the lattice $\text{Hom}(\mathbb{E}, \mathbb{E}')$ is a sublattice of $\text{Hom}(E, E')$ enjoying similar properties. Moreover, as already noted the curve with level structures rejected in Item a. can be made negligible.