# Unconditional foundations for supersingular isogeny-based cryptography

Arthur Herlédan Le Merdy[0009−0007−6116−6863] and
Benjamin Wesolowski[0000−0003−1249−6077]

ENS de Lyon, CNRS, UMPA, UMR 5669, Lyon, France

**Abstract.** In this paper, we prove that the supersingular isogeny problem (Isogeny), endomorphism ring problem (EndRing) and maximal order problem (MaxOrder) are equivalent under probabilistic polynomial time reductions, unconditionally.
Isogeny-based cryptography is founded on the presumed hardness of these problems, and their interconnection is at the heart of the design and analysis of cryptosystems like the SQIsign digital signature scheme. Previously known reductions relied on unproven assumptions such as the generalized Riemann hypothesis. In this work, we present unconditional reductions, and extend this network of equivalences to the problem of computing the lattice of all isogenies between two supersingular elliptic curves (HomModule).
For cryptographic applications, one requires computational problems to be hard *on average* for random instances. It is well-known that if Isogeny is hard (in the worst case), then it is hard for random instances. We extend this result by proving that if any of the above-mentionned classical problems is hard in the worst case, then all of them are hard on average. In particular, if there exist hard instances of Isogeny, then all of Isogeny, EndRing, MaxOrder and HomModule are hard on average.

**Keywords:** Isogeny-based cryptography · Cryptanalysis · Endomorphism ring · Isogeny path · Supersingular elliptic curve

## 1 Introduction

Isogeny-based cryptography, a branch of post-quantum cryptography, rests on the presumed hardness of a few interconnected computational problems: variations around the supersingular *isogeny problem* (Isogeny) or the *endomorphism ring problem* (EndRing). A collection of "fundamental problems" has grown with our understanding of the field and with the needs of new cryptosystems. Some, like OneEnd are well-suited for security proofs, their hardness serving as a lower bound on the security of cryptographic schemes. Others, like EndRing, are better suited for attacks, thereby serving as upper bounds on the security. And some, like MaxOrder, reframe these problems in a radically different language, deepening our understanding of the field.

Connecting these problems, proving computational reductions, or even equivalences, has thus become a central and fruitful line of research. Most notably, the equivalence between the isogeny problem and the endomorphism ring problem [10,28] motivated the design of *SQIsign* [9], today the most compact post-quantum digital signature scheme.

While all these fundamental problems are considered to be equivalent, only few of the computational reductions linking them are fully, unconditionally proven. Almost all previously-known results rely on an unproven assumption: the generalized Riemann hypothesis (GRH). In this paper, we prove that all the aforementioned problems, and more, are in fact equivalent under classical, probabilistic polynomial time reductions, unconditionally.

### 1.1 Contribution

The main results of this paper are Theorem 1.1 and Theorem 1.2 below. Theorem 1.1, summarized in Figure 1, establishes the *unconditional* equivalence of fundamental problems of isogeny-based cryptography. Theorem 1.2 establishes their average-case hardness: if any of them is hard in the worst case, then all of them are hard on average, for uniformly random instances.

Let us start by informally introducing the computational problems at hand. Formal definitions are provided in Section 2.5. The central objects of interest are so-called *supersingular elliptic curves*. *Isogenies* are morphisms between elliptic curves. *Endomorphisms* of an elliptic curve $E$ are isogenies from $E$ to itself; they form a ring, written $\mathrm{End}(E)$.

- OneEnd (the One Endomorphism problem): Given a supersingular elliptic curve $E$, find an endomorphism that is not a scalar multiplication, i.e., an element of $\mathrm{End}(E) \setminus \mathbb{Z}$.
- EndRing (the Endomorphism Ring problem): Given a supersingular elliptic curve $E$, compute a basis of the endomorphism ring $\mathrm{End}(E)$.
- Isogeny (the Isogeny problem): Given two supersingular elliptic curves $E$ and $E'$, find an isogeny from $E$ to $E'$.
- $\ell$-IsogenyPath (the $\ell$-Isogeny Path problem): Given two supersingular elliptic curves $E$ and $E'$, and a prime number $\ell$, find an isogeny $E \to E'$ of degree a power of $\ell$ (i.e., an $\ell$-isogeny path from $E$ to $E'$).
- HomModule (the Homomorphism Module problem): Given two supersingular elliptic curves $E$ and $E'$, compute a basis of the lattice $\mathrm{Hom}(E, E')$ of all isogenies from $E$ to $E'$. This problem has received very little attention so far. It appears to have never been formally introduced in the literature, yet has implicitly played a role.
- MaxOrder (the Maximal Order problem): Given a supersingular elliptic curve $E$, find some "abstract ring" $\mathcal{O}$ isomorphic to $\mathrm{End}(E)$. More precisely, $\mathrm{End}(E)$ is known to be isomorphic to a *maximal order* $\mathcal{O}$ in a quaternion algebra $B_{p,\infty}$. The MaxOrder problem asks to find an order in $B_{p,\infty}$ isomorphic to $\mathrm{End}(E)$. To resolve an ambiguity in previous literature (see Section 3), we formalize two variants: MaxOrder, where the solver is free to

choose his own model for $B_{p,\infty}$, and MaxOrder$_{\mathcal{Q}}$, where the solution has to be in a model specified by an algorithm $\mathcal{Q}$.
– MOER (the Maximal Order and Endomorphism Ring problem): Given a supersingular elliptic curve $E$, compute a basis of the endomorphism ring $\mathrm{End}(E)$, together with an isomorphism with an order in the quaternion algebra $B_{p,\infty}$.

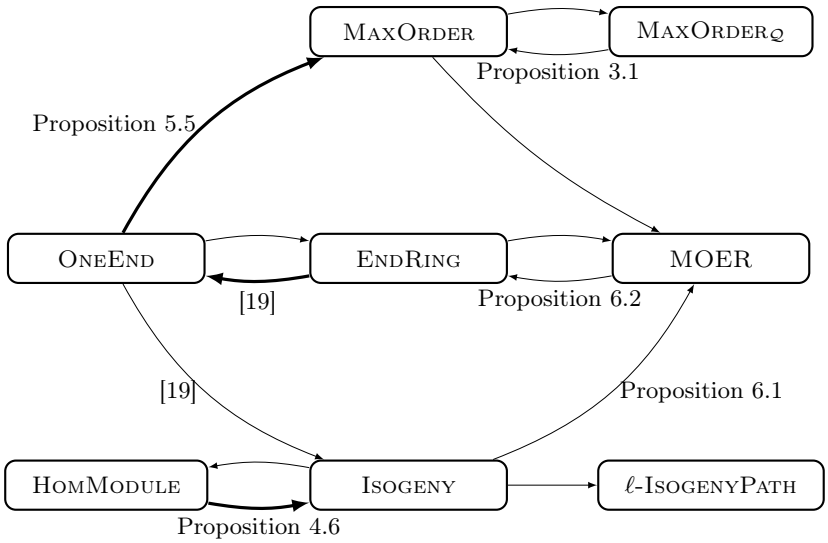


**Fig. 1.** Summary of the relations between fundamental isogeny-based problems. All arrows are unconditional classical polynomial time reductions. Thin arrows have a $O(1)$ query-complexity, and thick arrows have a $\mathrm{polylog}(p)$ query-complexity. Reductions with no reference are trivial, and all others are proved in the associated reference. Reductions involving MaxOrder$_{\mathcal{Q}}$ require oracle access to $\mathcal{Q}$.

**Theorem 1.1.** *The problems* Isogeny*,* EndRing*,* OneEnd*,* MOER*,* MaxOrder*,* MaxOrder$_{\mathcal{Q}}$ *and* HomModule *are all equivalent under probabilistic polynomial time reductions. Reductions involving* MaxOrder$_{\mathcal{Q}}$ *require oracle access to* $\mathcal{Q}$*.*

**Map of the proof of Theorem 1.1** The strategy consists in proving the computational reductions exhibited in Figure 1. Each arrow represents a computational reduction, and comes with a pointer to the proof. Note that our unconditional reductions are substantially different from the existing conditional reductions. To eliminate any reliance on GRH, we avoid all arguments that rely on the "good" distribution of numbers represented by quadratic forms. This

forbids us from using the powerful tools of KLPT-type algorithms [12]. In particular, we need to construct different "paths" in the network of reductions, and develop new types of arguments. We prove the reductions in the following order.

- The novel distinction between the two computational problems MaxOrder and $\text{MaxOrder}_{\mathcal{Q}}$ is discussed in Section 3. Their equivalence, proved in Proposition 3.1, hinges on a recent result [7, Proposition 4.1] to compute isomorphisms between quaternion algebras, when some maximal orders are known in each.
- The HomModule problem is the object of Section 4, where we prove that it reduces to Isogeny. Given two curves $E_1$ and $E_2$, the strategy is the following. First, we exploit the reduction from EndRing to Isogeny proved in [19] to compute bases of $\mathrm{End}(E_1)$ and $\mathrm{End}(E_2)$. Then, we solve Isogeny again to find some $\varphi : E_1 \to E_2$. Through algebraic arguments, we prove that one can extract a basis of $\mathrm{Hom}(E_1, E_2)$ from the data of $\mathrm{End}(E_1)$, $\mathrm{End}(E_2)$, and $\varphi$.
- The reduction from OneEnd to MaxOrder is the object of Section 5. Navigating between a problem which deals with endomorphisms (like OneEnd) and another which deals with purely quaternionic data (like MaxOrder) typically requires to connect instances to some special elliptic curve $E_0$ for which both $\mathrm{End}(E_0)$ and its embedding in the quaternions are already known. This curve $E_0$ provides an "endomorphism/quaternion" dictionary. Without GRH, there is no guarantee that a special curve $E_0$ can be found. We thus need to develop a new strategy. To reduce OneEnd (say on some input $E$) to MaxOrder, we solve MaxOrder on $E$ and on a few "close neighbours" of $E$. Doing so, we construct a "local" correspondence between neighbours of $E$ and quaternionic orders, and we prove that from enough such "local" information, we can reconstruct a full "endomorphism/quaternion" dictionary.
- The reduction from Isogeny to MOER is the object of Proposition 6.1. This reduction hinges on recent advances in isogeny-based cryptography facilitating the conversion of ideals in quaternionic orders into the corresponding isogenies [18].
- Finally, the reduction from MOER to EndRing is the object of Proposition 6.2. Of all the reductions, this one resembles the most closely an existing reduction: the reduction from MaxOrder to EndRing in [10,28]. However, these former reductions required GRH to provably avoid hard factorisations. Instead, we show that no factorisation is needed if we are free to choose our own model $(\frac{a,b}{\mathbb{Q}})$ for the quaternion algebra. The parameters $a$ and $b$ are possibly hard to factor, but it does not matter: the result [7, Proposition 4.1] allows one to convert the solution to more standard models without factoring.

**Discussion of Theorem 1.1 and comparison with previous work.** The former state of the art is summarized in Figure 2. We make the following observations.

– The HomModule problem is absent from Figure 2: its relation to other problems was never studied before.
– The MOER problem is also absent, yet it is folklore that, assuming GRH, the reductions of [28] also extend to MOER.
– Reflecting previous litterature, Figure 2 makes no distinction between the problems MaxOrder and $\text{MaxOrder}_{\mathcal{Q}}$. Indeed, this distinction is only useful if one refuses to believe in GRH (see Section 3).
– There remains one reduction which is only known conditionally on GRH: the reduction from $\ell$-IsogenyPath to EndRing (or to any other problem in our list). Indeed, by definition, $\ell$-IsogenyPath asks to find isogenies with degree of a prescribed form. The study of isogenies of prescribed degree closely relates to the study of integers represented by certain quadratic forms. GRH has a consequential impact on the distribution of integers represented by quadratic forms, and currently known unconditional results seem insufficient for the study of $\ell$-IsogenyPath. [1]

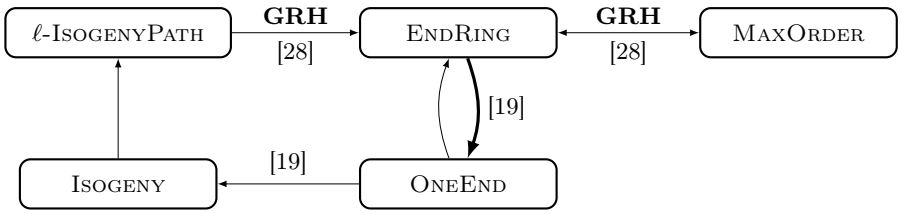


**Fig. 2.** Former state of the art of (conditional) reductions between foundational problems of isogeny-based cryptography. All arrows are classical polynomial time reductions. Thin arrows have a $O(1)$ query-complexity, and the thick arrow has a $\text{polylog}(p)$ query-complexity. Reductions with no reference are trivial, and all others are proved in the associated reference. The **GRH** label signifies that a reduction assumes the Generalized Riemann Hypothesis.

Theorem 1.1 implies that if hard instances exist for any one of the listed problems, then hard instances must exist for all of them. However, the security of isogeny-based schemes typically relies on the presumed hardness of *random instances* of these problems. These random instances often follow a "natural" distribution called the *stationary distribution* (see Definition 2.15 — note that it is statistically indistinguishable from the uniform distribution). This distribution emerged from the use of random walks as early as the Charles–Goren–Lauter hash function [6], and up to the latest advances on the SQIsign digital signature scheme [8,3]. We are thus interested in the hardness of the *average case* of the

[1] Note that an attempt at replacing the GRH assumption with a factoring oracle is presented in [15]. A mistake in the proof has been reported, but if it can be fixed, it would link $\ell$-IsogenyPath to the other problems under unconditional polynomial time *quantum* reductions.

fundamental problems (see Definition 2.19), with respect to the stationary (or uniform) distribution.

The following Theorem 1.2 says that there are *worst-case to average-case* reductions between all of these problems. In particular, if there exists even a single hard instance for any of the listed problems, then all of the problems are hard on average — a powerful statement for security analysis.

**Theorem 1.2.** *For any pair of problems* $(P, Q)$ *chosen from the problems* Isogeny*,* EndRing*,* OneEnd*,* MOER*,* MaxOrder*,* $\text{MaxOrder}_{\mathcal{Q}}$*,* HomModule*, and* $\ell$-IsogenyPath *there exists a probablistic polynomial time worst-case to average-case reduction from* $P$ *to* $Q$*. All reductions hold unconditionally, with the two following exceptions which require the generalized Riemann hypothesis:*

- *if* $P = \ell$-IsogenyPath*, or*
- *if* $Q \in \{\text{MaxOrder}, \text{MaxOrder}_{\mathcal{Q}}\}$ *and* $p \equiv 1 \bmod 8$*.*

*Reductions involving* $\text{MaxOrder}_{\mathcal{Q}}$ *require oracle access to* $\mathcal{Q}$*.*

**Map of the proof of Theorem 1.2** The strategy, carried out in Section 7, consists in proving that the worst-case OneEnd problem reduces to the average case of any other problem in the list. The precise network of reductions is summarized in Figure 3, page 26. We conclude from the fact, established in Theorem 1.1, that the worst case of any problem in the list reduces to a worst-case OneEnd instance (except for $P = \ell$-IsogenyPath, which relies on the conditional reduction of [28]).

**Discussion of Theorem 1.2 and comparison with previous work.** Some of the worst-case to average-case reductions between the problems of interest are already folklore. It is well known, for instance, that random walks in $\ell$-isogeny graphs can be used to re-randomize an instance of the $\ell$-IsogenyPath, leading naturally to a self-reduction. This straightforward approach extends to other cases, but is not sufficient to obtain the full network of reductions proved in Theorem 1.2. For instance, the reduction from the worst-case OneEnd problem to the average case Isogeny, HomModule or $\ell$-IsogenyPath problems is obtained by modifying a worst-case reduction proposed in [19]. The reduction from the worst-case OneEnd problem to the average case MaxOrder or $\text{MaxOrder}_{\mathcal{Q}}$ problems relies on recent advances facilitating the conversion between ideals and isogenies and the division of isogenies.

### 1.2 Acknowledgements

The authors would like to thank Travis Morrison for fruitful discussions, and for bringing our attention to [7, Proposition 4.1], which simplified and improved some of the results of this paper. The authors were supported by the Agence Nationale de la Recherche under grants ANR-22-PETQ-0008 (PQ-TLS) and ANR-22-PNCQ-0002 (HQI), and the European Research Council under grant No. 101116169 (AGATHA CRYPTY).

## 2 Preliminaries

### 2.1 Notation

We write $\mathbb{Z}$ for the ring of integers and $\mathbb{Q}$ for the field of rational numbers. For any prime power $q$, we write $\mathbb{F}_q$ for the finite field with $q$ elements. For any set $S$, we denote by $\#S$ its cardinality. For any field $K$, we write $\overline{K}$ for its algebraic closure. We write $f = O(g)$ for the classic big O notation, and use the soft O notation $\tilde{O}(g) = \log(g)^{O(1)} \cdot O(g)$. We also write $\mathrm{poly}(f_1, \ldots, f_n) = (f_1 + \cdots + f_n)^{O(1)}$. The function log is in base 2. For any ring $R$, we write $R^\times$ for its group if invertible elements, and $M_2(R)$ for the ring of $2 \times 2$ matrices with coefficients in $R$.

### 2.2 Quaternion algebras

See [26] for a detailed reference on quaternion algebras. For any $a, b \in \mathbb{Q}^\times$, the *quaternion algebra* $B = (\frac{a,b}{\mathbb{Q}})$ is a ring generated by a $\mathbb{Q}$-basis $(1, i, j, k)$ satisfying the multiplication rules

$$i^2 = a, j^2 = b, k = ij = -ji.$$

In this article, we only consider quaternion algebra of this form. For any prime $p$, we say that $B$ is *ramified at* $p$ if $B \otimes \mathbb{Q}_p \ncong M_2(\mathbb{Q}_p)$. It is *ramified at* $\infty$ if $B \otimes \mathbb{R} \ncong M_2(\mathbb{R})$. We write $B_{p,\infty}$ for a quaternion algebra (unique up to isomorphism) ramified at $p$ and $\infty$ (and unramified at all other primes).

**Lemma 2.1 ([20]).** *Let $p > 2$ be a prime. Then, $B_{p,\infty} \cong \left(\frac{-q,-p}{\mathbb{Q}}\right)$, where*

$$q = \begin{cases} 1 & \text{if } p \equiv 3 \bmod 4, \\ 2 & \text{if } p \equiv 5 \bmod 8, \\ q_p & \text{if } p \equiv 1 \bmod 8, \end{cases}$$

*where $q_p$ is any prime such that $q_p \equiv 3 \bmod 4$ and $\left(\frac{p}{q_p}\right) = -1$.*

Note that if GRH is true, when $p \equiv 1 \bmod 8$, the smallest suitable $q_p$ satisfies $q_p = O((\log p)^2)$ (this follows from [13], see also [10, Proposition 1]).

Let $B$ be a quaternion algebra. The canonical involution

$$\overline{a + ib + jc + kd} \longmapsto a - ib - jc - kd$$

induces the *reduced trace* $\mathrm{Trd}(\alpha) = \alpha + \overline{\alpha}$ and the *reduced norm* $\mathrm{Nrd}(\alpha) = \alpha\overline{\alpha}$. The reduced norm is a quadratic form on $B$, with the associated bilinear form

$$\langle \alpha, \beta \rangle = \frac{1}{2} \mathrm{Trd}(\alpha\overline{\beta}) = \frac{1}{2} \left( \mathrm{Nrd}(\alpha + \beta) - \mathrm{Nrd}(\alpha) - \mathrm{Nrd}\, \beta \right).$$

When $B$ is ramified at $\infty$, the reduced norm is positive definite.

A *quadratic space* is a $\mathbb{Q}$-vector space $V$ of finite dimension $d$ together with a (positive definite) quadratic form $f : V \to \mathbb{Q}$. A *lattice* in $V$ is a subgroup $\Lambda \subset V$ of rank $d$ such that $V = \mathbb{Q}\Lambda$. Given a $\mathbb{Z}$-basis $(b_i)_{i=1}^d$ of a lattice $\Lambda$, its *Gram matrix* is $G = (\langle b_i, b_j \rangle)_{i,j=1}^d$. The *volume* of the lattice is $\mathrm{Vol}(\Lambda) = \sqrt{|\det(G)|}$, where $G$ is the Gram matrix of any basis of $\Lambda$. The *discriminant* of $\Lambda$ is $\mathrm{disc}(\Lambda) = 16\mathrm{Vol}(\Lambda)^2$.

An *order* in a quaternion algebra $B$ is a subring $\mathcal{O} \subset B$ that is also a lattice. It is a *maximal order* if it is not contained in any other order. Maximal orders in $B_{p,\infty}$ have $\mathrm{Vol}(\mathcal{O}) = p/4$.

The following proposition shows that given maximal orders, one can efficiently compute an isomorphism between different models of $B_{p,\infty}$.

**Proposition 2.2.** *[7, Proposition 4.1] Let $A, B$ be quaternion algebras isomorphic to $B_{p,\infty}$. Given $\mathcal{O}_A$ a maximal order in $A$ and $\mathcal{O}_B$ a maximal order in $B$, one can compute an isomorphism between $A$ and $B$ in polynomial time.*

For any lattice $\Lambda \subset B$, its *left order* and *right order* are the orders

$$\mathcal{O}_L(\Lambda) = \{\alpha \in B \mid \alpha\Lambda \subseteq \Lambda\}, \quad \text{and } \mathcal{O}_R(\Lambda) = \{\alpha \in B \mid \Lambda\alpha \subseteq \Lambda\}.$$

If $\mathcal{O}$ is a maximal order, and $I$ is a left ideal in $\mathcal{O}$, then $\mathcal{O}_L(I) = I$, and $\mathcal{O}_R(I)$ is another maximal order. The *connecting ideal* of two maximal order $\mathcal{O}_1$ and $\mathcal{O}_2$ is the lattice

$$I(\mathcal{O}_1, \mathcal{O}_2) = \{\alpha \in B \mid \alpha\mathcal{O}_2\overline{\alpha} \subseteq [\mathcal{O}_2 : \mathcal{O}_1 \cap \mathcal{O}_2]\mathcal{O}_1\}.$$

It is a left $\mathcal{O}_1$-ideal and a right $\mathcal{O}_2$-ideal.

Let $I$ be a left ideal in a maximal order $\mathcal{O}$. Its *reduced norm* is $\mathrm{Nrd}(I) = \gcd(\mathrm{Nrd}(\alpha) \mid \alpha \in I) = \sqrt{\#(\mathcal{O}/I)}$. Its *normalized quadratic form* is the integral quadratic form

$$q_I : I \longrightarrow \mathbb{Z} : \alpha \longmapsto \frac{\mathrm{Nrd}(\alpha)}{\mathrm{Nrd}(I)}.$$

In $B_{p,\infty}$, the volume of $I$ with respect to this quadratic form is $p/4$.

### 2.3 Elliptic curves

See [24] for a detailed reference on elliptic curves. An *elliptic curve* is an abelian variety of dimension 1. Given a field $k$ of characteristic $p > 3$, an elliptic curve $E$ can be described by a short Weierstrass equation $y^2 = x^3 + ax + b$ for $a, b \in k$ with $4a^3 + 27b^2 \neq 0$. The *$k$-rational points* of $E$ is the set $E(k)$ of pairs $(x, y) \in k^2$ satisfying the curve equation, together with a point $\infty_E$ 'at infinity'. They form an abelian group, written additively, where $\infty_E$ is the neutral element.

Given two elliptic curves $E_1$ and $E_2$ defined over $k$, an isogeny $\varphi : E_1 \to E_2$ is a non-constant rational map which is also a group homomorphism from $E_1(\overline{k})$ to $E_2(\overline{k})$. The *kernel* $\ker(\varphi)$ is a finite subgroup of $E_1(\overline{k})$. The *degree* $\deg(\varphi)$ is its degree as a rational map. An *isomorphism* is an isogeny of degree 1.

For any integer $m$, the multiplication-by-$m$ map $[m] : E \to E$ is an isogeny. For any isogeny $\varphi : E \to E'$, its *dual* is the unique isogeny $\hat{\varphi} : E' \to E$ such that $\hat{\varphi} \circ \varphi = [\deg(\varphi)]$.

The isogeny $\varphi$ is *separable* if $\deg(\varphi) = \#\ker(\varphi)$, and *inseparable* otherwise. The isogeny is *purely inseparable* if $\ker(\varphi)$ is trivial (note that an isogeny is an isomorphism if and only if it is both separable and purely inseparable). For any finite subgroup $G \subset E(\overline{k})$, there exists a separable isogeny $\varphi : E \to E/G$ with $\ker(\varphi) = G$ (and $\varphi$ is unique up to an isomorphism of the target).

If $k$ has characteristic $p > 0$, the map $\phi_{p^n}^E : E \to E^{(p^n)} : (x, y) \mapsto (x^{p^n}, y^{p^n})$ is the $p^n$-*Frobenius isogeny*. For any isogeny $\varphi : E \to E'$, there is a maximal integer $n$ such that $\varphi$ factors as $\varphi = \psi \circ \phi_{p^n}^E$. Then, $\psi$ is separable. The isogenies $\phi_{p^n}^E$ are *purely inseparable*.

If $\varphi$ is separable and $\deg(\varphi) = \ell$ is prime, we say that $\varphi$ is an $\ell$-isogeny.

An *endomorphism* of $E$ is an isogeny $E \to E$. Endomorphisms, together with the zero morphism, form the *endomorphism ring* $\mathrm{End}(E)$. The curve $E$ is *supersingular* when $\mathrm{End}(E)$ is a lattice of rank 4. Then, $\mathrm{End}(E) \otimes \mathbb{Q}$ is isomorphic to the quaternion algebra $B_{p,\infty}$, and $\mathrm{End}(E)$ is a maximal order. The degree map $\deg : \mathrm{End}(E) \to \mathbb{Z}$ coincides with the reduced norm of the algebra.

We write $\mathrm{SS}_p$ for the set of $\overline{\mathbb{F}}_p$-isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$. We have $\#\mathrm{SS}_p = \lfloor p/12 \rfloor + \varepsilon$, with $\varepsilon \in \{0, 1, 2\}$, and all supersingular elliptic curves have a model over $\mathbb{F}_{p^2}$.

The Deuring correspondence highlights a deep connection between supersingular elliptic curves and maximal orders in the quaternion algebra $B_{p,\infty}$. Indeed, for any supersingular $E/\mathbb{F}_{p^2}$, we have that $\mathrm{End}(E)$ is a maximal order in the algebra $\mathrm{End}(E) \otimes \mathbb{Q} \simeq B_{p,\infty}$. For any isogeny $\varphi : E \to E'$, we have a left ideal

$$I_\varphi = \mathrm{Hom}(E', E) \circ \varphi \subseteq \mathrm{End}(E),$$

and the right order $\mathcal{O}_R(I_\varphi)$ is isomorphic to $\mathrm{End}(E')$. Any non-zero left ideal $I$ in $\mathrm{End}(E)$ is of this form, and we write $\varphi_I : E \to E_I$ for the corresponding isogeny. We thus have a bijection $\varphi \mapsto I_\varphi$ (with inverse $I \mapsto \varphi_\varphi$) between

- Isogenies from $E$ (up to isomorphism of the target), and
- Left ideals in $\mathrm{End}(E)$.

Furthermore, for any $\varphi : E \to E'$, the lattice $I_\varphi$ (with its normalized quadratic form $q_{I_\varphi}$) is isomorphic to $\mathrm{Hom}(E, E')$ (with the quadratic form deg).

### 2.4 Isogeny algorithms

There are several ways to encode an isogeny. In computational questions involving isogenies, we typically do not care how an isogeny is encoded, at long as it is an *efficient representation*: an encoding that allows to store and evaluate the isogeny $\varphi$ in polynomial time in $\log(\deg(\varphi))$.

**Definition 2.3 (Efficient representation, following [29, Definition 1.3]).** *Let $\mathcal{A}$ be a polynomial time algorithm. It is an* efficient isogeny evaluator *if for any $D \in \{0,1\}^*$ such that $\mathcal{A}(\texttt{validity}, D)$ outputs $\top$, there exists an isogeny $\varphi : E \to E'$ (defined over some finite field $\mathbb{F}_q$) such that:*

1. *on input $(\texttt{curves}, D)$, $\mathcal{A}$ returns $(E, E')$,*
2. *on input $(\texttt{degree}, D)$, $\mathcal{A}$ returns $\deg(\varphi)$,*
3. *on input $(\texttt{eval}, D, P)$ with $P \in E(\mathbb{F}_{q^k})$, $\mathcal{A}$ returns $\varphi(P)$.*

*If furthermore $D$ is of polynomial size in $\log(\deg \varphi)$ and $\log q$, then $D$ is an* efficient representation *of $\varphi$ (with respect to $\mathcal{A}$).*

The break of SIDH [5,14,22] had a major consequence on the computation of isogenies: they can be interpolated. More precisely, one can compute an efficient representation of an isogeny given only its image on a sufficiently large subgroup of its domain. In this paper, we will use the following simplified version of this result.

**Proposition 2.4 (`IsogenyInterpolation` [23, Theorem 5.19]).** *Let $\varphi : E \to E'$ be an $n$-isogeny between supersingular elliptic curves defined over $\mathbb{F}_{p^2}$. Let $N > n$ be an integer coprime to $pn$ with prime power decomposition $\prod_{i=1}^{r} \ell_r^{e_r}$. Let $(P_1, Q_1, \ldots, P_r, Q_r)$ be a set of generators of the $N$-torsion $E[N]$ such that $(P_i, Q_i)$ is a basis of $E[\ell_i^{e_i}]$, for $i = 1, \ldots, r$.*

*Then, given $(P_1, Q_1, \ldots, P_r, Q_r, \varphi(P_1), \varphi(Q_1), \ldots, \varphi(P_r), \varphi(Q_r))$, one can compute an efficient representation of $\varphi$ in polynomial time in the length of the input and in the largest prime factor of $N$.*

Using this interpolation result, it was then proved that there is an efficient algorithm to divide isogenies. This application was first presented in [21] is some particular case, and later generalised in [16].

**Proposition 2.5 (`IsogenyDivision`, [21] and [16, Theorem 3]).** *Given an isogeny $\varphi : E_1 \to E_2$, where $E_1$ and $E_2$ are supersingular elliptic curves defined over $\mathbb{F}_{p^2}$, and an integer $n < \deg \varphi$, one can return an efficient representation of $\varphi/n$ if it is a well-defined isogeny, and return `False` otherwise, in time polynomial in $\log p$ and $\log \deg \varphi$.*

Finally, we will use a recent unconditional polynomial-time algorithm to translate $\mathcal{O}$-left ideals to corresponding isogenies, where $\mathcal{O}$ is a maximal order in a quaternion algebra isomorphic to $B_{p,\infty}$. It is a direct generalisation of the Clapoti algorithm [18] for computing class group action on oriented elliptic curves in polynomial time, even if the norm of the acting ideal is not smooth.

Translating Clapoti into a general IdealToIsogeny algorithm has been done in prior work, such as [3]. Notice that, for the sake of efficiency, the authors of [3] chose to use isogenies in dimension 2, which required assuming heuristics. In contrast, to obtain a rigorous polynomial-time algorithm, we consider the most direct generalisation of Clapoti, using abelian varieties of dimension 8.

**Proposition 2.6 (`IdealToIsogeny` [18]).** *Let $E$ be a supersingular elliptic curve defined over $\mathbb{F}_q$ such that an isomorphism $\varepsilon : \mathrm{End}(E) \simeq \mathcal{O}$ is known, where $\mathcal{O}$ is a maximal order in some quaternion algebra isomorphic to $B_{p,\infty}$. Given a left $\mathcal{O}$-ideal $I$, one can compute an efficient representation of the isogeny $\varphi_I : E \to E/E[I]$ in polynomial time in the length of the input.*

### 2.5 Computational problems

We now formally define the computational problems of interest. Every isogeny in the input or output of these problems is considered to be in efficient representation 2.3. The *supersingular isogeny problem* can then be simply expressed as follows.

*Problem 2.7 (*Isogeny*).* Given $E$ and $E'$ two supersingular elliptic curves defined over $\mathbb{F}_{p^2}$, compute an isogeny $\varphi : E \to E'$.

Instead of asking for a single isogeny, one can ask for the collection of all isogenies from $E$ to $E'$. As this collection is a lattice, the following problem asks to find a basis of this lattice.

*Problem 2.8 (*HomModule*).* Given two supersingular elliptic curves $E$ and $E'$ defined over $\mathbb{F}_{p^2}$, find four isogenies generating $\mathrm{Hom}(E, E')$ as a $\mathbb{Z}$-module.

It is often convenient to find an isogeny of a particular form. An *$\ell$-isogeny path* (of length $n$) from $E$ to $E'$ is a sequence of $\ell$-isogenies $\varphi_i : E_i \to E_{i+1}$ such that $E_0 = E$ and $E_n = E'$. Such a path provides an efficient representation of the degree $\ell^n$ composition $E \to E'$. The following version of the isogeny problem appeared as early as [6], when no general method was known for the efficient representation of arbitrary isogenies.

*Problem 2.9 ($\ell$-*IsogenyPath*).* Given $E$ and $E'$ two supersingular elliptic curves defined over $\mathbb{F}_{p^2}$, compute an $\ell$-isogeny path from $E$ to $E'$.

It soon appeared that the problem of finding isogenies is closely related to the problem of finding endomorphisms. Again, there are several ways to formalize it. The first asks to find a basis of the endomorphism ring.

*Problem 2.10 (*EndRing*).* Given a supersingular elliptic curve $E$ defined over $\mathbb{F}_{p^2}$, find four endomorphisms generating $\mathrm{End}(E)$ as a $\mathbb{Z}$-module.

Similarly to isogenies, we could ask to find a single endomorphism instead of the whole ring. But extra care is required: some endomorphisms are always easy to find: any scalar multiplication $[m]$ on $E$ is an endomorphism, forming the subring $\mathbb{Z} \subset \mathrm{End}(E)$.

*Problem 2.11 (*OneEnd*).* Given a supersingular elliptic curve $E$ defined over $\mathbb{F}_{p^2}$, find an endomorphism in $\mathrm{End}(E) \setminus \mathbb{Z}$.

Now, *computing the endomorphism ring of $E$* could be interpreted in a different way. Instead of finding actual endomorphisms of $E$ as in EndRing, one could ask for the abstract structure of $\mathrm{End}(E)$. Indeed, this ring is always isomorphic to a maximal order in $B_{p,\infty}$, and determining which is the following problem.

*Problem 2.12 (*MaxOrder*).* Given a supersingular elliptic curve $E$ defined over $\mathbb{F}_{p^2}$, find a quaternion algebra $B = (\frac{-a,-b}{\mathbb{Q}}) \simeq B_{p,\infty}$, together with four quaternions in $B$ generating a maximal order isomorphic to $\mathrm{End}(E)$.

Note that in previous work such as [10,28], the problem MaxOrder does not require finding a model $(\frac{-a,-b}{\mathbb{Q}})$ for $B_{p,\infty}$. Instead, they make the implicit assumption that a fixed model of the form $B_{p,\infty} = (\frac{-p,-q}{\mathbb{Q}})$ is used. Since there is no "canonical" model of $B_{p,\infty}$, we include the choice of a model in the definition of the problem. We discuss this subtlety in further detail in Section 3, where we prove that it does not actually matter: it is equivalent to the following problem where a model for $B_{p,\infty}$ of the same form as [10,28] is provided.

*Problem 2.13 (*$\text{MaxOrder}_{\mathcal{Q}}$*).* Let $\mathcal{Q}$ be an algorithm which for any prime number $p$, outputs a prime $q = \mathcal{Q}(p)$ such that $B_{p,\infty} \simeq (\frac{-p,-q}{\mathbb{Q}})$. The problem $\text{MaxOrder}_{\mathcal{Q}}$ is the following. Given a supersingular elliptic curve $E$ defined over $\mathbb{F}_{p^2}$, find four quaternions in $(\frac{-p,-\mathcal{Q}(p)}{\mathbb{Q}})$ generating a maximal order isomorphic to $\mathrm{End}(E)$.

As the EndRing problem asks to find actual endomorphisms generating $\mathrm{End}(E)$, and the MaxOrder problem asks to find the "quaternionic" structure of $\mathrm{End}(E)$, one can combine these two tasks as in the following problem.

*Problem 2.14 (*MOER*).* Given a supersingular elliptic curve $E$ defined over $\mathbb{F}_{p^2}$, find four endomorphisms $(\alpha_i)_{i=1}^4$ generating $\mathrm{End}(E)$ as a $\mathbb{Z}$-module, a quaternion algebra $B = (\frac{-a,-b}{\mathbb{Q}}) \simeq B_{p,\infty}$, and four quaternions $(\beta_i)_{i=1}^4$ in $B$ such that

$$\mathrm{End}(E) \otimes \mathbb{Q} \longrightarrow B : \alpha_i \longmapsto \beta_i$$

is an isomorphism.

### 2.6 Random walks

We will consider random processes in the set of supersingular elliptic curves. Let $\mathbb{C}^{\mathrm{SS}_p}$ be the set of functions $\mathrm{SS}_p \to \mathbb{C}$. We consider two natural distances on $\mathbb{C}^{\mathrm{SS}_p}$. First,

$$d_{\mathrm{TV}}(f,g) = \frac{1}{2}\|f-g\|_1 = \frac{1}{2}\sum_{E\in\mathrm{SS}_p} |f(E)-g(E)|.$$

When $f$ and $g$ are distributions on $\mathrm{SS}_p$, this is known as the *total variation distance*. Second, we have the scalar product

$$\langle f,g\rangle = \sum_{E\in\mathrm{SS}_p} f(E)\overline{g(E)}\#\mathrm{Aut}(E),$$

inducing the norm $\|f\| = \langle f, f\rangle^{1/2}$. Note that by the Cauchy-Schwarz inequality and Eichler's formula, for any $f, g$, we have

$$d_{\mathrm{TV}}(f,g) \leq \frac{\|f-g\|}{2}\left(\sum_{E\in \mathrm{SS}_p}\frac{1}{\#\mathrm{Aut}(E)}\right)^{1/2} = \frac{\|f-g\|}{2}\left(\frac{p-1}{24}\right)^{1/2}.$$

Given an elliptic curve $E$, a prime $\ell$ and an integer $k$, a random $\ell$-walk from $E$ of length $k$ is a random sequence $(\varphi_0, \ldots, \varphi_{k-1})$ sampled as follows:

1. Let $E_0 = E$,
2. For each $i$, let $G_i$ be a uniformly random subgroup of order $\ell$ in $E_i$, and let $E_{i+1} = E_i/G_i$
3. For each $i$, let $\varphi_i : E_i \to E_{i+1}$ be the quotient isogeny.

The curve $E$ is the *source* of the walk, and the codomain of $\varphi_{k-1}$ is called the *target* of the walk. Let $N$ be a positive integer with prime factorization $N = \prod_{i=1}^{t} \ell_i^{k_i}$. A random $N$-walk from $E$ is a sequence $(w_i)_{i=1}^{t}$ where

1. The source of $w_1$ is $E$,
2. Each $w_i$ is a random $\ell_i$-walk of length $k_i$, and
3. For each $i$, the target of $w_i$ is the source of $w_{i+1}$.

The *target* of the walk is the target of $w_t$. Note that the walk itself depends on an order of the prime factors of $N$, but the distribution of the target does not.

The following proposition states that random walks rapidly converge to the so-called *stationary distribution*.

**Definition 2.15.** *The* stationary distribution *on* $\mathrm{SS}_p$ *is the probability distribution defined by* $\mu(E) = \frac{24}{(p-1)\#\mathrm{Aut}(E)}$.

*Remark 2.16.* For any $p > 3$, the quantity $\#\mathrm{Aut}(E)$ is equal to 2 for all curves $E$ with two exceptions: if $j(E) = 1728$, then $\#\mathrm{Aut}(E) = 4$, and if $j(E) = 0$, then $\#\mathrm{Aut}(E) = 6$. Therefore, the total variation distance between the uniform distribution and the stationary distribution on $\mathrm{SS}_p$ is $O(1/p)$. In particular, the two distributions are statistically and computationally indistinguishable.

**Proposition 2.17.** *Let $N$ be a positive integer with prime factorization $N = \prod_{i=1}^{t} \ell_i^{k_i}$. Let $E$ be a random supersingular elliptic curve defined over $\mathbb{F}_{p^2}$, for some distribution $f$. Let $W_N(f)$ be the distribution of the target of a random $N$-walk from $E$. Then,*

$$\|W_N(f) - \mu\| \leq \|f - \mu\| \cdot \prod_{i=1}^{t}\left(\frac{2\sqrt{\ell_i}}{\ell_i+1}\right)^{k_i},$$

*where $\mu$ is the stationary distribution.*

*Proof.* This is a folklore consequence of Pizer's proof that the supersingular $\ell$-isogeny graph is Ramanujan [20]. However, previous literature only details the case where $N$ is a prime power, so let us show that it extends to the general case. Following [19, Appendix A.1], let $W_\ell = B_\ell/(\ell+1)$ be the $\ell$-walk operator in $X$: for any distribution $f$ on $\mathrm{SS}_p$, we have that $W_\ell^k(f)$ is the distribution of the target of a random $\ell$-walk of length $k$. From [19, Appendix A.1] and [19, Theorem 3.10], we have $\|W_\ell^k(f) - \mu\| \leq \frac{2\sqrt{\ell}}{\ell+1}\|f-\mu\|$. We deduce that

$$\|W_N(f) - \mu\| = \|(W_{\ell_1}^{k_1} \circ \cdots \circ W_{\ell_t}^{k_t})(f) - \mu\| \leq \|f-\mu\| \cdot \prod_{i=1}^{t} \left(\frac{2\sqrt{\ell_i}}{\ell_i+1}\right)^{k_i},$$

as claimed. □

In our applications, we only need the following corollary, where we introduce a useful notation $\tau(p,\varepsilon)$ for the subsequent proofs.

**Corollary 2.18.** *Let $E$ be a random supersingular elliptic curve defined over $\mathbb{F}_{p^2}$, for some distribution $f$, and let $\varepsilon > 0$. There exists a bound $\tau(p,\varepsilon) = O(\log(p) - \log(\varepsilon))$ such that for any $N > 2^{\tau(p,\varepsilon)}$, the output distribution of a random $N$-walk is at total variation distance at most $\varepsilon$ to the stationary distribution.*

*Proof.* By [2, Theorem 7, Item 5], we have $\|f-\mu\| \leq \sqrt{3}$. Let $\lambda = \log(3/(2\sqrt{2}))$. From Proposition 2.17, we have

$$\|W_N(f) - \mu\| \leq \|f-\mu\| \cdot \prod_{i=1}^{t} \left(\frac{2\sqrt{\ell_i}}{\ell_i+1}\right)^{k_i} \leq \sqrt{3} \cdot \left(\frac{2\sqrt{2}}{3}\right)^{\log(N)} = \sqrt{3} \cdot 2^{-\lambda \log(N)}.$$

Now,

$$d_{\mathrm{TV}}(W_N(f), \mu) \leq \frac{\|W_N(f) - g\|}{2} \left(\frac{p-1}{24}\right)^{1/2} \leq 2^{-\lambda \log(N)} \left(\frac{p-1}{24}\right)^{1/2}.$$

The latter quantity is smaller than $\varepsilon$ if and only if

$$\log(N) \geq \frac{\lambda}{2}\left(\log(p-1) - \log(24) - 2\log(\varepsilon)\right) = O(\log(p) - \log(\varepsilon)),$$

which proves the result. □

Thanks to the concepts introduced in this section, we can now properly define *average-case* problems.

**Definition 2.19.** *Let $P$ be a problem from the list* $\ell$-IsogenyPath, Isogeny, EndRing, OneEnd, MOER, MaxOrder, MaxOrder$_{\mathcal{Q}}$ *and* HomModule. *The input of the problem $P$ consists of one or two supersingular elliptic curves defined over $\mathbb{F}_{p^2}$. We define the* average-case *for $P$ as the case where the input curves are drawn from the stationary distribution on $\mathrm{SS}_p$.*

## 3 The Maximal Order problem

In this section, we discuss the MaxOrder problem, and a subtlety in its definition when one does not assume GRH. The classical definition makes the implicit assumption that a reference quaternion algebra $B_{p,\infty}$ is provided. However, there is no "canonical" model of $B_{p,\infty}$. When $p \equiv 3 \bmod 4$ (respectively $p \equiv 5 \bmod 8$), one can argue that the algebra $(\frac{-p,-1}{\mathbb{Q}})$ (respectively $(\frac{-p,-2}{\mathbb{Q}})$) is a natural model for $B_{p,\infty}$. However, when $p \equiv 1 \bmod 8$, there is no uniform value of $q$ for which $B_{p,\infty} \simeq (\frac{-p,-q}{\mathbb{Q}})$. In order to fix an algebra for each $p$, previous works fix a procedure $\mathcal{Q}$ such that on input $p$, the output $\mathcal{Q}(p)$ is a prime satisfying $B_{p,\infty} \simeq (\frac{-p,-\mathcal{Q}(p)}{\mathbb{Q}})$. This $\mathcal{Q}(p)$ is typically set to be the smallest prime number with the requested property. While a convenient choice, it is somewhat arbitrary. Furthermore, without GRH, there is no guarantee for this value to be small, nor easy to find.

As this model $B_{p,\infty} = (\frac{-a,-b}{\mathbb{Q}})$ *might* be hard to compute (without GRH, when $p \equiv 1 \bmod 8$), the original definition of MaxOrder becomes ambiguous: are $a$ and $b$ provided, or are they to be computed? We settle for a definition of MaxOrder where $a$ and $b$ are left to be found. Let us show that the impact of this choice is minimal: it is equivalent to the variant $\text{MaxOrder}_{\mathcal{Q}}$ where the algebra is imposed to be of the classical form $(\frac{-p,-\mathcal{Q}(p)}{\mathbb{Q}})$, for any procedure $\mathcal{Q}$ which returns a suitable prime. The key is Proposition 2.2, which allows one to translate solutions accross different models of $B_{p,\infty}$, so the choice of a particular model matters not.

**Proposition 3.1 ($\text{MaxOrder}_{\mathcal{Q}}$ is equivalent to MaxOrder).** *Given oracle access to $\mathcal{Q}$, the two problems* MaxOrder *and* $\text{MaxOrder}_{\mathcal{Q}}$ *are equivalent under probabilistic polynomial time reductions. The reductions make a single query to each oracle.*

*Proof.* Let $E/\mathbb{F}_{p^2}$ be a supersingular elliptic curve. We first prove that MaxOrder reduces to $\text{MaxOrder}_{\mathcal{Q}}$. Indeed, if $\mathcal{O} \subset (\frac{-p,-\mathcal{Q}(p)}{\mathbb{Q}})$ is a solution of $\text{MaxOrder}_{\mathcal{Q}}$, then $(p, \mathcal{Q}(p), \mathcal{O})$ is a solution of MaxOrder.

We now prove that $\text{MaxOrder}_{\mathcal{Q}}$ reduces to MaxOrder. Let $\mathcal{O} \subseteq (\frac{-a,-b}{\mathbb{Q}})$ be a solution of MaxOrder, and let $q = \mathcal{Q}(p)$. Let $\Lambda_0$ be the (non-maximal) order spanned by the canonical basis $(1, i, j, k)$ of $(\frac{-p,-q}{\mathbb{Q}})$. Thanks to the orthogonality of this basis and since the discriminant of any order $\mathcal{O} = (\alpha_0, \ldots, \alpha_4)$ is given by $\text{disc}(\mathcal{O}) = \sqrt{|\det((\langle \alpha_i, \alpha_j \rangle)_{i,j})|}$, the discriminant of $\Lambda_0$ is $pq$. The factorisation of $\text{disc}(\Lambda_0)$ being known, one can construct a maximal order $\mathcal{O}_0 \supseteq \Lambda_0$ in polynomial time with [25, Theorem 7.14].

From Proposition 2.2, one can compute an order $\mathcal{O}'$ in $(\frac{-p,-q}{\mathbb{Q}})$ isomorphic to $\mathcal{O}$. Then, $\mathcal{O}'$ is a solution of $\text{MaxOrder}_{\mathcal{Q}}$. □

## 4 The Homomorphism Module problem

The HomModule problem has not been formally studied in the previous literature, yet it naturally appears in isogeny-based cryptography. For instance, the homomorphism module between the commitment curve and the challenge curve in SQISign [9] is the space of all possible responses during an identification. While it is clear that Isogeny reduces to HomModule, we prove in this section that both are actually equivalent.

The relation between HomModule and Isogeny is reminiscent of the relations between EndRing and OneEnd. The latter equivalence has been proved in [19]. In this same paper, the authors also proved that OneEnd reduces to Isogeny, both of these reductions being unconditional. Therefore, there is a probabilistic polynomial time algorithm solving EndRing given an Isogeny oracle. In order to take advantage of this fact to solve HomModule we prove that knowing an isogeny between two elliptic curves and their respective endomorphism rings, one can compute efficiently a basis of the homomorphism module between the said curves, Proposition 4.4 and Proposition 4.5. This leads to the main result of the section Proposition 4.6, proving that HomModule reduces to Isogeny.

**Lemma 4.1.** *Let $\varphi_i : E \to E_i$, for $i \in \{1, 2\}$, be separable isogenies such that $\ker \varphi_1 \cap \ker \varphi_2 = 0$. Then,*

$$\mathrm{Hom}(E_1, E)\varphi_1 + \mathrm{Hom}(E_2, E)\varphi_2 = \mathrm{End}(E).$$

*Proof.* Let $\varphi_3 : E \to E_3$ be a separable isogeny with $\ker \varphi_3 = \ker \varphi_1 + \ker \varphi_2$. Since $\ker \varphi_1 \cap \ker \varphi_2 = 0$, we have $|\ker \varphi_3| = |\ker \varphi_1||\ker \varphi_2|$. Each

$$I_i = \mathrm{Hom}(E_i, E)\varphi_i = \{\alpha \in \mathrm{End}(E) \mid \ker \varphi_i \subseteq \ker \alpha\}$$

is a left $\mathrm{End}(E)$-ideal of reduced norm $\mathrm{Nrd}(I_i) = |\ker \varphi_i|$. We have

$$I_1 \cap I_2 = \{\alpha \in \mathrm{End}(E) \mid (\ker \varphi_1 + \ker \varphi_2) \subseteq \ker \alpha\} = I_3.$$

We have,

$$\begin{aligned} |I_1/(I_1 \cap I_2)|^{1/2} = \frac{\mathrm{Nrd}(I_3)}{\mathrm{Nrd}(I_1)} = \frac{|\ker \varphi_3|}{|\ker \varphi_1|} = \frac{|\ker \varphi_1||\ker \varphi_2|}{|\ker \varphi_1|} \\ = \mathrm{Nrd}(I_2) = |\mathrm{End}(E)/I_2|^{1/2}. \end{aligned}$$

By the *second isomorphism theorem*,

$$I_1/(I_1 \cap I_2) \cong (I_1 + I_2)/I_2 \subseteq \mathrm{End}(E)/I_2,$$

and since the leftmost and rightmost quotients have the same cardinality, we deduce $(I_1 + I_2)/I_2 = \mathrm{End}(E)/I_2$, hence $I_1 + I_2 = \mathrm{End}(E)$. □

**Lemma 4.2.** *Let $\varphi_i : E \to E_i$, for $i \in \{1, 2\}$, be separable isogenies such that $\ker \varphi_1 \cap \ker \varphi_2 = 0$. Then, for any elliptic curve $E'$,*

$$\mathrm{Hom}(E_1, E')\varphi_1 + \mathrm{Hom}(E_2, E')\varphi_2 = \mathrm{Hom}(E, E').$$

*Proof.* Clearly $\mathrm{Hom}(E_1, E')\varphi_1 + \mathrm{Hom}(E_2, E')\varphi_2 \subseteq \mathrm{Hom}(E, E')$, so let us prove the second inclusion. By Lemma 4.1,

$$\begin{aligned}\mathrm{Hom}(E, E') &= \mathrm{Hom}(E, E')\,\mathrm{End}(E)\\ &= \mathrm{Hom}(E, E')(\mathrm{Hom}(E_1, E)\varphi_1 + \mathrm{Hom}(E_2, E)\varphi_2)\\ &\subseteq \mathrm{Hom}(E_1, E')\varphi_1 + \mathrm{Hom}(E_2, E')\varphi_2,\end{aligned}$$

which proves the result. □

**Proposition 4.3.** *Let $\varphi : E \to E'$ be a separable isogeny. Then,*

$$\mathrm{span}_{\mathbb{Z}}(\mathrm{End}(E')\varphi\,\mathrm{End}(E)) = m\,\mathrm{Hom}(E, E'),$$

*where $m \in \mathbb{Z}$ is the largest integer dividing $\varphi$.*

*Proof.* Clearly $\mathrm{span}_{\mathbb{Z}}(\mathrm{End}(E')\varphi\,\mathrm{End}(E)) \subseteq m\,\mathrm{Hom}(E, E')$, so let us prove the other inclusion. Write $\varphi = m\psi$ with $\ker\psi$ cyclic. Let $n = \deg(\psi)$. The kernel $\ker\psi \cong \mathbb{Z}/n\mathbb{Z}$ is a cyclic subgroup of $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$. The action of $\mathrm{End}(E)/n\,\mathrm{End}(E)$ on $E[n]$ is isomorphic to the action of $M_2(\mathbb{Z}/n\mathbb{Z})$ on $(\mathbb{Z}/n\mathbb{Z})^2$, so there exists an endomorphism $\alpha \in \mathrm{End}(E)$ (of degree coprime with $n$) such that $\ker(\psi) \cap \alpha^{-1}(\ker\psi) = 0$. In other words, $\ker(\psi) \cap \ker(\psi\alpha) = 0$. Applying Lemma 4.2, we deduce

$$\mathrm{End}(E')\psi + \mathrm{End}(E')\psi\alpha = \mathrm{Hom}(E, E').$$

We deduce

$$m\,\mathrm{Hom}(E, E') = \mathrm{End}(E')\varphi + \mathrm{End}(E')\varphi\alpha \subseteq \mathrm{span}_{\mathbb{Z}}(\mathrm{End}(E')\varphi\,\mathrm{End}(E)),$$

which proves the proposition. □

Recall that any isogeny can be factored as $\phi\varphi$ where $\varphi$ is separable, and $\phi$ is purely inseparable ($\phi$ might be an isomorphism). Then, the following proposition generalized Proposition 4.3 to arbitrary isogenies.

**Proposition 4.4.** *Let $\varphi : E \to E''$ be a separable isogeny, and $\phi : E'' \to E'$ a purely inseparable isogeny $E$. Then,*

$$L = \mathrm{span}_{\mathbb{Z}}(\mathrm{End}(E')\phi\varphi\,\mathrm{End}(E)) = m\phi\,\mathrm{Hom}(E, E''),$$

*where $m \in \mathbb{Z}$ is the largest integer dividing $\varphi$.*

*Proof.* Since $\phi : E'' \to E'$ is purely inseparable, we have $\mathrm{End}(E')\phi = \phi\,\mathrm{End}(E'')$. The result then immediately follows from Proposition 4.3. □

**Proposition 4.5.** *Let $E$, $E'$ and $E''$ be supersingular elliptic curves, and $\phi : E'' \to E'$ a purely inseparable isogeny $E$. Given a basis of $\phi\,\mathrm{Hom}(E, E'')$, one can compute a basis of $\mathrm{Hom}(E, E')$ in polynomial time.*

*Proof.* Let $(b_i)_{i=1}^4$ be the provided basis of the lattice $L = \phi \operatorname{Hom}(E, E'')$. Let $p^n = \deg(\phi)$. If $n = 2m$ is even, then $\phi = p^m \alpha$ where $\alpha : E'' \to E'$ is an isomorphism. Then $(b_i/p^m)_{i=1}^4$ is a basis of $\alpha \operatorname{Hom}(E, E'') = \operatorname{Hom}(E, E')$. If $n = 2m+1$ is odd, one can similarly divide by $p^m$, and without loss of generality we now consider the case where $\phi$ is the $p$-Frobenius. Consider the quadratic form

$$q : L \longrightarrow \mathbb{Z} : \varphi \longmapsto \deg(\varphi)/p.$$

We have

$$p \operatorname{Hom}(E, E') = L \cap (p \operatorname{Hom}(E, E')) = \{\varphi \in L \mid q(\varphi) \equiv 0 \bmod p\}.$$

The equation $q(\varphi) \equiv 0 \bmod p$ defines an $\mathbb{F}_p$-linear subspace of $L/pL$ which can be computed as the kernel of the Gram matrix over $\mathbb{F}_p$. □

**Algorithm 1** Reducing HomModule to Isogeny

**Input:** Two isogeneous elliptic curves $E_1$ and $E_2$ and an access to an oracle of Isogeny.

**Output:** Four isogenies $\varphi_i : E_1 \to E_2$, $i \in \{1, ..., 4\}$ generating $\operatorname{Hom}(E_1, E_2)$ as a $\mathbb{Z}$-module.

1: $(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \leftarrow$ a basis of $\operatorname{End}(E_1)$ ▷ [19, Theorem 8.6]
2: $(\beta_1, \beta_2, \beta_3, \beta_4) \leftarrow$ a basis of $\operatorname{End}(E_2)$ ▷ [19, Theorem 8.6]
3: Compute an isogeny $\varphi : E_1 \to E_2$ ▷ Using the Isogeny oracle
4: $v \leftarrow v_p(\deg \varphi)$ ▷ $p$-adic valuation of $\deg \varphi$
5: $S \leftarrow \{\beta_j \circ \varphi \circ \alpha_i\} \subset \operatorname{Hom}(E_1, E_2)$
6: $(\gamma_1, \gamma_2, \gamma_3, \gamma_4) \leftarrow$ a basis of the lattice generated by $S$ ▷ [4]
7: $m \leftarrow \left(16 \det(\langle \gamma_i, \gamma_j \rangle)/p^{4v+2}\right)^{1/8}$
8: $B_0 \leftarrow (\gamma_1/m, \gamma_2/m, \gamma_3/m, \gamma_4/m)$ ▷ Proposition 2.5
9: Extract a basis of $\operatorname{Hom}(E, E')$ from $B$ ▷ Proposition 4.5
10: **return** $B$

**Proposition 4.6 (HomModule reduces to Isogeny).** *Algorithm 1 is correct and runs in time polynomial in* $\log p$ *and in the length of the oracle outputs.*

*Proof.* The running time of each step is ensured by the corresponding reference. In particular, each is polynomial in $\log p$ and in the length of the oracle's outputs.

Let us prove the correctness of the algorithm by treating the cases where the isogeny $\varphi$, returned by the Isogeny oracle at Step 3, is inseparable and separable independently.

We now assume that $\varphi = \phi \circ \psi$ where $\psi : E_1 \to E'$ is a separable isogeny and $\phi : E' \to E_2$ is a purely inseparable isogeny of degree $p^v \geq 1$, where $v := v_p(\deg \varphi)$ (when $v = 0$, the purely inseparable part $\phi$ is an isomorphism). Let $m$ be the largest integer that divides $\psi$. Then, by Proposition 4.4, the set

$S$ generates the lattice $m\phi\,\mathrm{Hom}(E_1, E')$. For a basis $(\gamma_1, \ldots, \gamma_4)$ of the lattice generated by $S$, we have

$$\begin{aligned}\det(\langle \gamma_i, \gamma_j \rangle) &= \mathrm{Vol}(m\phi\,\mathrm{Hom}(E_1, E'))^2 \\ &= (m^4 \deg(\phi)^2 \mathrm{Vol}(\mathrm{Hom}(E_1, E')))^2 \\ &= m^8 p^{4v+2}/16,\end{aligned}$$

thus the computation at Step 7 gives the correct $m$. In particular, the basis $B = (\gamma_1/m, \ldots, \gamma_4/m)$ generates $\phi\,\mathrm{Hom}(E_1, E')$. From it, one can compute a basis of $\mathrm{Hom}(E_1, E_2)$ using Proposition 4.5. □

## 5 Finding endomorphisms from quaternions

In the section we develop an unconditional reduction from the OneEnd problem to the MaxOrder problem. The main difficulty is that without GRH, there is no general way to compute a "special" elliptic curve $E_0$ for which both $\mathrm{End}(E_0)$ and its embedding in the quaternions are already known. Such a curve provides an "endomorphism/quaternion" dictionary, and previous literature on MaxOrder made critical use of that fact. Without such an $E_0$, we need to develop a completely different strategy. To reduce OneEnd (say on some input $E$) to MaxOrder, we solve the MaxOrder problem on $E$, giving an order $\mathcal{O}$, but also on a few of its "neighbours". We thereby constructing a "local" correspondence: a canonical bijection between $\ell$-isogenies from $E$ and ideals of norm $\ell$ in the order $\mathcal{O}$. This is done in Algorithm 2. We then prove that this information can be converted into isomorphisms $\mathrm{End}(E[\ell]) \simeq \mathcal{O}/\ell\mathcal{O}$ which all descend from the same implicit isomorphism $\mathrm{End}(E) \simeq \mathcal{O}$, via Algorithm 3. Finally, from this local data, we reconstruct a full "endomorphism/quaternion" dictionary $\mathrm{End}(E) \simeq \mathcal{O}$ in Algorithm 4.

At several steps of this process, one might fail to construct the dictionary (for instance when the isomorphism $\mathrm{End}(E) \simeq \mathcal{O}$ is not unique). In such a scenario, a non-scalar endomorphism of $E$ is revealed, and we have solved OneEnd anyway. If no such failure occurs, we successfully obtain a dictionary, which in turn reveals (all!) non-scalar endomorphisms of $E$.

**Lemma 5.1.** *Algorithm 2 is correct and runs in time polynomial in the length of the input, in $\ell$, and in the length of the* MaxOrder *oracle outputs.*

*Proof.* The claim that the running time is polynomial follows from the references provided in the comments of Algorithm 2.

Let us prove that the algorithm is correct.

First, the endomorphism $\alpha = \hat{\varphi}_j \circ \gamma \circ \varphi_i$ returned at Line 4 is not scalar. Indeed, suppose by contradiction that $\alpha \in \mathbb{Z}$. It is of degree $\ell^2$, so $\alpha = [\ell]$. We thus have $\hat{\varphi}_j \circ \varphi_j = [\ell] = \hat{\varphi}_j \circ \gamma \circ \varphi_i$, hence $\varphi_j = \gamma \circ \varphi_i$, hence $\ker(\varphi_j) = \ker(\varphi_i)$, hence $G_i = G_j$, contradicting that $i \neq j$.

Second, the endomorphism returned at Line 8 is not scalar either. Indeed, it has degree $\ell^2 p$, which is not a square, so it cannot be scalar.

**Algorithm 2** Computing a bijection between $\ell$-isogenies and ideals, given a MaxOrder oracle

**Input:** A supersingular elliptic curve $E/\mathbb{F}_{p^2}$, a prime $\ell \neq p$, a list $(G_i)_{i=0}^{\ell}$ of all subgroups of order $\ell$ in $E$, an algebra $B = (\frac{-a,-b}{\mathbb{Q}}) \simeq B_{p,\infty}$, a maximal order $\mathcal{O} \simeq \mathrm{End}(E)$ in $B$, and access to an oracle for MaxOrder.

**Output:** Either an endomorphism $\alpha \in \mathrm{End}(E) \setminus \mathbb{Z}$, or the list $(I_i)_{i=0}^{\ell}$ of left $\mathcal{O}$-ideals such that $\mathcal{O}_R(I_i) \simeq \mathrm{End}(E/G_j)$ if and only if $i = j$.

1: Compute $\varphi_i : E \to E/G_i$ using Vélu's formulas for $i = 0, \ldots, \ell$
2: **if** $E/G_i \simeq E/G_j$ for some $i \neq j$ **then**
3: $\quad\gamma \leftarrow$ an isomorphism between $E/G_i$ and $E/G_j$
4: $\quad$**return** $\hat{\varphi}_j \circ \gamma \circ \varphi_i \in \mathrm{End}(E) \setminus \mathbb{Z}$
5: **if** $E/G_i \simeq (E/G_j)^{(p)}$ for some $i \neq j$ **then**
6: $\quad\gamma \leftarrow$ an isomorphism between $E/G_i$ and $(E/G_j)^{(p)}$
7: $\quad\phi_p \leftarrow$ the Frobenius isogeny $\phi_p : E/G_j \to (E/G_j)^{(p)}$
8: $\quad$**return** $\hat{\varphi}_j \circ \phi_p \circ \gamma \circ \varphi_i \in \mathrm{End}(E) \setminus \mathbb{Z}$
9: **for** $i = 0, \ldots, \ell$ **do**
10: $\quad(B_i, \tilde{\mathcal{O}}_i) \leftarrow$ an algebra $B_i \simeq B_{p,\infty}$ and a maximal order $\tilde{\mathcal{O}}_i \subset B_i$ such that $\tilde{\mathcal{O}}_i \simeq \mathrm{End}(E/G_i)$. ▷ Using the oracle for MaxOrder on $E/G_i$
11: $\quad\mathcal{O}_i \leftarrow$ an order in $B$ isomorphic to $\mathrm{End}(E/G_i)$ ▷ Proposition 2.2 on $(B, \mathcal{O})$ and $(B_i, \tilde{\mathcal{O}}_i)$.
12: $\quad J_i \leftarrow I(\mathcal{O}, \mathcal{O}_i)$ the connecting ideal ▷ [11, Algorithm 3.5]
13: $\quad\langle \alpha_1, \ldots, \alpha_4 \rangle \leftarrow$ a Minkowski-reduced basis of $J_i$ ▷ [17]
14: $\quad$**if** $\mathrm{Nrd}(\alpha_2) \leq \ell\,\mathrm{Nrd}(J_i)$ **then**
15: $\quad\quad\alpha \leftarrow$ a non-scalar endomorphism of $E$ of degree at most $\ell^2$ ▷ For instance, by exhaustive enumeration of isogenies of degree at most $\ell^2$ from $E$.
16: $\quad\quad$**return** $\alpha$
17: $\quad I_i \leftarrow J_i \overline{\alpha}_1 / \mathrm{Nrd}(J_i)$ ▷ The unique left $\mathcal{O}$-ideal of norm $\ell$ equivalent to $J_i$.
18: **return** $(B, \mathcal{O}, (I_i)_{i=0}^{\ell})$

Note that after Line 8, the rings $\mathrm{End}(E/G_i)$ are pairwise non-isomorphic. Indeed, by [26, Lemma 42.4.1], if $\mathrm{End}(E/G_i) \simeq \mathrm{End}(E/G_j)$, then $E/G_i$ is isomorphic to either $E/G_j$ or to its Galois conjugate $(E/G_j)^{(p)}$, in which case the algorithm has terminated before Line 8. In particular, the codomains of all $\ell$-isogenies from $E$ have pairwise distinct endomorphism rings, hence left ideals of norm $\ell$ in $\mathcal{O}$ are uniquely identified by the isomorphism class of their right-order.

At each iteration of the for-loop, we consider two cases.

– If $\mathrm{Nrd}(\alpha_2) \leq \ell\,\mathrm{Nrd}(J_i)$, by definition of Minkowski bases, we have that $\mathrm{Nrd}(\alpha_1) \leq \ell\,\mathrm{Nrd}(J_i)$. As $J_i \bar{J}_i = \mathrm{Nrd}(J_i)\mathcal{O}$, the element $\alpha_1 \bar{\alpha}_2 / \mathrm{Nrd}(J_i)$ is in $\mathcal{O}$. Furthermore, $\alpha_1 \bar{\alpha}_2 / \mathrm{Nrd}(J_i)$ is not a scalar, otherwise $\alpha_1$ and $\alpha_2$ would be linearly dependent. Therefore $\mathcal{O}$ (hence also $\mathrm{End}(E)$) contains a non-scalar element of norm

$$\mathrm{Nrd}\left(\frac{\alpha_1 \bar{\alpha}_2}{\mathrm{Nrd}(J_i)}\right) = \frac{\mathrm{Nrd}\,(\alpha_1)\,\mathrm{Nrd}\,(\alpha_2)}{\mathrm{Nrd}(J_i)^2} \leq \ell^2$$

Then, a non-trivial endomorphism of degree at most $\ell^2$ can be found in time polynomial in $\log p$ and $\ell$ by exhaustive search.

– Otherwise, $\mathrm{Nrd}(\alpha_2) > \ell\,\mathrm{Nrd}(J_i)$. Let us prove that in that case, the ideal $I_i = J_i\bar{\alpha}_1/\mathrm{Nrd}(J_i)$ is the unique left $\mathcal{O}$-ideal of norm $\ell$ with $\mathcal{O}_R(I_i) \simeq \mathrm{End}(E/G_i)$. Recall that by the Deuring correspondence, the lattice $\mathrm{Hom}(E, E/G_i)$ (for the quadratic form deg) is isomorphic to $J_i$ (with quadratic form $q_{J_i} : \alpha \mapsto \mathrm{Nrd}(\alpha)/\mathrm{Nrd}(J_i)$). Therefore, there exists an element $\beta \in J_i$ such that $q_{J_i}(\beta) = \ell$. Since $q_{J_i}(\beta) < q_{J_i}(\alpha_2)$, the element $\beta$ must be a multiple of $\alpha_1$: there exists $m \in \mathbb{Z}$ such that $\beta = m\alpha_1$. Since

$$\ell = q_{J_i}(\beta) = q_{J_i}(m\alpha_1) = m^2 q_{J_i}(\alpha_1)$$

and $\ell$ is prime, we must have that $m = 1$ and $q_{J_i}(\alpha_1) = \ell$. This implies that $\mathrm{Nrd}(I_i) = \ell$.
The unicity of $I_i$ follows from the previously established fact that left ideals of norm $\ell$ in $\mathcal{O}$ are uniquely identified by the isomorphism class of their right-order.

The unicity of each $I_i$ proves that if Line 18 is reached, we indeed have $\mathcal{O}_R(I_i) \simeq \mathrm{End}(E/G_j)$ if and only if $i = j$. □

**Lemma 5.2.** *Let $\rho : M_2(\mathbb{F}_\ell) \to M_2(\mathbb{F}_\ell)$ be a ring automorphism. If $\ker(m) = \ker(\rho(m))$ for all $m \in M_2(\mathbb{F}_\ell)$, then $\rho$ is the identity.*

*Proof.* All automorphisms of $M_2(\mathbb{F}_\ell)$ are inner, so there exists $p \in \mathrm{GL}_2(\mathbb{F}_\ell)$ such that $\rho(m) = p^{-1}mp$ for all $m \in M_2(\mathbb{F}_\ell)$.

First, suppose there exists a line $L \subset \mathbb{F}_\ell^2$ such that $p(L) \neq L$. Then, there exists $m \in M_2(\mathbb{F}_\ell)$ such that $m(L) = p(L)$ and $m(p(L)) = \{0\}$. We obtain

$$\rho(m)(L) = (p^{-1}mp)(L) = p^{-1}(m(p(L)) = p^{-1}(\{0\}) = \{0\}.$$

By construction, $m$ cannot be invertible or the zero matrix; consequently, both $\ker(\rho(m))$ and $\ker(m)$ have dimension 1. Therefore $L = \ker(\rho(m)) = \ker(m) = p(L)$, a contradiction. We deduce that for any line $L \subset \mathbb{F}_\ell^2$, we have $p(L) = L$. Since $p$ fixes all lines in $\mathbb{F}_\ell^2$, all vectors of $\mathbb{F}_\ell^2$ are eigenvectors of $p$, so $p$ is a scalar matrix. In particular, $\rho(m) = p^{-1}mp = m$. □

**Corollary 5.3.** *Consider rings $R \simeq R' \simeq M_2(\mathbb{F}_\ell)$. Let $\iota_1, \iota_2 : R \to R'$ be two ring isomorphisms. If $\iota_1(I) = \iota_2(I)$ for all left-ideals $I$ in $R$, then $\iota_1 = \iota_2$.*

*Proof.* Fix two isomorphisms $g : R' \to M_2(\mathbb{F}_\ell)$ and $f : M_2(\mathbb{F}_\ell) \to R$, and define

$$\rho_i = g \circ \iota_i \circ f : M_2(\mathbb{F}_\ell) \to M_2(\mathbb{F}_\ell).$$

Let $\rho = \rho_2^{-1} \circ \rho_1$. Let us prove that $\rho$ satisfies the condition of Lemma 5.2. Let $m \in M_2(\mathbb{F}_\ell)$. Let $J = M_2(\mathbb{F}_\ell)m = \{\tilde{m} \in M_2(\mathbb{F}_\ell) \mid \ker(m) \subseteq \ker(\tilde{m})\}$ be the left-ideal generated by $m$. Then, its image $f(J)$ is a left-ideal in $R$, hence $\iota_1(f(J)) = \iota_2(f(J))$, and

$$\rho(J) = f^{-1} \circ \iota_2^{-1} \circ \iota_1 \circ f(J) = f^{-1} \circ \iota_2^{-1} \circ \iota_2 \circ f(J) = J.$$

In particular, $\rho(m) \in \rho(J) = J$, so $\ker(m) \subseteq \ker(\rho(m))$. Since $\rho$ is an isomorphism, the matrices $m$ and $\rho(m)$ have the same rank, hence $\ker(m) = \ker(\rho(m))$.

We can thus apply Lemma 5.2, and deduce that $\rho$ is the identity.

In particular, we obtain $\rho_1 = \rho_2$, therefore $\iota_1 = \iota_2$. □

**Algorithm 3** Computing an isomorphism between quaternions and endomorphisms modulo $\ell$, given a MaxOrder oracle

**Input:** A supersingular elliptic curve $E/\mathbb{F}_{p^2}$, a prime $\ell$, an algebra $B \simeq B_{p,\infty}$, a maximal order $\mathcal{O} \simeq \mathrm{End}(E)$ in $B$, and access to an oracle for MaxOrder.

**Output:** Either an endomorphism $\alpha \in \mathrm{End}(E) \setminus \mathbb{Z}$, or an isomorphism $\lambda : \mathcal{O}/\ell\mathcal{O} \to \mathrm{End}(E[\ell])$.

$(G_i)_{i=0}^{\ell} \leftarrow$ a list of all subgroups of order $\ell$ of the elliptic curve $E$.
Using the oracle access, run Algorithm 2 on the list $(G_i)_{i=0}^{\ell}$ to obtain either
- a non trivial endomorphism $\alpha \in \mathrm{End}(E) \setminus \mathbb{Z}$,
- or a list $(I_i)_{i=0}^{\ell}$ such that $I_i$ is the unique left $\mathcal{O}$-ideal of norm $\ell$ with $\mathcal{O}_R(I_i) \simeq \mathrm{End}(E/G_i)$.

**if** $\alpha \in \mathrm{End}(E) \setminus \mathbb{Z}$ was found **then**
    **return** $\alpha$
$g \leftarrow$ an isomorphism from $\mathrm{End}(E[\ell])$ to $M_2(\mathbb{F}_\ell)$.
$f \leftarrow$ an isomorphism $\mathcal{O}/\ell\mathcal{O}$ to $M_2(\mathbb{F}_\ell)$.
$J_i \leftarrow \{\alpha \in \mathrm{End}(E[\ell]) | G_i \subset \ker \alpha\}$, for $i \in \{0, \ldots, \ell\}$.
$h \leftarrow$ an automorphism from $M_2(\mathbb{F}_\ell)$ to $M_2(\mathbb{F}_\ell)$ such that $h(f(\tilde{I}_i)) = g(J_i)$ where $\tilde{I}_i$ is the reduction of $I_i$ modulo $\ell$.
$\lambda \leftarrow g^{-1} \circ h \circ f : \mathcal{O}/\ell\mathcal{O} \to \mathrm{End}(E[\ell])$.
**return** $\lambda$.

**Lemma 5.4.** *Algorithm 3 is correct and runs in time polynomial in the length of the input, in $\ell$, and in the length of the output of the oracle for* MaxOrder.

*Proof.* Let $\iota : \mathcal{O} \xrightarrow{\sim} \mathrm{End}(E)$ be an isomorphism. Let us prove that the isomorphism $\lambda$ computed by Algorithm 3 is its reduction modulo $\ell$, thereby also proving the correctness of this algorithm.

Since $I_i$ is the unique left $\mathcal{O}$-ideal of norm $\ell$ with $\mathcal{O}_R(I_i) \simeq \mathrm{End}(E/G_i)$, we have that

$$\iota(I_i) = \{\alpha \in \mathrm{End}(E) | G_i \subseteq \ker(\alpha)\}.$$

Then, reduced modulo $\ell$, the equality becomes

$$\iota_\ell(\tilde{I}_i) = J_i,$$

where $\tilde{I}_i$ is the reduction of $I_i$ modulo $\ell$. On the other hand, by construction, we have $\lambda(\tilde{I}_i) = J_i$. Thus, by Corollary 5.3, the isomorphism $\lambda_\ell$ is equal to the isomorphism $\lambda$.

Now, we demonstraste the complexity of the algorithm by giving the complexity of its different steps. Obtaining the list of subgroup of order $\ell$ of the elliptic curve $E$ can be done by computing a basis of the $\ell$-torsion of $E$. This take a polynomial time in $\ell$ and in $\log p$.

One can define the isomorphisms $g, f$ and $h$ by mapping the basis of the domain to a basis of the codomain such that the map verified the respective required properties. Since there are $O(\ell^4)$ ordered bases of $M_2(\mathbb{F}_\ell)$, these constructions can be carried out using an exhaustive search.

Finally, by Lemma 5.1, running Algorithm 2 takes a polynomial time in the length of the input, in $\ell$ and in the length of the output of the oracle for MaxOrder. All the previously discussed complexities are encompassed within this running time.

□

**Algorithm 4** Computing a non-scalar endomorphism, given a MaxOrder oracle

**Input:** A supersingular elliptic curve $E/\mathbb{F}_{p^2}$ and an access to an oracle for MaxOrder.

**Output:** An endomorphism $\theta \in \mathrm{End}(E) \setminus \mathbb{Z}$.

1: $\mathcal{O} \leftarrow$ a maximal order in a quaternion algebra such that $\mathcal{O} \simeq \mathrm{End}(E)$ ▷ Using MaxOrder oracle
2: $(\beta_i)_{i=1}^4 \leftarrow$ a Minkowski-reduced basis of $\mathcal{O}$ ▷ [17]
3: $\alpha \leftarrow \beta_2$ ▷ $\alpha$ is a shortest non-scalar vector in $\mathcal{O}$
4: $\ell \leftarrow 1, N \leftarrow 1$
5: **while** $N < \mathrm{Nrd}(\alpha)$ **do**
6: $\quad \ell \leftarrow$ the next prime after $\ell$ which is coprime to $\mathrm{Nrd}(\alpha)$
7: $\quad N \leftarrow \ell N$
8: $\quad (P_\ell, Q_\ell) \leftarrow$ a basis of the $\ell$-torsion $E[\ell]$ ▷ [1, Lemma 6.9]
9: $\quad \lambda_\ell \leftarrow$ the isomorphism $\mathcal{O}/\ell\mathcal{O} \simeq \mathrm{End}(E[\ell])$ ▷ Using Algorithm 3
10: $\quad (P'_\ell, Q'_\ell) \leftarrow (\lambda_\ell(P_\ell), \lambda_\ell(Q_\ell))$
11: $\theta \leftarrow$ `IsogenyInterpolation`$((P_\ell, Q_\ell)_\ell, (P'_\ell, Q'_\ell)_\ell)$ ▷ Proposition 2.4

**Proposition 5.5 (OneEnd reduces to MaxOrder).** *Algorithm 4 is correct and runs in probabilistic polynomial time in the length of the instance and in the length of the oracle's output.*

*Proof.* By the references cited in the comments, each step is at most polynomial in $\log p$, in the length of the MaxOrder oracle's output and in $\ell$ (whenever a prime $\ell$ is involved in the computation). Therefore, to prove the claimed complexity, it remains only to establish bounds on the number of iterations of the loop at line 5 and on the considered primes $\ell$.

By [27], a Minkowski-reduced basis of a lattice in dimension 4 reaches all the successive minimas. Hence, $\mathrm{Nrd}(\alpha)$ is the second minima of $\mathcal{O}$, i.e. the first

minima of $\mathcal{O} \setminus \mathbb{Z}$. Additionally, by Minkowski's second theorem, the product of the successive minimas of $\mathcal{O}$ is smaller than $\gamma_4^2 \operatorname{disc}(\mathcal{O})$, where $\gamma_4$ is the Hermite constant in dimension 4. Thus we have that $\operatorname{Nrd}(\alpha) \leq 2p^2$. Therefore, by the prime number theorem, the while loop at line 5 has $O(\log p)$ iterations and the largest $\ell$ considered is $O(\log p)$, proving the claimed complexity.

The correctness of Algorithm 4 comes from the fact that we return the output of `IsogenyInterpolation` called on input corresponding to the evaluation of $\iota(\alpha)$ on the $N$-torsion subgroup $E[N]$ with $N > \operatorname{Nrd}(\alpha)$, where $\iota$ is the Deuring isomorphism. □

## 6 Reductions to the Endomorphism Ring problem

We now turn to proving that Isogeny and MOER reduce in polynomial time to EndRing, thereby completing the equivalence of all problems presented in Figure 1. We shall proceed by proving the following sequence of reductions:


The main difficulty in reducing the Isogeny problem between two curves to the MaxOrder problem lies in translating a connecting ideal between two maximal orders, which are isomorphic to the endomorphism ring of the curves, into an isogeny between the curves. Before the break of SIDH [5,14,22], this process required first finding a more suitable ideal, using KLPT-type algorithms [12], which can be proven under GRH [28], and then computing the corresponding isogeny using an elliptic curve with known endomorphism ring as a dictionnary between endomorphisms and quaternions. Thanks to Proposition 2.6, it is now possible to directly compute the isogeny corresponding to the connecting ideal. However, one still needs to known an elliptic curve with an explicit basis of its endomorphism ring. This is why, instead of reducing Isogeny to MaxOrder, we reduce it to the MOER problem, ensuring access to such a curve.

**Proposition 6.1 (Isogeny reduces to MOER).** *Given access to a* MOER *oracle, one can solve the* Isogeny *problem in time polynomial in the length of its input and in the length of the oracle's output.*

*Proof.* Let $E_1$ and $E_2$ be two supersingular elliptic curves defined over $\mathbb{F}_{p^2}$. For $i \in \{1, 2\}$, a MOER oracle provides a maximal order $\mathcal{O}_i$ in a quaternion algebra $B_i \simeq B_{p,\infty}$ together with an isomorphism $\varepsilon_i : \mathcal{O}_i \xrightarrow{\sim} \operatorname{End}(E_i)$. By proposition 2.2, one can compute in polynomial time an isomorphism $\varepsilon : B_2 \xrightarrow{\sim} B_1$. Then $\mathcal{O}_2' := \varepsilon(\mathcal{O}_2)$ is a maximal order in $B_1$ isomorphic to $\operatorname{End}(E_2)$. Using [11, Algorithm 3.5], one can compute efficiently the connecting ideal $I = I(\mathcal{O}_1, \mathcal{O}_2')$.

Finally, by Proposition 2.6, one can compute the isogeny $\varphi_I : E_1 \to E_2$ in polynomial time. □

We reduce MOER to EndRing by adapting the strategy of [10, Algorithm 6]. The freedom to chose a model for $B_{p,\infty}$ in the definition of MOER allows us to eliminate all heuristics in the proof of [10, Algorithm 6]. We recall that, using Proposition 2.2, one can always translate a MOER solution into any target quaternion algebra where a maximal order is already known.

**Proposition 6.2 (**MOER **reduces to** EndRing**).** *Given a supersingular elliptic curve $E$ defined over $\mathbb{F}_{p^2}$ together with a basis of its endomorphism ring* $\mathrm{End}(E)$*, one can solve the* MOER *instance corresponding to the curve $E$ in time polynomial in* $\log p$ *and in the length of the elements in the provided basis of* $\mathrm{End}(E)$*.*

*Proof.* Let $(\gamma_i)_{i=0}^4$ be a basis of the endomorphism ring of a supersingular elliptic curve $E$ defined over $\mathbb{F}_{p^2}$. By [10, Lemma 4 and Lemma 5], one can compute, in time polynomial in $\log p$ and in $\log \max_{i=1}^4(\deg(\gamma_i))$, a rational invertible linear transformation $F$ sending $(\gamma)_{i=1}^4$ to some orthogonal basis $(1, \alpha, \beta, \alpha\beta)$. In particular, $(1, \alpha, \beta, \alpha\beta)$ is a basis of the endomorphism algebra $\mathrm{End}(E) \otimes \mathbb{Q}$ such that $\alpha^2 < 0$, $\beta^2 < 0$ and $\alpha\beta = -\beta\alpha$. Hence, it is isomorphic to the quaternion algebra $B = (\frac{\alpha^2, \beta^2}{\mathbb{Q}})$, with basis $(1, i, j, ij)$ such that $i^2 = \alpha^2$, $j^2 = \beta^2$ and $ij = -ji$. Let $\varepsilon : \mathrm{End}(E) \otimes \mathbb{Q} \xrightarrow{\sim} B$ be the explicit isomorphism sending $(1, \alpha, \beta, \alpha\beta)$ to $(1, i, j, ij)$. By applying $F^{-1}$ to $(1, i, j, ij)$ we get a maximal order $\mathcal{O} = \varepsilon((\gamma_i)_{i=1}^4)$ in $B$ isomorphic to $\mathrm{End}(E)$. Finally, since $B$ is isomorphic to $\mathrm{End}(E) \otimes \mathbb{Q}$, which is itself isomorphic to $B_{p,\infty}$, the solution we found satisfies all the conditions of the MOER problem. □

## 7 Worst-case to Average-Case reductions

The goal of this section is to prove Theorem 1.2: there are worst-case to average-case reductions between all of the listed fundamental problems of isogeny-based cryptography. Recall that all of these problems take as input one or two elliptic curves, and the average case of these problems corresponds to random instances where the curves follow the stationary distribution (Definition 2.15).

To prove Theorem 1.2, we follow the network of reductions summarized in Figure 3. Once established, this network of reductions implies that OneEnd (in the worst-case) reduces to the average-case of any other problem. We then conclude from Theorem 1.1, which establishes that all problems reduce to OneEnd.

Note that since the stationary distribution is computationally indistinguishable from the uniform distribution (Remark 2.16), the reductions also apply to the "uniform" version of the average-case problems.

**The straightforward reductions.** In Figure 3, every non-labeled arrow denotes a "trivial" reduction. To be more precise, these reductions simply forward

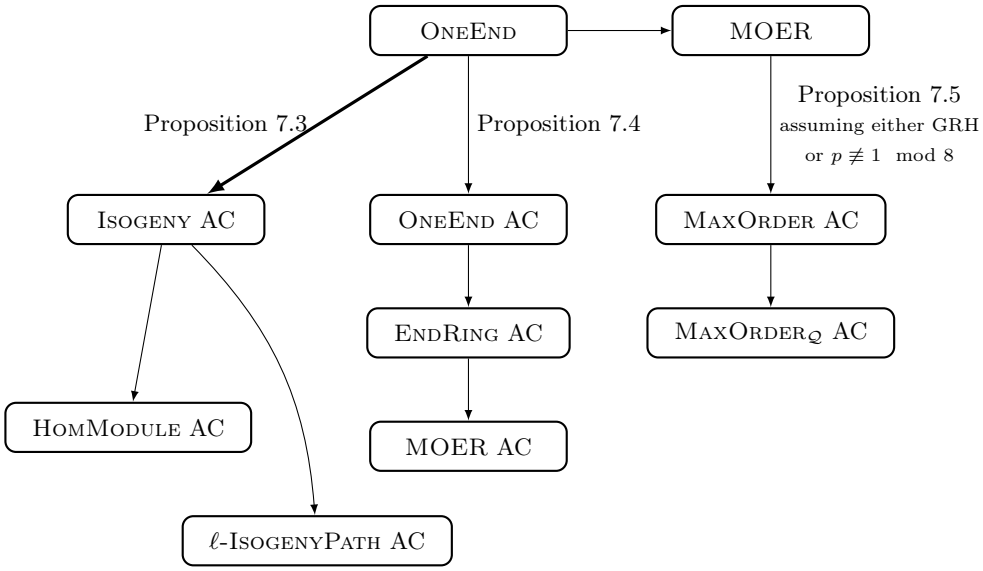


**Fig. 3.** Summary of worst-case to average-case reductions. Each arrow represents a probabilistic polynomial time reduction. Let "AC" label means "average-case". All reductions are one-to-one except for the thick arrow, which requires on average fewer than 3 oracle calls. Each arrow is proved in the associated reference. Arrows without reference are trivial reductions.

an instance for a given problem to an instance for a (at least as hard) variant of this problem. In particular, the input of the average-case problems involved in those reductions always follows the same distribution. For example, the input distribution of the average-case Isogeny problem is a pair of two elliptic curves following the stationary distribution which is also the input distribution of the average-case HomModule. In addition, the solution we get for the harder problem directly includes a solution to the weaker one. For instance, solving the MOER problem also yields a solution to the corresponding EndRing instance. Therefore, all these reductions are trivial, and we only need to prove the reductions from worst-case OneEnd to the average-case problems to complete the figure. We shall address each proof of these non-trivial reductions in a dedicated subsection.

### 7.1 The OneEnd problem reduces to the average-case Isogeny problem

As there exist solutions of Isogeny of arbitrarily large degree, we ease the analysis of the reduction by making a bound explicit, as in [19].

**Definition 7.1 (ISOGENY$_\lambda$).** *Let $\lambda : \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$ be a function. The* ISOGENY$_\lambda$ *problem is a variant of the* ISOGENY *problem where the solution $\varphi$ needs to verify that* $\log(\deg(\varphi)) \leq \lambda(\log p)$.

In [19], the authors have proven that one can solve the ONEEND problem in expected polynomial time in $\log(p)$ and $\lambda(\log p)$ by calling on average at most 3 times an ISOGENY$_\lambda$ oracle. In this section, we adapt this reduction [19, Algorithm 6] to ensure that it produces an *semi average-case* ISOGENY instance, in the sense that *at least one* of the elliptic curves involved follows a distribution indistinguishable from the stationary distribution. We then prove that the *semi* average-case ISOGENY$_\lambda$ reduces to the average-case ISOGENY$_\lambda$, and deduce the claimed excepted polynomial time reduction from ONEEND to ISOGENY$_\lambda$.

**Proposition 7.2.** *Let $c_1, c_2 > 0$, and consider the following variant of [19, Algorithm 6] where*

- *the parameter $\varepsilon$ is smaller than $1/p$,*
- *the length of the non-backtracking random walks in the 3-isogeny graph is $n$, where $n$ satisfies $n \geq c_1 \log(p) - c_2 \log(\varepsilon)$.*

*There exist absolute computable constants $c_1$ and $c_2$ such that this algorithm computes an endomorphism in excepted polynomial time in $\log p$, $\lambda(\log p)$ and $n$ with at most 3 calls to an* ISOGENY$_\lambda$ *oracle. In addition, these calls are done on* semi *average-case instances.*

*Proof.* For $p > 6$, the proof of [19, Theorem 8.6] still applies to this variant of [19, Algorithm 6] $\varepsilon < \frac{1}{6}$, as we can set $c_1$ and $c_2$ such that $n$ is larger than $\lceil 2\log_3(p) - 4\log_3(\varepsilon) \rceil$, as needed. In particular, the algorithm computes an endomorphism in excepted polynomial time in $\log p$, $\lambda(\log p)$ and $n$ with at most 3 calls to an ISOGENY$_\lambda$ oracle.

We now prove the statement about the distribution of the instances given to the oracle. Let $E$ be the ONEEND instance (a supersingular elliptic curve over $\mathbb{F}_{p^2}$). Let us denote by $\mathcal{O}_{\text{ISOGENY}}$ the ISOGENY$_\lambda$ oracle we have access to. Following [19, Algorithm 6], a point $P \in E[2]$ is fixed, and each call to the oracle $\mathcal{O}_{\text{ISOGENY}}$ is done on an instance $(E'', E)$ where $E''$ is the codomain of the composition of isogenies $\nu \circ \varphi$ where $\varphi : E \to E'$ is a non-backtracking random walk in the 3-isogeny graph of length $n$ and $\nu : E' \to E''$ is an isogeny of kernel $\langle \varphi(S) \rangle$. As $\nu$ and $\varphi$ have coprime degree, the distribution of $E''$ is the same as the codomain of $\varphi' \circ \nu'$ where $\nu' : E \to E/\langle S \rangle$, and $\varphi' : E/\langle S \rangle \to E''$ is a non-backtracking random walk in the 3-isogeny graph of length $n$. By [2, Theorem 11], we can set $c_1$ and $c_2$ to ensure that for any $n \geq c_1 \log(p) - c_2 \log(\varepsilon)$, the distribution of $E''$ is an statistical distance at most $\varepsilon$ from the stationary distribution. In particular, each call to the oracle $\mathcal{O}_{\text{ISOGENY}}$ is done on *semi* average-case instances.

□

**Proposition 7.3 (ONEEND reduces to average-case ISOGENY).** *Solving an instance of the worst-case* ONEEND *problem can be reduced in excepted polynomial time in $\log p$ and $\lambda(\log p)$ to solving 3 average instances of the* ISOGENY$_\lambda$ *problem.*

*Proof.* First, we show that an *semi* average instance of $\text{ISOGENY}_{\lambda_c}$ reduces to an average instance of $\text{ISOGENY}_{\lambda}$, where $\lambda_c(n) := \lambda(n) + 2cn + 1$, with $c$ the $O$-constant of Corollary 2.18. Note that $c$ depends only on $p$ and on some positive parameter $\varepsilon$, which we fix to be $\varepsilon := 1/p$. Let $E_0$ and $E_1$ be two supersingular elliptic curves defined over $\mathbb{F}_{p^2}$ such that $E_1$ is sampled from the stationary distribution. By Corollary 2.18, one can compute a random walk $\eta : E_0 \to E_2$ in the 2-isogeny graph of length $\lceil \tau(p, \varepsilon) \rceil$ such that the distribution followed by $E_2$ is at total variation distance at most $\varepsilon$ to the stationary distribution. Then, as $\varepsilon = 1/p$, the two distributions are computationally indistiguishable.

Moreover, since $\tau(p, \varepsilon) = O(\log(p) - \log(\varepsilon))$ and $\varepsilon = 1/p$, we have that $\lceil \tau(p, \varepsilon) \rceil \leq 2c \log(p) + 1$. Then, the random $2^{\lceil \tau(p,\varepsilon) \rceil}$-walk isogeny $\eta$ verifies that $\log(\deg(\eta)) \leq 2c \log p + 1$.

A call to an $\text{ISOGENY}_{\lambda}$ oracle the pair $(E_2, E_1)$, which is indistinguishable from an average-case instance, returns an isogeny $\varphi : E_2 \to E_1$ such that $\log \deg(\varphi) \leq \lambda(\log p)$. Then, the isogeny $\psi := \varphi \circ \eta : E_0 \to E_1$ verifies that $\log(\deg \psi) \leq 2c \log(p) + \lambda(\log p) + 1 = \lambda_c(\log(p))$. Thus the isogeny $\psi$ is a solution to the initial $\text{ISOGENY}_{\lambda_c}$ problem corresponding to $(E_0, E_1)$. This concludes the proof that an *semi* average instance of $\text{ISOGENY}_{\lambda_c}$ reduces to an average instance of $\text{ISOGENY}_{\lambda}$.

We can now conclude the proof: by Proposition 7.2 and because $\lambda_c(\log p)$ is polynomial in $\lambda(\log p)$ and $\log p$, the ONEEND worst-case problem reduces in expected polynomial time in $\log(p)$ and $\lambda(\log(p))$ to 3 *semi* average instances of $\text{ISOGENY}_{\lambda_c}$, which itself reduces to 3 average instances of $\text{ISOGENY}_{\lambda}$ in polynomial time as proven above. □

### 7.2 The ONEEND problem reduces to the average-case ONEEND problem

The reduction presented in this subsection is analogous to the most folkoric methods for self-reducing the ISOGENY problem from the worst-case to the average-case, leveraging the rapid mixing properties of isogeny graphs.

**Proposition 7.4 (ONEEND reduces to average-case ONEEND).** *Solving an instance of the worst-case* ONEEND *problem can be reduced to solving an average-case instance of the* ONEEND *problem in time polynomial in* $\log p$ *and in the length of the averace-case solution.*

*Proof.* Let $E$ be a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$. Let $\eta : E \to E'$ be a random-walk in the 2-isogeny graph of length $n = \lceil \tau(p, 1/p) \rceil$, so that the distribution followed by $E'$ is asymptotically indistinguishable from the stationary distribution by Corollary 2.18. Then, from a solution $\theta : E' \to E'$ to the average-case ONEEND instance corresponding to the curve $E'$, one obtains a non trivial endomorphism $\hat{\eta} \circ \theta \circ \eta : E \to E$ which is a solution to the worst-case instance of ONEEND given by $E$. Indeed, this endomorphism is non trivial; otherwise there exists $n \in \mathbb{Z}$ such that $\hat{\eta} \circ \theta \circ \eta = n$ so $[\deg \eta] \circ \theta = n$, thus $\theta$ is a scalar endomorphism which is a contradiction. □

### 7.3 The MOER problem reduces to the average-case MaxOrder problem

The main challenge in proving unconditional reductions to the MaxOrder problem lies in leveraging the information obtained from the quaternion world to aid in isogeny computation, without having an access to a dictionnary between endomorphisms and quaternions. Indeed, we recall that when $p \equiv 1 \mod 8$, there is currently no known polynomial time algorithm free from GRH that can compute a supersingular elliptic curve defined over $\bar{\mathbb{F}}_p$ together with an embedding of its endomorphism ring into some quaternion algebra isomorphic to $B_{p,\infty}$. In Section 5, we address this difficulty by "locally" computing this embedding for sufficiently many primes, allowing us to apply the recent `IsogenyInterpolation` algorithm. Unfortunately, this method requires solving the MaxOrder problem for elliptic curves which are close to each other in the some isogeny graph. Thus, it cannot be turned into a reduction to the average-case MaxOrder problem. For this reason, the reduction presented below requires the construction of a curve $E_0$ for which a solution of MOERis known. This requires either $p \not\equiv 1 \mod 8$, or to assume GRH.

**Proposition 7.5 (MOER reduces to average-case MaxOrder).** *An instance of the worst-case* MOER *can be reduced to an average instance of the* MaxOrder *problem in polynomial time in the length of the input. If* $p \equiv 1 \mod 8$*, this result assumes GRH.*

*Proof.* By [10, Proposition 3], one can compute in polynomial-time a curve $E_0$ together with a quaternionic order $\mathcal{O}_0$ and an isomorphism $\varepsilon_0 : \mathcal{O}_0 \xrightarrow{\sim} \mathrm{End}(E_0)$ (i.e., a solution to MOER). This result assumes GRH in the case where $p \equiv 1 \mod 8$. We denote by $B$ the quaternion algebra containing $\mathcal{O}_0$.

Let $E$ be a supersingular elliptic curves defined over $\mathbb{F}_{p^2}$. Let us solve the MOER problem for the elliptic curve $E$ calling once a MaxOrder oracle on an average elliptic curve $E'$.

Let $N = \prod_{i=1}^{n} \ell_i$, where $\ell_i$ is the $i$-th smallest prime number, Let $\eta : E \to E'$ be a random $N$-walk. By Corollary 2.18, by choosing $n$ such that $\log(N) \geq \tau(p, 1/p)$, one can ensure that $E'$ follows a distribution statistically indistinguishable from the stationary distribution. In particular, as $\tau(p, 1/p) = O(\log p)$, by the prime number theorem, it is sufficient to consider primes up to some $\ell_n = O(\log(p))$. Thus, the computation of $\eta$ takes a time polynomial in $\log p$.

Let us now solve the worst-case MOER instance corresponding to $E$ from a solution $\mathcal{O}'$ to the average instance given by $E'$. Thanks to Proposition 2.2, one can assume that $\mathcal{O}'$ is a maximal order in the quaternion algebra $B$.

First, we compute a connecting ideal $I$ between $\mathcal{O}'$ and $\mathcal{O}_0$, [11, Algorithm 3.5], and the corresponding isogeny using Proposition 2.6. By running [8, Algorithm 8], where the final division is done using Proposition 2.5, one obtains an isomorphism between $\mathrm{End}(E')$ and a maximal order $\mathcal{O}'$ in polynomial time. Then by using [28, Lemma 7.1] on the isogeny $\hat{\eta}$, one can compute, in polynomial time in $\log p$, the corresponding left $\mathcal{O}'$ ideal $I_{\hat{\eta}}$ such that $\mathcal{O}_R(I) = \mathcal{O}$. Hence,

thanks again to [8, Algorithm 8], we obtain an explicit isomorphism between $\mathrm{End}(E)$ and a maximal order in $B$. □

### 7.4 Proof of Theorem 1.2

We can now turn to the proof of the main theorem of this section.

*Proof (of Theorem 1.2).* Let $P$ and $Q$ be two problems chosen from the problems $\ell$-IsogenyPath, Isogeny, EndRing, OneEnd, MOER, MaxOrder, $\text{MaxOrder}_{\mathcal{Q}}$, and HomModule.

By Theorem 1.1, if $P$ is not $\ell$-IsogenyPath, we have a probabilistic polynomial time reduction from $P$ in the worst-case to OneEnd in the worst-case. Otherwise, assuming the generalised Riemann hypothesis, there is a probabilistic polynomial time reduction from $\ell$-IsogenyPath in the worst-case to OneEnd in the worst-case by [28] and [19]. Then using the results summarized in Figure 3, there is a probabilistic polynomial time reduction from OneEnd in the worst-case to $Q$ in the average-case. □

## References

1. Bank, E., Camacho-Navarro, C., Eisenträger, K., Morrison, T., Park, J.: Cycles in the supersingular l-isogeny graph and corresponding endomorphisms. In: Balakrishnan, J.S., Folsom, A., Lalín, M., Manes, M. (eds.) Research Directions in Number Theory. pp. 41–66. Springer International Publishing, Cham (2019)
2. Basso, A., Codogni, G., Connolly, D., De Feo, L., Fouotsa, T.B., Lido, G.M., Morrison, T., Panny, L., Patranabis, S., Wesolowski, B.: Supersingular curves you can trust. In: Hazay, C., Stam, M. (eds.) Advances in Cryptology – EUROCRYPT 2023, Part II. Lecture Notes in Computer Science, vol. 14005, pp. 405–437. Springer, Cham, Switzerland, Lyon, France (Apr 23–27, 2023). https://doi.org/10.1007/978-3-031-30617-4_14
3. Basso, A., Dartois, P., De Feo, L., Leroux, A., Maino, L., Pope, G., Robert, D., Wesolowski, B.: SQIsign2D-west - the fast, the small, and the safer. In: Chung, K.M., Sasaki, Y. (eds.) Advances in Cryptology – ASIACRYPT 2024, Part III. Lecture Notes in Computer Science, vol. 15486, pp. 339–370. Springer, Singapore, Singapore, Kolkata, India (Dec 9–13, 2024). https://doi.org/10.1007/978-981-96-0891-1_11
4. Buchmann, J., Pohst, M.: Computing a lattice basis from a system of generating vectors. In: Eurocal'87: European Conference on Computer Algebra Leipzig, GDR, June 2–5, 1987 Proceedings. pp. 54–63. Springer (1989)
5. Castryck, W., Decru, T.: An efficient key recovery attack on SIDH. In: Hazay, C., Stam, M. (eds.) Advances in Cryptology – EUROCRYPT 2023, Part V. Lecture Notes in Computer Science, vol. 14008, pp. 423–447. Springer, Cham, Switzerland, Lyon, France (Apr 23–27, 2023). https://doi.org/10.1007/978-3-031-30589-4_15
6. Charles, D.X., Lauter, K.E., Goren, E.Z.: Cryptographic hash functions from expander graphs. Journal of Cryptology **22**(1), 93–113 (Jan 2009). https://doi.org/10.1007/s00145-007-9002-x

7. Csahók, T., Kutas, P., Montessinos, M., Zábrádi, G.: Explicit isomorphisms of quaternion algebras over quadratic global fields. Research in Number Theory **8**(4), 77 (2022)
8. Dartois, P., Leroux, A., Robert, D., Wesolowski, B.: SQIsignHD: New dimensions in cryptography. In: Joye, M., Leander, G. (eds.) Advances in Cryptology – EUROCRYPT 2024, Part I. Lecture Notes in Computer Science, vol. 14651, pp. 3–32. Springer, Cham, Switzerland, Zurich, Switzerland (May 26–30, 2024). https://doi.org/10.1007/978-3-031-58716-0_1
9. De Feo, L., Kohel, D., Leroux, A., Petit, C., Wesolowski, B.: SQISign: Compact post-quantum signatures from quaternions and isogenies. In: Moriai, S., Wang, H. (eds.) Advances in Cryptology – ASIACRYPT 2020, Part I. Lecture Notes in Computer Science, vol. 12491, pp. 64–93. Springer, Cham, Switzerland, Daejeon, South Korea (Dec 7–11, 2020). https://doi.org/10.1007/978-3-030-64837-4_3
10. 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.) Advances in Cryptology – EUROCRYPT 2018, Part III. Lecture Notes in Computer Science, vol. 10822, pp. 329–368. Springer, Cham, Switzerland, Tel Aviv, Israel (Apr 29 – May 3, 2018). https://doi.org/10.1007/978-3-319-78372-7_11
11. Kirschmer, M., Voight, J.: Algorithmic Enumeration of Ideal Classes for Quaternion Orders. SIAM Journal on Computing **39**(5), 1714–1747 (2010). https://doi.org/10.1137/080734467, https://doi.org/10.1137/080734467
12. 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)
13. Lagarias, J.C., Odlyzko, A.M.: Effective versions of the chebotarev density theorem. In: Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975). vol. 7, pp. 409–464 (1977)
14. Maino, L., Martindale, C., Panny, L., Pope, G., Wesolowski, B.: A direct key recovery attack on SIDH. In: Hazay, C., Stam, M. (eds.) Advances in Cryptology – EUROCRYPT 2023, Part V. Lecture Notes in Computer Science, vol. 14008, pp. 448–471. Springer, Cham, Switzerland, Lyon, France (Apr 23–27, 2023). https://doi.org/10.1007/978-3-031-30589-4_16
15. Mamah, M.: The supersingular isogeny path and endomorphism ring problems: Unconditional reductions. Cryptology ePrint Archive, Paper 2024/1569 (2024), https://eprint.iacr.org/2024/1569
16. Merdy, A.H.L., Wesolowski, B.: The supersingular endomorphism ring problem given one endomorphism. Cryptology ePrint Archive, Report 2023/1448 (2023), https://eprint.iacr.org/2023/1448
17. Nguyen, P.Q., Stehlé, D.: Low-dimensional lattice basis reduction revisited. ACM Transactions on algorithms (TALG) **5**(4), 1–48 (2009), publisher: ACM New York, NY, USA
18. 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
19. Page, A., Wesolowski, B.: The supersingular endomorphism ring and one endomorphism problems are equivalent. In: Joye, M., Leander, G. (eds.) Advances in Cryptology – EUROCRYPT 2024, Part VI. Lecture Notes in Computer Science, vol. 14656, pp. 388–417. Springer, Cham, Switzerland, Zurich, Switzerland (May 26–30, 2024). https://doi.org/10.1007/978-3-031-58751-1_14

20. Pizer, A.: An algorithm for computing modular forms on $\Gamma_0(N)$. Journal of Algebra **64**(2), 340–390 (1980). https://doi.org/https://doi.org/10.1016/0021-8693(80)90151-9, https://www.sciencedirect.com/science/article/pii/0021869380901519
21. Robert, D.: Some applications of higher dimensional isogenies to elliptic curves (overview of results). Cryptology ePrint Archive, Report 2022/1704 (2022), https://eprint.iacr.org/2022/1704
22. Robert, D.: Breaking SIDH in polynomial time. In: Hazay, C., Stam, M. (eds.) Advances in Cryptology – EUROCRYPT 2023, Part V. Lecture Notes in Computer Science, vol. 14008, pp. 472–503. Springer, Cham, Switzerland, Lyon, France (Apr 23–27, 2023). https://doi.org/10.1007/978-3-031-30589-4_17
23. Robert, D.: On the efficient representation of isogenies (a survey). Cryptology ePrint Archive, Report 2024/1071 (2024), https://eprint.iacr.org/2024/1071
24. Silverman, J.H.: The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics, vol. 106. Springer New York, New York, NY (2009). https://doi.org/10.1007/978-0-387-09494-6, http://link.springer.com/10.1007/978-0-387-09494-6
25. Voight, J.: Identifying the Matrix Ring: Algorithms for Quaternion Algebras and Quadratic Forms. In: Alladi, K., Bhargava, M., Savitt, D., Tiep, P.H. (eds.) Quadratic and Higher Degree Forms, pp. 255–298. Springer New York, New York, NY (2013). https://doi.org/10.1007/978-1-4614-7488-3_10, https://doi.org/10.1007/978-1-4614-7488-3_10
26. Voight, J.: Quaternion Algebras, Graduate Texts in Mathematics, vol. 288. Springer International Publishing, Cham (2021). https://doi.org/10.1007/978-3-030-56694-4, https://link.springer.com/10.1007/978-3-030-56694-4
27. van der Waerden, B.L.: Die Reduktionstheorie der positiven quadratischen Formen. Acta Mathematica **96**(1), 265–309 (1956), publisher: Kluwer Academic Publishers Dordrecht
28. Wesolowski, B.: The supersingular isogeny path and endomorphism ring problems are equivalent. In: 62nd Annual Symposium on Foundations of Computer Science. pp. 1100–1111. IEEE Computer Society Press, Denver, CO, USA (Feb 7–10, 2022). https://doi.org/10.1109/FOCS52979.2021.00109
29. Wesolowski, B.: Random Walks in Number-theoretic Cryptology. HDR Thesis, ENS Lyon (2024), https://bweso.com/hdr.pdf