Problem 6

Transferring Endomorphism Rings along Isogenies

by Wouter Castryck

1 Introduction

It used to be a widespread assumption among isogenists that the knowledge of an isogeny between two elliptic curves can be used to efficiently transfer knowledge of the endomorphism ring from one curve to the other. In recent years, our understanding of what it means to "know an isogeny" has evolved. It is a stubborn open problem whether this new, relaxed understanding of what it means to know an isogeny still allows to efficiently transfer knowledge of the endomorphism ring.

2 History

Until recently, all known practical ways to represent a separable isogeny between two elliptic curves E and E' over $\mathbb{F}_q$ naturally disclosed a smooth-degree isogeny between E, E', given to us as a composition of small-degree isogenies, explicitly described by their defining polynomials. In this scenario, if the endomorphism ring of E is known then this smoothness can be exploited to extract the endomorphism ring of E' in polynomial time, and vice versa. This is not entirely straightforward, especially in the case of an isogeny of smooth-but-not-powersmooth degree, but now considered a standard reduction [EHL+18; Wes21].

Leroux [Ler22] appears to be the first to cast doubt on the slogan that isogenies inherently allow for an efficient transfer of endomorphism ring knowledge. He introduced the concept of a "suborder representation" of an isogeny φ between supersingular elliptic curves E, E' and showed that it allows to efficiently evaluate φ at any input. So it is natural to regard the isogeny as being "publicly known". However, if $\deg \varphi$ is not smooth then this representation does not come with an obvious efficient method for extracting $\mathrm{End}(E')$ from $\mathrm{End}(E)$ or vice versa. He suggested that it might be an intractable problem and proposed pSIDH, a key exchange protocol whose security relies on this intractability (now broken by a quantum attack).

This more general perspective on isogeny representations, i.e., as mere algorithms allowing for evaluation at any input, has now become the standard viewpoint. This was boosted by the higher-dimensional isogeny representations from [Rob22a], where an isogeny $\varphi : E \to E'$ is represented by its degree d

and interpolation data $(P, \varphi(P))$, with P iterating over a set of generators of a smooth-order subgroup $G \subset E$ containing at least $4d + 1$ elements: this allows for the efficient evaluation of φ at any point $P \in E$ (it is during this evaluation that the higher dimensions kick in). Anno 2026, higher-dimensional isogeny representations have become widespread, e.g., the current version of SQIsign heavily relies on it.

3 Problem statements

In the following statements, all isogenies (including non-zero endomorphisms) between two elliptic curves E, E' defined over a finite field $\mathbb{F}_q$ are thought of as evaluation algorithms that can be called at cost $\text{poly}(\log q, k, \log d)$, where d denotes the degree of the isogeny and k denotes the extension degree of the defining field of the input point $P \in E(\mathbb{F}_{q^k})$. We write $B_{p,\infty}$ for the rational quaternion algebra ramified at ∞ and the prime number p.

Problem 6: Transferring Endomorphism Rings along Isogenies

Find a classical Las Vegas algorithm which, upon input of

- *two supersingular elliptic curves E, E' over $\mathbb{F}_{p^2}$ (p prime),*
- *a maximal order $\mathcal{O} \subset B_{p,\infty}$ along with a ring isomorphism $\iota : \mathcal{O} \to \text{End}(E)$,*
- *an isogeny $\varphi : E \to E'$ of known degree d,*

returns $\beta_2, \beta_3, \beta_4 \in B_{p,\infty}$ and $b_2, b_3, b_4 \in \text{End}(E')$ such that the $\mathbb{Z}$-linear map

$$\iota' \ : \ \langle 1, b_2, b_3, b_4 \rangle_{\mathbb{Z}} \subset B_{p,\infty} \ \to \ \text{End}(E') \ : \ 1 \mapsto id, \ \beta_i \mapsto b_i \text{ for } i = 2, 3, 4$$

is an isomorphism of rings. The expected runtime of the algorithm, including the combined cost of the calls to φ or $\iota(\alpha)$ for some $\alpha \in \mathcal{O}$, should be polynomial in $\log d$ and $\log p$.

Reasonable heuristic assumptions are tolerated. In particular, it should be convenient to assume the Generalized Riemann Hypothesis (GRH) for the reasons discussed in [Wes21, §1], even though [HW26] explains how such assumptions can often be lifted. If this helps, then it can also be assumed that the factorization of d is known. The prototypical target is where $d = \deg \varphi$ is a large prime number different from p, chosen such that the extension degree of the field over which the points of $E[d]$ are defined is in the order of magnitude of d, and where φ is given using a higher-dimensional isogeny representation.

Remark. In view of [Wes21, §8] it is in fact equally fine to just return $\beta_2, \beta_3, \beta_4$, as long as the corresponding endomorphisms b_2, b_3, b_4 exist.

Problem 6 is equivalent with isogeny-to-ideal conversion (under GRH):

Problem 6.1: *Find a classical Las Vegas algorithm which, upon the same input as in Problem 6, returns generators for the kernel ideal* $I_\varphi = \{\, \alpha \in \mathcal{O} \mid \varphi \circ \iota(\alpha) = 0 \,\}$*, with an expected runtime that is polynomial in* $\log d$ *and* $\log p$*, again including the combined cost of calls to* φ *or* $\iota(\alpha)$*,* $\alpha \in \mathcal{O}$*.*

The equivalence is no surprise to specialists, e.g., this can be read along the lines of [HW26]. In a nutshell, it can be seen as follows. If I_φ is known, then by computing the right order $\mathcal{O}'$ of $I_\varphi \subset B_{p,\infty}$, we know which elements of $\mathbb{Z} + \varphi \circ \mathrm{End}(E) \circ \hat{\varphi} \subset \mathrm{End}(E')$ are divisible by an integer greater than 1. The corresponding divisions can be carried out using the methods from [Rob22b; HW26], allowing one to make the isomorphism $\iota' : \mathcal{O}' \to \mathrm{End}(E')$ effective, as wanted. Conversely, if both $\mathrm{End}(E), \mathrm{End}(E')$ are known, then one can find an isogeny $\psi : E \to E'$ of smooth degree using the KLPT algorithm [KLPT14; Wes21], consider its kernel ideal I_ψ, and then

$$I_\varphi = I_\psi \frac{\iota^{-1}(\hat{\psi} \circ \varphi)}{\deg \psi}.$$

Remark. We have stated the problems for supersingular elliptic curves only, even though they also make sense for ordinary elliptic curves, except that now the endomorphism ring is isomorphic to an order $\mathcal{O}$ in an imaginary quadratic number field, rather than a maximal order in $B_{p,\infty}$. Assuming that the factorization of d is known, these problems can be solved in polynomial time. For Problem 6.1 on isogeny-to-ideal conversion this roughly works as follows: for each prime divisor $\ell \mid d$ one can list the ideals $(\ell, \alpha) \subset \mathcal{O}$ of norm ℓ, of which there are two at most since now $\mathcal{O}$ is an imaginary quadratic order, and check which ones contain I_φ by testing whether $\varphi \circ \iota(\alpha) \circ \hat{\varphi}$ is divisible by ℓ using the method from [Rob22b; HW26]. For Problem 6 on endomorphism ring transference, in the ordinary case there is a direct polynomial-time method for computing $\mathrm{End}(E')$, see [Rob22b, §4], apart from the factorization of the discriminant of the Frobenius endomorphism on E'; but it is easily seen that, in our case, the relevant factors can be extracted from d and the knowledge of $\mathrm{End}(E)$.

4 Quantumly solved

The word "classical" was included in both problem statements because Chen, Imran, Ivanyos, Kutas, Leroux and Petit [CII+23; CP25] found a polynomial-time quantum algorithm for Problem 6.1, and therefore also for Problem 6. This rules out pSIDH for use in post-quantum cryptography. The method is quite ingenious and is based on the observation that the map

$$(\mathcal{O}/d\mathcal{O})^\times \to \{\, \text{supersingular elliptic curves} \,\},$$

sending $\alpha + d\mathcal{O}$ to the codomain of $\varphi_*\iota(\alpha)$, i.e., the push-forward of $\iota(\alpha)$ under φ, is well-defined, computable, and constant precisely on the left cosets of the subgroup of elements $\alpha + d\mathcal{O}$ for which $\alpha \in \mathbb{Z} + I_\varphi$ (here we assume φ cyclic, but this can be done w.l.o.g.). It turns out that this instance of the hidden subgroup problem in the (non-abelian!) group $(\mathcal{O}/d\mathcal{O})^\times \cong \mathrm{GL}_2(\mathbb{Z}/d\mathbb{Z})$ can be solved quantumly in polynomial time, and from this solution it is easy to extract I_φ.

Acknowledgements. Thanks to Mingjie Chen for publicizing this problem and to her and Arthur Herlédan le Merdy for helpful discussions. Wouter Castryck is supported by the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement ISOCRYPT – No. 101020788), by the Research Council KU Leuven grant C14/ 24/099, as well as by CyberSecurity Research Flanders with reference number VR20192203.

References

[CII+23] Mingjie Chen, Muhammad Imran, Gábor Ivanyos, Péter Kutas, Antonin Leroux, and Christophe Petit. "Hidden Stabilizers, the Isogeny to Endomorphism Ring Problem and the Cryptanalysis of pSIDH". In: *Advances in Cryptology – ASIACRYPT 2023*. Vol. 14440. LNCS. Springer, 2023, pp. 99–130 (cit. on p. 3).

[CP25] Mingjie Chen and Christophe Petit. "Computing the Endomorphism Ring of a Supersingular Elliptic Curve from a Full Rank Suborder". In: *Advances in Cryptology – EUROCRYPT 2025*. Vol. 15606. LNCS. Springer, 2025, pp. 446–474 (cit. on p. 3).

[EHL+18] Kirsten Eisenträger, Sean Hallgren, Kristin Lauter, Travis Morrison, and Christophe Petit. "Supersingular Isogeny Graphs and Endomorphism Rings: Reductions and Solutions". In: *Advances in Cryptology – EUROCRYPT 2018*. Ed. by Jesper Buus Nielsen and Vincent Rijmen. Vol. 10822. LNCS. Springer, 2018, pp. 329–368 (cit. on p. 1).

[HW26] Arthur Herlédan Le Merdy and Benjamin Wesolowski. "Unconditional Foundations for Supersingular Isogeny-Based Cryptography". In: *Theory of Cryptography*. Vol. 16270. LNCS. Springer, 2026, pp. 266–297 (cit. on pp. 2, 3).

[KLPT14] David Kohel, Kristin Lauter, Christophe Petit, and Jean-Pierre Tignol. "On the quaternion isogeny path problem". In: *LMS Journal of Computation and Mathematics* 17.A (2014). https://doi.org/10.1112/S1461157014000151, pp. 418–432 (cit. on p. 3).

[Ler22] Antonin Leroux. "A New Isogeny Representation and Applications to Cryptography". In: *Advances in Cryptology – ASIACRYPT 2022*. Vol. 13792. LNCS. Springer, 2022, pp. 3–35 (cit. on p. 1).

[Rob22a] Damien Robert. *Evaluating isogenies in polylogarithmic time*. Cryptology ePrint Archive, Paper 2022/1068. 2022. URL: https://eprint.iacr.org/2022/1068 (cit. on p. 1).

[Rob22b] Damien Robert. *Some applications of higher dimensional isogenies to elliptic curves (overview of results)*. Cryptology ePrint Archive, Paper 2022/1704. 2022. URL: https://eprint.iacr.org/2022/1704 (cit. on p. 3).

[Wes21] Benjamin Wesolowski. "The supersingular isogeny path and endomorphism ring problems are equivalent". In: *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)* (2021). Full version available at https://eprint.iacr.org/2021/919, pp. 1100–1111 (cit. on pp. 1–3).