Problem 5

Large-degree Isogenies from Elliptic Curves

by Wouter Castryck

1 Introduction

Given an elliptic curve E over a finite field $\mathbb{F}_q$, the easiest way to generate a primitive (i.e., not factoring through multiplication by a scalar greater than 1) high-degree isogeny emanating from E is as a composition of small-degree isogenies, computed using Vélu-type formulas, and Frobenius maps. This is then also the easiest way to represent it: one simply writes down the defining polynomials of each component. Away from smooth degrees and up to Frobenius factors, we are unaware of efficient methods for computing outgoing isogenies, except under extra assumptions on E.

2 Supersingular case

The main case where one can do better is when E is supersingular and $\mathrm{End}(E)$ is known. Then it is possible to efficiently compute primitive isogenies from E of any given degree d, so long as $\nu_p(d) \leq 1$ ($\nu_p = p$-adic valuation; if $p^2 \mid d$ then such isogenies do not exist). Indeed, one can choose a primitive (i.e., not a multiple of an ideal generated by an integer greater than 1) left ideal $I \subset \mathrm{End}(E)$ of reduced norm d and convert it into an isogeny $\varphi : E \to E'$.

Until fairly recently, all known ways of carrying out this conversion made use of the KLPT algorithm [KLPT14; Wes21], and all known ways of representing φ naturally disclosed some information about $\mathrm{End}(E)$. This situation has changed. Indeed, using the higher-dimensional isogeny representations from [Rob22a] we can now represent φ 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 is enough for the efficient evaluation of φ at any point $P \in E$ (it is during this evaluation that the higher dimensions kick in). In particular, there is no need to reveal information about $\mathrm{End}(E)$. This "zero-knowledge" feature is very attractive from a cryptographic viewpoint: e.g., it opened the door for two signature schemes [BBC+25; Ler25] in which the signature is an isogeny of large prime degree from a supersingular elliptic curve $E/\mathbb{F}_{p^2}$ whose endomorphism ring is known to the signer only. Moreover, along with the higher-dimensional machinery came the "Clapoti" technique for ideal-to-isogeny conversion [BDF+25; PR23], allowing one to by-pass the KLPT algorithm and making these signature schemes comparatively fast.

3 Ordinary case

The ordinary case comes with specific challenges; note that, here, it can always be assumed that $\mathrm{End}(E)$ is known, perhaps apart from factoring the discriminant $\Delta_q = t_E^2 - 4q$ of the q-th power Frobenius endomorphism on E [Rob22b, §4].

First, it is important to observe that, for the vast majority of positive integers d, we cannot hope for an efficient method to compute a primitive outgoing isogeny $\varphi : E \to E'$ of degree d. The main difference with the supersingular case is that ideals of norm d do not exist in general, so that φ necessarily involves "descending" steps. This will be the case if and only if d has a prime factor ℓ that is inert in $\mathrm{End}(E)$. Then unless

$$\ell \mid \Delta_q/\Delta_{\mathrm{End}(E)} \tag{5.1}$$

for all such factors ℓ, the codomain E' is necessarily defined over a strict extension field $\mathbb{F}_{q^k} \supset \mathbb{F}_q$, whose degree k is typically exponential in $\log d$. In such cases it is unreasonable to ask for an efficient method for computing a primitive d-isogeny from E.

We therefore restrict to the case where an ideal $I \subset \mathrm{End}(E)$ of norm d exists (for other meaningful variants, see [Gal25]); then the corresponding isogeny φ and codomain E' can always be defined over $\mathbb{F}_q$. While this case remains unsolved in general, the aforementioned Clapoti technique can be used for a polynomial-time method in all cases where I is invertible, i.e., corresponding to a "horizontal" isogeny [PR23].

4 Problem statements

In the following statements, an isogeny between two elliptic curves E, E' defined over a finite field $\mathbb{F}_q$ is thought of as any evaluation algorithm that can be called at cost $\mathrm{poly}(\log q, k, \log d)$, 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 first state the problem(s) in the supersingular case:

Problem 5: Large-degree Isogenies from Elliptic Curves

Find a Las Vegas algorithm which, upon input of

- *a supersingular elliptic curve $E/\mathbb{F}_{p^2}$ (p prime),*
- *a positive integer d with $\nu_p(d) \leq 1$,*

outputs an elliptic curve E' and a primitive isogeny $E \to E'$ of degree d. The expected runtime of the algorithm should be sub-exponential in $\log d$ and $\log p$.

Reasonable heuristic assumptions such as the Generalized Riemann Hypothesis (GRH) are tolerated. Likewise for quantum subroutines: a sub-exponential

quantum solution to Problem 5 would already suffice for cryptanalytic impact. But, of course, a classical polynomial-time solution would be the ideal outcome (perhaps apart from the cost of factoring d, in case this turns out to be a necessary step). The prototypical target is where d is a large prime number different from p, where even the special case $E[d] \subset E(\mathbb{F}_{p^2})$ is of great interest.

Cryptographic applications more realistically rely on the following relaxed version of the problem, in which an attacker has oracle access to a solver for Problem 5 and is asked to return an "independent" solution:

Problem 5.1: *Find a Las Vegas algorithm which, upon input of*

- *a supersingular elliptic curve $E/\mathbb{F}_{p^2}$ (p prime),*
- *a positive integer d,*

and with oracle access to a function which upon input of any positive integer e, coprime to p, returns an elliptic curve E'' and a primitive degree-e isogeny $E \to E''$, outputs the following:

- *an elliptic curve E' and a primitive isogeny $E \to E'$ of degree d whose kernel trivially intersects the kernel of any isogeny returned by the oracle,*
- *or $\perp$ if no such isogeny exists.*

The expected runtime of the algorithm should be sub-exponential in $\log d$, $\log p$ and the number of calls to the oracle.

It is not known whether Problem 5.1 is easier than Problem 5, apart from the pathological cases where the output is $\perp$ (which happens when $p^2 \mid d$ or when $\ell \mid d$ for a small prime ℓ and the oracle calls exhaust all of $E[\ell]$, kernel-wise). See the next section for a brief discussion.

Remark. The condition that the oracle can only return isogenies with domain E, resp., that the final isogeny should be independent from those returned by the oracle (rather than just different), is needed for an interesting problem: otherwise an efficient solution can be found by means of isogeny pull-backs, resp., isogeny factorizations, which can be carried out efficiently [Rob25].

In the ordinary case, we state:

Problem 5.2: *Find a Las Vegas algorithm which, upon input of*

- *an ordinary elliptic curve E over a finite field $\mathbb{F}_q$,*
- *an imaginary quadratic order $\mathcal{O}$ with an isomorphism $\iota : \mathcal{O} \to \mathrm{End}(E)$,*
- *a primitive ideal $I \subset \mathcal{O}$ of norm d,*

outputs an elliptic curve $E'/\mathbb{F}_q$ and an isogeny $E \to E'$ with kernel ideal $\iota(I)$. The expected runtime of the algorithm should be sub-exponential in $\log d$, $\log q$ and the combined cost of the calls to $\iota(\alpha)$, $\alpha \in \mathcal{O}$.

Here, the prototypical target is where d is a large prime number different from p and I is not invertible in $\mathcal{O}$.

5 Hardness

Currently, the best general approach to Problem 5 and Problems 5.1 and 5.2 is to factor d and do a piece-wise application of Vélu-type formulae. In the special case where the required kernel points can be found over the base field, using the $\sqrt{\text{élu}}$ formulae from [BDLS20] this runs in time $\tilde{O}(\ell^{1/2})$ with ℓ the largest prime factor of d. But in general the kernel points are defined over a field extension of degree $O(\ell)$ only. As explained in [Gal25; NO26], the method is then dominated by the sampling of a point of order ℓ over this field extension, which takes time $\tilde{O}(\ell^2)$.

Remark. As pointed out in [NO26], the mere construction of this field extension is even more expensive: $\tilde{O}(\ell^2)$ classically and $\tilde{O}(\ell^{5/2})$ quantumly.

Recall that Problem 5 admits a classical polynomial-time solution as soon as $\mathrm{End}(E)$ is known, so the hardness of the supersingular endomorphism ring problem is an upper bound for the hardness of Problem 5. The converse reduction is not known and most researchers expect that such a reduction would not be easy to establish. In turn, it is clear that Problem 5.1 is at most as hard as Problem 5. Again, the converse reduction is not known, but here is a loose argument why the oracle access does not make Problem 5 substantially easier: all current approaches to the supersingular endomorphism ring problem strongly rely on the computation of random large-degree isogenies, and at no point in these approaches it would come in helpful if these isogenies were of non-smooth degree (except for the Frobenius isogeny which was used, e.g., in [FIK+25]). So, at least, it seems that the oracle access does not make the supersingular endomorphism ring problem any easier.

Acknowledgements. 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

[BBC+25] Andrea Basso, Giacomo Borin, Wouter Castryck, Maria Corte-Real Santos, Riccardo Invernizzi, Antonin Leroux, Luciano Maino, Frederik Vercauteren, and Benjamin Wesolowski. "PRISM: Simple and Compact Identification and Signatures from Large Prime Degree Isogenies". In: *Public-Key Cryptography – PKC 2025*. LNCS. Springer, 2025, pp. 300–332 (cit. on p. 1).

[BDF+25] Andrea Basso, Pierrick Dartois, Luca De Feo, Antonin Leroux, Luciano Maino, Giacomo Pope, Damien Robert, and Benjamin Wesolowski. "SQIsign2D–West". In: *Advances in Cryptology – ASIACRYPT 2024*. Ed. by Kai-Min Chung and Yu Sasaki. LNCS. Springer, 2025, pp. 339–370 (cit. on p. 1).

[BDLS20] Daniel J Bernstein, Luca De Feo, Antonin Leroux, and Benjamin Smith. "Faster computation of isogenies of large prime degree". In: *Open Book Series* 4.1 (2020), pp. 39–55 (cit. on p. 4).

[FIK+25] Jenny Fuselier, Annamaria Iezzi, Mark Kozek, Travis Morrison, and Changningphaabi Namoijam. "Computing supersingular endomorphism rings using inseparable endomorphisms". In: *Journal of Algebra* 668 (2025), pp. 145–189 (cit. on p. 4).

[Gal25] Steven Galbraith. "Climbing and descending tall isogeny volcanos". In: *Research in Number Theory (Proceedings of the Fifteenth Algorithmic Number Theory Symposium, ANTS-XV)* 11 (2025). Article nr 7 (cit. on pp. 2, 4).

[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. 1).

[Ler25] Antonin Leroux. "Verifiable Random Function from the Deuring Correspondence and Higher Dimensional Isogenies". In: *Advances in Cryptology – EUROCRYPT 2025*. LNCS. Springer, 2025, pp. 167–194 (cit. on p. 1).

[NO26] Kohei Nakagawa and Hiroshi Onuki. "Attacks on PRISM-id via Torsion over Small Extension Fields". In: *Public-Key Cryptography – PKC 2026*. LNCS. Springer, 2026 (cit. on p. 4).

[PR23] Aurel Page and Damien Robert. *Introducing Clapoti(s): Evaluating the isogeny class group action in polynomial time*. IACR Cryptology ePrint Archive, Paper 2023/1766. 2023 (cit. on pp. 1, 2).

[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. 2).

[Rob25] Damien Robert. "On the Efficient Representation of Isogenies". In: *Number-Theoretic Methods in Cryptology*. Springer, 2025, pp. 3–84 (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 p. 1).