Problem 1

The Supersingular Isogeny Problem

by Benjamin Wesolowski[1]

1 Introduction

The Supersingular Isogeny Problem is *the* central hard problem underlying isogeny-based cryptography.

Informally, an "isogeny problem" is a computational problem of the following form: given two elliptic curves over the same finite field, compute, if it exists, an isogeny between them. Certain versions of this problem are believed to be hard, and isogeny-based cryptography relies on this presumed hardness. Among these, the case in which both curves are supersingular has emerged as by far the most important, and an efficient solution to this Supersingular Isogeny Problem would effectively undermine the entire field of isogeny-based cryptography.

2 History

The Supersingular Isogeny Problem first emerged as an explicit computational problem in the work of Charles, Goren, and Lauter [CGL09], where its presumed hardness was used to construct a cryptographic hash function. They approached the problem from a graph-theoretic angle.

Let p be a (large) prime, and let $\overline{\mathbb{F}}_p$ denote an algebraic closure of the finite field $\mathbb{F}_p$. Fix a small prime number ℓ (typically, $\ell = 2$). The supersingular ℓ-isogeny graph over $\overline{\mathbb{F}}_p$ is the graph whose vertices are supersingular elliptic curves over $\overline{\mathbb{F}}_p$ (up to isomorphism), and whose edges correspond to isogenies of degree ℓ between them. This graph is finite, since every supersingular elliptic curve over $\overline{\mathbb{F}}_p$ is isomorphic to one defined over $\mathbb{F}_{p^2}$.

A path in this graph can be interpreted as a composition of isogenies, each of degree ℓ. Finding such a path between two given vertices is known as the Supersingular ℓ-Isogeny Path Problem. Pizer [Piz90] proved that supersingular ℓ-isogeny graphs are Ramanujan graphs of size $O(p)$, a property that *suggests* inherent algorithmic hardness and motivated the design of [CGL09].

The best known classical algorithms for the Supersingular Isogeny Problem are essentially generic graph-search methods with complexity[2] $\tilde{O}(p^{1/2})$. Exploiting algebro-geometric structure has so far only led to reductions in memory requirements [DG16], or to practical improvements hidden within the $\tilde{O}$-notation [CCS22]. Despite major cryptanalytic advances against more struc-

[1]ENS de Lyon, CNRS, UMPA, UMR 5669, Lyon, France

[2]We use the soft-O notation $f = \tilde{O}(g)$ to signify $f = (\log g)^{O(1)} \cdot O(g)$.

tured variants "with hints" (e.g., SIDH [CD23]), the complexity of solving the plain Supersingular Isogeny Problem has remained remarkably stable.

The importance of this problem in isogeny-based cryptography has continued to grow, fueled by results showing its equivalence to many other fundamental problems in the area — an investigation initiated in [EHL+18]. Most notably, the Supersingular Isogeny Problem is equivalent to the problem of finding one (or all) non-scalar endomorphisms of a supersingular elliptic curve [PW24]. Assuming the Generalized Riemann Hypothesis, it is also equivalent to the Supersingular ℓ-Isogeny Path Problem [Wes21; PW24], which *a priori* appears harder due to additional constraints on the admissible isogenies in a solution. Each of these polynomially equivalent problems offers a distinct viewpoint on the Supersingular Isogeny Problem, yet all have so far converged to a complexity of $\tilde{O}(p^{1/2})$.

3 Problem Statement

Problem 1: The Supersingular Isogeny Problem

Given supersingular elliptic curves E and E' over a finite field $\mathbb{F}_{p^2}$, compute an explicit isogeny $\varphi : E \to E'$.

*A solution consists of either: the description of a (probabilistic) classical algorithm with time complexity $O(p^{\frac{1}{2}-\varepsilon})$ for some $\varepsilon > 0$, **or** a proof that no such algorithm can exist.*

The input to the algorithm is straightforward to specify: a standard choice is to encode elliptic curves by (short) Weierstrass equations. The output, however, requires further discussion. What does an "explicit isogeny" mean? An isogeny may be represented as a rational map, but the polynomials involved have degree $O(\deg(\varphi))$. In general, the smallest isogeny between two given supersingular elliptic curves has degree on the order of $p^{1/2}$, which is far too large to be efficiently written down as a rational map.

The classical approach has been to express large-degree isogenies as compositions of small-degree ones. For instance, a path of length n in the ℓ-isogeny graph corresponds to an isogeny of exponentially large degree $O(\ell^n)$, while its representation as a sequence of steps grows only linearly in n. A solution of this form amounts to solving the Supersingular ℓ-Isogeny Path Problem.

More recent techniques allow arbitrary isogenies to be expressed in a highly compact form, via the so-called *HD representation* (or *interpolation representation*) of isogenies [Rob22]. For the purpose of resolving the Supersingular Isogeny Problem, the precise representation of the output isogeny is immaterial, provided that it constitutes an *efficient representation*: namely, an encoding that allows one to efficiently evaluate the isogeny on any input point. See [Wes24, Definition 1.3] for a formal definition of this notion.

Acknowledgements. Benjamin Wesolowski is supported by the European Research Council under grant No. 101116169 (AGATHA CRYPTY).

References

[CCS22] Maria Corte-Real Santos, Craig Costello, and Jia Shi. "Accelerating the Delfs-Galbraith Algorithm with Fast Subfield Root Detection". In: *Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part III*. Ed. by Yevgeniy Dodis and Thomas Shrimpton. Vol. 13509. Lecture Notes in Computer Science. Springer, 2022, pp. 285–314. ISBN: 978-3-031-15981-7. DOI: 10.1007/978-3-031-15982-4_10 (cit. on p. 1).

[CD23] Wouter Castryck and Thomas Decru. "An Efficient Key Recovery Attack on SIDH". In: *Advances in Cryptology - EUROCRYPT 2023 - 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23-27, 2023, Proceedings, Part V*. Ed. by Carmit Hazay and Martijn Stam. Vol. 14008. Lecture Notes in Computer Science. Springer, 2023, pp. 423–447. ISBN: 978-3-031-30588-7. DOI: 10.1007/978-3-031-30589-4_15 (cit. on p. 2).

[CGL09] Denis Xavier Charles, Eyal Z. Goren, and Kristin E. Lauter. "Cryptographic Hash Functions from Expander Graphs". In: *J. Cryptol.* 22.1 (2009), pp. 93–113. DOI: 10.1007/S00145-007-9002-X (cit. on p. 1).

[DG16] Christina Delfs and Steven D. Galbraith. "Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$". In: *Des. Codes Cryptogr.* 78.2 (2016), pp. 425–440. DOI: 10.1007/S10623-014-0010-1 (cit. on p. 1).

[EHL+18] Kirsten Eisenträger, Sean Hallgren, Kristin E. Lauter, Travis Morrison, and Christophe Petit. "Supersingular Isogeny Graphs and Endomorphism Rings: Reductions and Solutions". In: *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part III*. Ed. by Jesper Buus Nielsen and Vincent Rijmen. Vol. 10822. Lecture Notes in Computer Science. Springer, 2018, pp. 329–368. ISBN: 978-3-319-78371-0. DOI: 10.1007/978-3-319-78372-7_11 (cit. on p. 2).

[Piz90] Arnold K Pizer. "Ramanujan graphs and Hecke operators". In: *Bulletin of the American Mathematical Society* 23.1 (1990), pp. 127–137 (cit. on p. 1).

[PW24] Aurel Page and Benjamin Wesolowski. "The Supersingular Endomorphism Ring and One Endomorphism Problems are Equivalent". In: *Advances in Cryptology - EUROCRYPT 2024 - 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zurich, Switzerland, May 26-30, 2024, Proceedings, Part VI*. Ed. by Marc Joye and Gregor Leander. Vol. 14656. Lecture Notes in Computer Science. Springer, 2024, pp. 388–417. ISBN: 978-3-031-58750-4. DOI: 10.1007/978-3-031-58751-1_14 (cit. on p. 2).

[Rob22] Damien Robert. *Evaluating isogenies in polylogarithmic time*. Cryptology ePrint Archive, Paper 2022/1068. 2022. URL: https://eprint.iacr.org/2022/1068 (cit. on p. 2).

[Wes21] Benjamin Wesolowski. "The supersingular isogeny path and endomorphism ring problems are equivalent". In: *62nd IEEE Annual Symposium on Foundations of Computer Science, FOCS 2021, Denver, CO, USA, February 7-10, 2022*. IEEE, 2021, pp. 1100–1111. ISBN: 978-1-6654-2055-6. DOI: 10.1109/FOCS52979.2021.00109 (cit. on p. 2).

[Wes24] Benjamin Wesolowski. *Random Walks in Number-theoretic Cryptology*. HDR Thesis Manuscript, École Normale Supérieure de Lyon (ENS Lyon). Lyon, France, Aug. 2024 (cit. on p. 2).