The Isogeny Problems

What particular goals will there be toward which the leading cryptographical spirits of coming generations will strive?
(after D. Hilbert, 1900)

https://isogeni.es/problems

Editor's note

This document contains the list of the seven foremost unsolved problems in the domain of isogeny-based cryptography. To obtain this list, I asked eleven experts in isogeny-based cryptography what they considered to be the most important unsolved problems in isogeny-based cryptography, and curated this list down to the seven particular problems in this document. I then asked for a short write-up in a few pages per problem to a specific expert, which resulted in the chapters you find below. These give the precise statements and descriptions per problem. Only solutions that are peer-reviewed will be accepted. The authors reserve final discretion on whether any submission constitutes a valid solution.

Rewards. There are rewards for valid solutions to these problems, and these rewards are contributed by the community via pledges. The current state of rewards is visible on the website, and new pledges can always be submitted by contacting me.[1]

Krijn Reijnders, July 2026.

By Wouter Castryck, Luca De Feo, Steven D. Galbraith, Péter Kutas, Krijn Reijnders, and Benjamin Wesolowski.

[1] reijnderskrijn@gmail.com

List of Problems

1	The Supersingular Isogeny Problem	3
2	Vectorization for Oriented Elliptic Curves	7
3	Hashing into Supersingular Curves	11
4	Optimal KLPT	15
5	Large-degree Isogenies from Elliptic Curves	19
6	Transferring Endomorphism Rings along Isogenies	25
7	Strong Encryption Protocols	30

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

[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. 4).

[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. 3).

[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. 3).

[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. 3).

[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. 4).

[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. 4).

[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. 3).

[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. 4).

[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. 4).

[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. 4).

Problem 2

Vectorization for Oriented Elliptic Curves

by Benjamin Wesolowski[1]

1 Introduction

The *Vectorization Problem for Oriented Elliptic Curves* is a central computational problem underlying isogeny-based cryptography. Informally, it asks one to invert a particular group action: that of an ideal class group acting on a set of oriented elliptic curves. While this group action is efficiently computable, no algorithm is known to efficiently recover the acting group element from its effect on an elliptic curve.

Such a "hard-to-invert" group action can often be used in cryptographic protocols as a drop-in replacement for the discrete logarithm problem, with the major advantage that it appears to resist quantum algorithms. In particular, it can turn the Diffie–Hellman protocol [DH76] into a (presumably) post-quantum key exchange, such as CSIDH [CLM+18].

2 History

The origins of this problem can be traced back to the work of Couveignes in 1997 [Cou06], who proposed constructing cryptosystems from a group action arising in the theory of complex multiplication. In this work, Couveignes defined the Vectorization Problem for ordinary elliptic curves and conjectured its hardness. This work was only made public in 2006, when Rostovtsev and Stolbunov independently rediscovered the idea [RS06]. Computing the group action appeared to be highly inefficient, rendering the proposal unsuitable for practical applications.

The situation changed with the work of Castryck, Lange, Martindale, Panny, and Renes, who introduced CSIDH [CLM+18], the first practical realization of Couveignes' idea. Their key modification was to work with supersingular elliptic curves defined over a prime-order field $\mathbb{F}_p$, rather than ordinary elliptic curves. This leap in efficiency sparked a surge of interest in group-action-based cryptography and brought the Vectorization Problem to the forefront as a concrete cryptographic assumption.

The more general notion of an *oriented elliptic curve*, and the induced group action, was introduced in 2020 by Colò and Kohel [CK20]. Let E be an elliptic curve over a finite field $\mathbb{F}_q$, and let $\mathcal{O}$ be an imaginary quadratic order. An $\mathcal{O}$-orientation of E is an injective homomorphism $\omega : \mathcal{O} \to \mathrm{End}(E)$, where $\mathrm{End}(E)$

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

denotes the endomorphism ring of E. We say that (E, ω) is an $\mathcal{O}$-oriented elliptic curve. The orientation is called *primitive* if it cannot be extended to a strictly larger order than $\mathcal{O}$. We denote by $\mathcal{E}\ell\ell_p(\mathcal{O})$ the set of isomorphism classes of primitively $\mathcal{O}$-oriented elliptic curves over the algebraic closure $\overline{\mathbb{F}}_p$. There is a natural action of the class group $\mathrm{Cl}(\mathcal{O})$ on $\mathcal{E}\ell\ell_p(\mathcal{O})$, which we denote by $\mathfrak{a} \star (E, \omega)$ for any ideal $\mathfrak{a}$. This action is free, and Onuki showed that it has at most two orbits [Onu21].

The Vectorization Problem for Oriented Elliptic Curves is then the following computational problem: given two supersingular oriented elliptic curves (E, ω) and (E', ω') over $\mathbb{F}_{p^2}$, find, if it exists, an $\mathcal{O}$-ideal $\mathfrak{a}$ such that (E', ω') is isomorphic to $\mathfrak{a} \star (E, \omega)$. In the following, let $d = |\mathrm{disc}(\mathcal{O})|$.

The difficulty of this problem is governed by two parameters: the characteristic p and the discriminant d. The fastest known algorithms depend on which of these dominates. We briefly review the main algorithmic approaches.

One of the fastest known classical algorithms for this problem is a simple meet-in-the-middle algorithm with complexity $(\log d + \log p)^{O(1)} d^{1/4}$ (see [MW25, Theorem 6] for a precise analysis, assuming the Generalized Riemann Hypothesis). However, there appears to be a significant quantum advantage for this problem. In the ordinary setting, Childs, Jao, and Soukharev [CJS14] showed that it can be solved in subexponential time[2] $(\log p)^{O(1)} \cdot L_d(1/2)$ using Kuperberg's algorithm [Kup05]. This result was later extended to the supersingular oriented setting in [MW25, Theorem 9]. In the context of post-quantum cryptographic applications, this subexponential quantum complexity is a primary driver in the selection of secure parameters.

There exists a radically different approach to solving this problem. Given the endomorphism rings of E and E', the Vectorization Problem for Oriented Elliptic Curves can be solved in polynomial time [EL24, Corollary 5]. The endomorphism rings of E and E' can be computed in time $(\log p)^{O(1)} \cdot O(p^{1/2})$ classically, or $(\log p)^{O(1)} \cdot O(p^{1/4})$ quantumly [DG16]. This is currently the fastest known approach when $\log p \ll (\log d)^{1/2}$.

These two approaches (via Kuperberg and via endomorphism rings) are the fastest known general techniques. However, better algorithms are known in special cases, for instance for orders $\mathcal{O}$ with smooth conductor in a number field of small discriminant [Wes22, Theorem 5].

3 Problem Statement

Problem 2: Vectorization for Oriented Elliptic Curves

Given a finite field $\mathbb{F}_{p^2}$, an imaginary quadratic order $\mathcal{O}$ with $d = |\mathrm{disc}(\mathcal{O})|$, and two supersingular primitively $\mathcal{O}$-oriented elliptic curves (E, ω) and (E', ω') over

[2] We use the classical subexponential L-notation $L_x(\alpha) = \exp\left(O(\log x)^{\alpha}(\log\log x)^{1-\alpha}\right)$.

Problem 2: Vectorization for Oriented Elliptic Curves

$\mathbb{F}_{p^2}$*, find, if it exists, an* $\mathcal{O}$*-ideal* $\mathfrak{a}$ *such that*

$$(E', \omega') \cong \mathfrak{a} \star (E, \omega).$$

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

The targeted complexity $(\log p)^{O(1)} \cdot L_d(1/2-\varepsilon)$ is driven by two parameters, p and d, and a solution should cover all regimes.

Note that the quantum algorithm of complexity $(\log d + \log p)^{O(1)} O(p^{1/4})$, consisting in computing the endomorphism rings first, reaches the targeted complexity in the special regime where $\log p \ll (\log d)^{1/2-\varepsilon}$. Therefore, to solve the above problem, one should focus on the complementary regime, where the fastest known strategy is currently given by Kuperberg's algorithm.

Let us briefly discuss the encoding of each element in the input and output of the Vectorization for Oriented Elliptic Curves. The order $\mathcal{O}$ can be identified with a quotient $\mathbb{Z}[X]/(f)$ where $f \in \mathbb{Z}[X]$ has degree 2. Then, the order $\mathcal{O}$ is encoded by f. Elements of $\mathcal{O}$ are themselves encoded as polynomials, and $\mathcal{O}$-ideals can be encoded by generating sets. A standard choice to encode an elliptic curve E is as a (short) Weierstrass equation. An orientation ω can be encoded as a pair (α, φ), where α is a generator of $\mathcal{O}$, and $\varphi = \omega(\alpha) \in \mathrm{End}(E)$ is an endomorphism. Concretely, the endomorphism φ could be encoded in any way that allows one to efficiently compute $\varphi(P)$ for any point $P \in E$ (we call that an *efficient representation*, see [Wes24, Definition 1.3] for a formal definition).

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

References

[CLM+18] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. "CSIDH: An Efficient Post-Quantum Commutative Group Action". In: *Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2-6, 2018, Proceedings, Part III*. Ed. by Thomas Peyrin and Steven D. Galbraith. Vol. 11274. Lecture Notes in Computer Science. Springer, 2018, pp. 395–427. ISBN: 978-3-030-03331-6. DOI: 10.1007/978-3-030-03332-3_15 (cit. on p. 7).

[CJS14] Andrew Childs, David Jao, and Vladimir Soukharev. "Constructing elliptic curve isogenies in quantum subexponential time". In: *Journal of Mathematical Cryptology* 8.1 (2014), pp. 1–29 (cit. on p. 8).

[CK20] Leonardo Colò and David Kohel. "Orienting supersingular isogeny graphs". In: *Journal of Mathematical Cryptology* 14.1 (2020), pp. 414–437 (cit. on p. 7).

[Cou06] Jean Marc Couveignes. "Hard Homogeneous Spaces". In: *IACR Cryptol. ePrint Arch.* (2006), p. 291. URL: http://eprint.iacr.org/2006/291 (cit. on p. 7).

[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. 8).

[DH76] Whitfield Diffie and Martin Hellman. "New directions in cryptography". In: *IEEE transactions on Information Theory* 22.6 (1976), pp. 644–654 (cit. on p. 7).

[EL24] Jonathan Komada Eriksen and Antonin Leroux. "Computing Orientations from the Endomorphism Ring of Supersingular Curves and Applications". In: *IACR Commun. Cryptol.* 1.3 (2024), p. 5. DOI: 10.62056/AE0FHBM0 (cit. on p. 8).

[Kup05] Greg Kuperberg. "A subexponential-time quantum algorithm for the dihedral hidden subgroup problem". In: *SIAM Journal on Computing* 35.1 (2005), pp. 170–188 (cit. on p. 8).

[MW25] Arthur Herlédan Le Merdy and Benjamin Wesolowski. "The supersingular endomorphism ring problem given one endomorphism". In: *IACR Commun. Cryptol.* 2.1 (2025), p. 6. DOI: 10.62056/AKGYIVRZN (cit. on p. 8).

[Onu21] Hiroshi Onuki. "On oriented supersingular elliptic curves". In: *Finite Fields and Their Applications* 69 (2021), p. 101777 (cit. on p. 8).

[RS06] Alexander Rostovtsev and Anton Stolbunov. "Public-Key Cryptosystem Based on Isogenies". In: *IACR Cryptol. ePrint Arch.* (2006), p. 145. URL: http://eprint.iacr.org/2006/145 (cit. on p. 7).

[Wes22] Benjamin Wesolowski. "Orientations and the Supersingular Endomorphism Ring Problem". In: *Advances in Cryptology - EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30 - June 3, 2022, Proceedings, Part III*. Ed. by Orr Dunkelman and Stefan Dziembowski. Vol. 13277. Lecture Notes in Computer Science. Springer, 2022, pp. 345–371. ISBN: 978-3-031-07081-5. DOI: 10.1007/978-3-031-07082-2_13 (cit. on p. 8).

[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. 9).

Problem 3

Hashing into Supersingular Curves

by Steven D. Galbraith[1]

1 Introduction

There are many situations in discrete-log based cryptography when one wants to "hash" to the group. One famous example is the BLS signature scheme [BLS04], where $H(m)$ is a group element and the signature is $[s]H(m)$, where s is the private key of the signer. It is also a convenient fact that one can easily set up instances of the discrete logarithm problem such that no-one knows the solution. For example, one can choose a large prime p such that 2 is a primitive root modulo p, and ask for the discrete logarithm of 3 with respect to the base 2. This allows for *untrusted setup* for schemes like Pedersen commitments. For finite fields and elliptic curves it is well-understood how to generate arbitrary group elements and hence the problem of hashing to the group is easy. For ideal class groups there are some subtleties, but it is a solved problem [SBK25].

In isogeny-based cryptography it is natural to ask if these sorts of tasks can also be performed. In the context of isogenies, this usually means generating a supersingular curve E over a given field $\mathbb{F}_{p^2}$ in such a way that nothing is known about the endomorphism ring $\mathrm{End}(E)$, not even to the person who generated the curve. For example, this is needed to use the CGL hash securely [EHL+18], for a commitment scheme [Ste21], and for many other protocols.

2 History

The problem of generating a random supersingular curve was mentioned by Love and Boneh [LB20] where they called it *demonstrating a hard curve*.

There is no good solution known to the problem. Two papers explicitly discuss unsuccessful attempts to solve the problem [BBD+24; MMP25]. Mostly these are exploring mathematical ideas that might allow one to produce a supersingular curve without leaking information, but none of the solutions is satisfactory. There is also a quantum algorithm proposed in [BBD+24], where the idea is to perform a random walk "in superposition" and then observe the quantum state so that it "collapses" to a single elliptic curve (also see [MDJ26]). One problem with that approach is that it is intrinsically non-deterministic and so can't be used as a hash function. There is also the risk that a malicious party would perform the observations a different way to learn information about the isogeny path.

[1] University of Auckland, New Zealand

To get around the lack of a solution to the problem, multi-party protocols have been developed that allow such a curve to be set up by a collection of mutually untrusting players [BD21; BCC+23; MJ23]. This approach is suitable in some contexts, but is not always an acceptable solution to the problem.

3 Problem Statement

Problem 3: Hashing into Supersingular Curves

Given a prime p, output a deterministic algorithm H that takes a random seed m as input and computes in polynomial time the j-invariant[2] of a supersingular curve E over $\mathbb{F}_{p^2}$. Any user who runs H must not learn any information about the endomorphism ring beyond the information available if they were just provided with the curve E. Similarly, any user who runs H must not learn any information to help compute an isogeny from E to any other previously fixed supersingular curve E_0 over $\mathbb{F}_{p^2}$. Or, show that such an algorithm cannot exist.

It is important to understand that a solution to this problem is an algorithm, and the main property of the algorithm is that it is secure even when run by a malicious user. For example, it is easy to write an algorithm to sample a random supersingular curve that deletes the internal state when the algorithm terminates, and only outputs E. But a malicious user who deviates from the correct execution by remembering the internal state would be able to learn $\mathrm{End}(E)$. It is also important that the person who designed the algorithm should not have any advantage over other users. For example, an algorithm that contains a hard-coded list of supersingular curves would not be acceptable, since the implementer might know $\mathrm{End}(E)$ for all the curves.

This problem is of a different nature to other isogeny problems as it is about the existence of an algorithm, rather than about the complexity of solving a computational problem. So it is unclear if there is any way to relate it to any other standard computational problem in isogeny crypto. It is also unclear whether there is any way to prove it is hard to solve the problem.

In most applications we require the set of possible outputs of H to be exponentially large. Indeed, we would ideally want the output E to be uniformly distributed (in the sense that if the seeds m are sampled uniformly from a large enough set then the output distribution $H(m)$ is arbitrarily close to uniform on the set of supersingular j-invariants).

Note that one can efficiently recognise a supersingular curve E. The obstruction to solving this problem by random sampling is that the probability that a random $j \in \mathbb{F}_{p^2}$ is supersingular is roughly 1 in $12p$, and hence one cannot reach a supersingular curve in polynomial time.

Some related problems are discussed in [GS25].

[2] Any other well-defined representative of isomorphism classes of supersingular curves could also be used instead of the j-invariant.

References

[BCC+23] Andrea Basso, Giulio Codogni, Deirdre Connolly, Luca De Feo, Tako Boris Fouotsa, Guido Maria Lido, Travis Morrison, Lorenz Panny, Sikhar Patranabis, and Benjamin Wesolowski. "Supersingular Curves You Can Trust". In: *Advances in Cryptology - EUROCRYPT 2023*. Ed. by Carmit Hazay and Martijn Stam. Vol. 14005. Lecture Notes in Computer Science. Springer, 2023, pp. 405–437. DOI: 10.1007/978-3-031-30617-4_14 (cit. on p. 12).

[BLS04] Dan Boneh, Ben Lynn, and Hovav Shacham. "Short Signatures from the Weil Pairing". In: *J. Cryptol.* 17.4 (2004), pp. 297–319. DOI: 10.1007/S00145-004-0314-9 (cit. on p. 11).

[BBD+24] Jeremy Booher, Ross Bowden, Javad Doliskani, Tako Boris Fouotsa, Steven D. Galbraith, Sabrina Kunzweiler, Simon-Philipp Merz, Christophe Petit, Benjamin Smith, Katherine E. Stange, Yan Bo Ti, Christelle Vincent, José Felipe Voloch, Charlotte Weitkämper, and Lukas Zobernig. "Failing to hash into supersingular isogeny graphs". In: *The Computer Journal* 67.8 (2024), pp. 2702–2719 (cit. on p. 11).

[BD21] Jeffrey Burdges and Luca De Feo. "Delay Encryption". In: *Advances in Cryptology - EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17-21, 2021, Proceedings, Part I*. Ed. by Anne Canteaut and François-Xavier Standaert. Vol. 12696. Lecture Notes in Computer Science. Springer, 2021, pp. 302–326. ISBN: 978-3-030-77869-9. DOI: 10.1007/978-3-030-77870-5_11 (cit. on p. 12).

[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. 11).

[GS25] Elif Ozbay Gurler and Patrick Struck. "How (not) to Build Identity-Based Encryption from Isogenies". In: *Selected Areas in Cryptography - SAC 2025 - 32nd International Conference, Toronto, ON, Canada, August 13-15, 2025, Revised Selected Papers*. Ed. by Christina Boura, Atefeh Mashatan, and Ali Miri. Vol. 16207. Lecture Notes in Computer Science. Springer, 2025, pp. 589–615.

ISBN: 978-3-032-10535-6. DOI: 10.1007/978-3-032-10536-3_22 (cit. on p. 12).

[LB20] Jonathan Love and Dan Boneh. "Supersingular curves with small noninteger endomorphisms". In: *Proceedings of ANTS, Open Book Series* 4.1 (2020), pp. 7–22 (cit. on p. 11).

[MDJ26] Maher Mamah, Jake Doliskani, and David Jao. *Spectral Theory of Isogeny Graphs and Quantum Sampling of Secure Supersingular Elliptic Curves*. Cryptology ePrint Archive, Paper 2026/171. 2026. URL: https://eprint.iacr.org/2026/171 (cit. on p. 11).

[MJ23] Youcef Mokrani and David Jao. "Generating supersingular elliptic curves over $\mathbb{F}_p$ with unknown endomorphism ring". In: *International Conference on Cryptology in India*. Springer. 2023, pp. 159–174 (cit. on p. 12).

[MMP25] Marzio Mula, Nadir Murru, and Federico Pintore. "On random sampling of supersingular elliptic curves". In: *Annali di Matematica Pura ed Applicata (1923-)* 204.3 (2025), pp. 1293–1335 (cit. on p. 11).

[SBK25] István András Seres, Péter Burcsi, and Péter Kutas. "How (Not) to Hash into Class Groups of Imaginary Quadratic Fields?" In: *Topics in Cryptology - CT-RSA 2025 - Cryptographers' Track at the RSA Conference 2025, San Francisco, CA, USA, April 28-May 1, 2025, Proceedings*. Ed. by Arpita Patra. Vol. 15598. Lecture Notes in Computer Science. Springer, 2025, pp. 303–326. ISBN: 978-3-031-88660-7. DOI: 10.1007/978-3-031-88661-4_13 (cit. on p. 11).

[Ste21] Bruno Sterner. "Commitment Schemes from Supersingular Elliptic Curve Isogeny Graphs". In: *IACR Cryptol. ePrint Arch.* 2021 (2021), p. 1031. URL: https://eprint.iacr.org/2021/1031 (cit. on p. 11).

Problem 4

Optimal KLPT

by Péter Kutas[1]

1 Introduction

The Deuring correspondence provides a relation between supersingular elliptic curves defined over $\mathbb{F}_{p^2}$ and maximal orders of the rational quaternion algebra ramified at p and infinity. More precisely, it can be described as an equivalence of categories where on the geometry side one has supersingular elliptic curves modulo Galois conjugacy (i.e., a curve is considered to be equivalent to the image curve of the Frobenius isogeny) together with isogenies as the morphism. On the algebra side, one has maximal orders together with ideals that are left ideals of one maximal order (representing the domain of the isogeny) and right ideals of another maximal order (representing the codomain of the isogeny).

From a mathematical viewpoint, the Deuring correspondence allows one to move between algebra and geometry. The algebraic viewpoint is especially useful for proving theoretical statements such as the connectedness of isogeny graphs and the number of supersingular elliptic curves. Categorical equivalences are always powerful tools for proving statements, but one might wonder how one can algorithmically move between the quaternion and the elliptic curve worlds.

Computing the endomorphism ring of a supersingular elliptic curve is supposed to be a hard problem. This in the above language means that it is hard to move from geometry to algebra. As it turns out, there is a polynomial-time algorithm that computes a supersingular elliptic curve whose endomorphism ring is a given maximal order. In order to understand this problem, we need to understand variants of the isogeny problem on the quaternion side.

There is a standard terminology (using scheme theoretical kernels) that shows how the Deuring correspondence is obtained. Here, I will show a different viewpoint that is much more useful in understanding KLPT variants. Let E_1 and E_2 be supersingular elliptic curves and let $\phi : E_1 \to E_2$ be an isogeny. The goal is to associate an algebraic object to this isogeny. The trick is to compose ϕ with $\mathrm{Hom}(E_2, E_1)$ the collection of all isogenies from E_2 to E_1. Now we obtain a collection of endomorphisms of E_1 and this set is closed under addition and post-composition by an endomorphism of E_1. This is exactly the definition of a left ideal. If I compose ϕ with $\mathrm{Hom}(E_2, E_1)$ in the other direction I get a collection of endomorphisms of E_2 which now will have the structure of a right ideal of $\mathrm{End}(E_2)$.

This viewpoint essentially shows that taking any connecting ideal essentially parametrizes all isogenies between the two elliptic curves. Furthermore, every

[1]University of Birmingham, United Kingdom, and Eötvös Loránd University, Hungary

element of the left ideal has a degree that is divisible by the degree of ϕ. In quaternion land this is translated into the definition of the norm of an ideal which is defined to be the greatest common divisor of all the norms in the ideal. This provides us with a definition of the quaternion isogeny path problem:

Problem 4.1: *Given two (isomorphism classes of) maximal orders $\mathcal{O}_1$ and $\mathcal{O}_2$, find a connecting ideal of norm ℓ^k where ℓ is a given small prime.*

This definition while correct is not very useful in practice. It is much more useful to start out with some connecting ideal I which is actually very easy to find. The drawback now is that a priori we have no real control over the norm of I. However, as described before one ideal parametrizes all isogenies in some sense. One can now simply show that the quaternion path finding problem is equivalent to finding a single element $x \in I$ such that $\mathrm{Nrd}(x) = \mathrm{Nrd}(I)\ell^k$. From now on we focus on this problem, namely given an ideal I find an element of prescribed norm.

2 Description of KLPT

Now at this point we can ask ourselves two things. First, is there a polynomial-time algorithm to find any path where k can be bounded by a function of p (independent of the representation of the ideal). The second question, can we find a path where k is the smallest possible. The distinction is more evident in a graph theoretic language. The first problem asks for any path in the ℓ-isogeny graph whereas the second asks for the shortest one. This leads us to the statement of "Optimal KLPT" as an optimal variant of Problem 4.1.

Problem 4: The Optimal Quaternion Isogeny Path Problem

Given a prime number p, a maximal order $\mathcal{O}$ and a left integral $\mathcal{O}$-ideal I, find an equivalent ideal $J \sim I$ of norm $\mathrm{Nrd}(J) = \ell^e$ where e is as small as possible.

A solution consists of either: the description of a polynomial-time algorithm, or, a proof that no such algorithm can exist.

The good news is that the easier problem can be solved in polynomial time via the KLPT algorithm. The high level idea of the KLPT algorithm is the following. Let N be the norm of the ideal I. Now we want to find an element in I whose norm is $N\ell^k$. First we choose an endomorphism σ of degree $N\ell^k$ and look at the left ideal J generated by σ and N. Now J is great as it comes equipped with an element that we would like. The problem is we want this element in I. The idea is to rotate J into I in some sense. Both I and J are locally principal ideals. When one looks at maximal orders modulo N they become isomorphic to the ring of 2×2 matrices over $\mathbb{Z}/N\mathbb{Z}$. For simplicity, KLPT uses an initial connecting ideal of prime norm, so ideals in the matrix ring are a bit easier to handle. Now viewing I and J modulo N we can view them as left ideals in the matrix ring. Due to the way I and J were chosen

they both represent non-trivial ideals (neither 0 nor the whole ring) and since 2 is a very small number every left ideal that is not trivial is 1-dimensional. Furthermore, every two non-trivial ideals differ by right multiplication by an invertible element. So now I can choose an element like that and multiply J from the right to get to I (this is my local rotation). Luckily J was nice so if this rotator matrix has norm ℓ^k I would be done. Unfortunately, this should not be the case usually. On the other hand there are two hopeful things:

1. The rotator matrix is not unique, there are several invertible elements that take one left ideal to the other
2. These elements live in $\mathcal{O}/N\mathcal{O}$, so when considered as quaternion they have infinitely many lifts to choose from

KLPT uses both observations. It chooses a very special rotator matrix and then lifts it to a power of ℓ norm quaternion.

3 Problems and Improvements

The drawback of KLPT is that the path that it returns is way longer than the optimal path. How inherent is that from the method itself. Given that I is generated by some element z and N it is natural to consider some form of lifting. The element z can be viewed as a 2×2 matrix that needs to be lifted to a quaternion of norm ℓ^k. However, in KLPT this z was obtained as a product of very special structure. So whilst lifting is some inherent in the problem, the fact that the verbatim KLPT approach can't be improved further is not a roadblock to better algorithms. Furthermore, KLPT makes several choices to ensure that the associated Diophantine equation is solvable with elementary methods. It is highly likely, that major improvements will not come from mild adjustments of KLPT.

A different approach is laid out in [BKM+24] and [AAF+26]. As described before the entire problem can be written down by one simple norm equation: representing $N\ell^k$ by the norm form of the ideal. Actually when one writes down this norm equation one can simply divide out by N and then one obtains the quadratic form associated to $\mathrm{Hom}(E_1, E_2)$ representing the integer ℓ^k. If ℓ^k is small, more precisely, smaller than $\sqrt{p}$, then this approach works very easily as it will likely be the shortest isogeny in $\mathrm{Hom}(E_1, E_2)$ and thus LLL will reveal it. If one computes an LLL reduced basis of $\mathrm{Hom}(E_1, E_2)$, then the coordinates of a short isogeny are also somewhat short. This leads to the idea of solving the quaternion norm equation using Coppersmith methods. As it turns out, if $\ell^k < p^{2/3-\varepsilon}$ for any $\varepsilon > 0$, this approach works. Unfortunately, for two random curves the expected lower bound should be around p so the above method only works in special circumstances. The drawback of this method is it treats the problem as a random Diophantine equation and likely the problem has more structure to exploit.

4 Conclusion

An optimal pathfinding algorithm would have many great applications. It would simplify maximal order to elliptic curve computations. This is of course polynomial time but costly in practice. The second application would be likely the best available SQIsign variant with all the good properties of all SQIsign variants. In some sense it would be the "Book" version of SQIsign using the terminology of Erdős.

The lack of an optimal KLPT algorithm is a major gap in our algorithmic understanding of the Deuring correspondence. In my humble of opinion, as the SIDH showed the right way to interpret torsion point information, an optimal KLPT will show how to properly view the Deuring correspondence.

Acknowledgements. Péter Kutas is partially supported by Engineering and Physical Sciences Research Council (EPSRC) grant number EP/V011324/1. Péter Kutas is supported by the Ministry of Culture and Innovation and the National Research, Development, and Innovation Office within the Quantum Information National Laboratory of Hungary (Grant No. 2022-2.1.1-NL-2022-00004). Péter Kutas is also supported by the NRDIO grant "EXCELLENCE-151343".

References

[AAF+26] Marius A Aardal, Diego F Aranha, Yansong Feng, Yiming Gao, and Yanbin Pan. "Better Bounds for Finding Fixed-Degree Isogenies via Coppersmith's Method". In: (2026), pp. 541–572 (cit. on p. 17).

[BKM+24] Benjamin Benčina, Péter Kutas, Simon-Philipp Merz, Christophe Petit, Miha Stopar, and Charlotte Weitkämper. "Improved algorithms for finding fixed-degree isogenies between supersingular elliptic curves". In: *Annual International Cryptology Conference*. Springer. 2024, pp. 183–217 (cit. on p. 17).

Problem 5

Large-degree Isogenies from Elliptic Curves

by Wouter Castryck[1]

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

[1] COSIC, KU Leuven, Belgium

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

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

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 $\log p$. Or, show that such an algorithm cannot exist.

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 $\log d$, $\log q$, including 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 formulas. In the special case where the required kernel points can be found over the base field, using the $\sqrt{\text{élu}}$ formulas 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: $\tilde{O}(\ell^3)$ 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. 19).

[BDF+25] Andrea Basso, Pierrick Dartois, Luca De Feo, Antonin Leroux, Luciano Maino, Giacomo Pope, Damien Robert, and Benjamin Wesolowski. "SQIsign2D–West: The Fast, the Small, and the Safer". In: *Advances in Cryptology – ASIACRYPT 2024*. Ed. by Kai-Min Chung and Yu Sasaki. LNCS. Springer, 2025, pp. 339–370 (cit. on p. 20).

[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. 22).

[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. 22).

[Gal25] Steven D. 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. 20, 22).

[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. 19).

[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. 19).

[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. 22).

[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 p. 20).

[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. 19).

[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. 20).

[Rob25] Damien Robert. "On the Efficient Representation of Isogenies". In: *Number-Theoretic Methods in Cryptology*. Springer, 2025, pp. 3–84 (cit. on p. 21).

[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. 19).

Problem 6

Transferring Endomorphism Rings along Isogenies

by Wouter Castryck[1]

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 one 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 one 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

[1]COSIC, KU Leuven, Belgium

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). As of 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

$$\iota' \ : \ \langle 1, \beta_2, \beta_3, \beta_4 \rangle_{\mathbb{Z}} \subset B_{p,\infty} \ \to \ \text{End}(E') \ : \ 1 \mapsto \text{id}, \ \beta_i \mapsto b_i \text{ for } i = 2, 3, 4$$

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 $\log p$. Or, show that such an algorithm cannot exist.

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* $I_\varphi = \{\, \alpha \in \mathcal{O} \mid \iota(\alpha)(\ker \varphi) = 0 \,\}$*, 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. 27).

[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. 27).

[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. 25).

[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. 26, 27).

[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. 27).

[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. 25).

[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. 26).

[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. 27).

[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 pp. 25–27).

Problem 7

Strong Encryption Protocols

by Luca De Feo[1]

1 Introduction

Construct public key encryption (nearly) as secure as SQIsign.

2 History

The journy of isogeny-based key exchange and public key encryption (PKE) has been bumpy. The Couveignes–Rostovtsev–Stolbunov [Cou06; RS06] key exchange started the whole field. Today, it is understood as one instantiation of a cryptographic group action, together with CSIDH [CLM+18], SCALLOP [FFK+23], PEGASIS [DEF+25], etc. It is a simple and elegant scheme whose security reduces to the group-action analogue of CDH, or even of discrete logarithm, thanks to a quantum reduction [GPSV18]. However, group-action-discrete-log is solved in quantum subexponential time by Kuperberg's algorithm, which is less than ideal.

SIDH [JD11] initiated the trend of isogeny-based key exchange based on "experimental" assumptions. It took 10 years for the experiment to terminate with a non-passing grade [CD23; MMP+23; Rob23]. Since then, several "fixes" to SIDH have emerged [FMP23; BF23; BMP23; BM25]. What they've got over group actions, is exponential quantum security, and thus (to varying degrees) small ciphertexts and public keys. However they are all based on some isogeny-with-torsion-information type of assumption [DFP24], unnervingly reminiscent of SIDH.

20+ years of research on isogeny-based crypto have singled out the Supersingular Isogeny Problem as the gold standard for a post-quantum assumption. The problem is now known to be equivalent to the *supersingular endomorphism ring problem (EndRing)* [Wes21], and the best quantum algorithms essentially amount to Grover search over the solution space [DG16; BJS14]. Despite this, **we only know how to build signatures whose security reduces to (nearly) EndRing** [BCC+23; ABD+25]. Ok, signatures and a handful of related primitives.

[1]IBM Research Europe, Zurich, Switzerland

3 Problem Statement

Ideally, a solution to this problem would be a key exchange or PKE/KEM whose security reduces to EndRing, no strings attached. However this is probably asking too much: the security of PKEs is defined via a deciding game, thus a reduction to a decisional problem is to be expected, but the obvious decisional version of EndRing is easy to decide.

The Random Oracle Model (ROM) can often be leveraged to reduce a distinguishing problem to a search problem, e.g., in the well known reduction of hashed ElGamal's IND-CPA to CDH. We're ready to accept a proof in the ROM, as we are to accept one in an even more powerful model such as the Algebraic Isogeny Model [ABD+25]. Quantum reductions are of course allowed.

Problem 7: Strong Encryption Protocols

Define a Key Exchange or Public Key Encryption / Key Encapsulation Mechanism and prove its passive / IND-CPA security reduces to the supersingular endomorphism ring problem (EndRing) via quantum polynomial reductions.

You are permitted use of:

- *The Generalized/Extended Riemann Hypothesis;*
- *Any standard symmetric assumptions on block/stream ciphers and hash functions;*
- *The Random Oracle Model;*
- *The Algebraic Isogeny Model.*

Or, show that such a scheme cannot exist.

Efficiency of the scheme and tightness of the reduction are not criteria taken into account for this problem.

And if none of this is sufficient, we also accept as a solution a proof of impossibility of achieving key exchange or PKE/KEM based on EndRing in a *sufficiently credible* model. Because an abstract computation model must inevitably be formulated for this, and because opinions may vary on what "sufficiently credible" means, adjudging such a solution is left to the discretion of the proposers.

If we feel particularly inspired, we may even accept solutions that invoke extra assumptions, as long as they are widely accepted as "insignificant" in the face of EndRing. An example of such assumptions may be the "EndRing with hints" used to prove security of SQIsign [ABD+25]. Again, given the subjectivity of this criterion, we reserve full discretion in interpreting it.

Ultimately, the spirit of the problem is: **create PKE as secure as SQIsign**. As long as SQIsign is secure, that is... So don't be shy and submit your solution, if you feel it matches the description.

References

[ABD+25] Marius A. Aardal, Andrea Basso, Luca De Feo, Sikhar Patranabis, and Benjamin Wesolowski. "A Complete Security Proof of SQIsign". In: *Advances in Cryptology - CRYPTO 2025 - 45th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2025, Proceedings, Part VI*. Ed. by Yael Tauman Kalai and Seny F. Kamara. Vol. 16005. Lecture Notes in Computer Science. Springer, 2025, pp. 190–222. ISBN: 978-3-032-01886-1. DOI: 10.1007/978-3-032-01887-8_7 (cit. on pp. 30, 31).

[BCC+23] Andrea Basso, Giulio Codogni, Deirdre Connolly, Luca De Feo, Tako Boris Fouotsa, Guido Maria Lido, Travis Morrison, Lorenz Panny, Sikhar Patranabis, and Benjamin Wesolowski. "Supersingular Curves You Can Trust". In: *Advances in Cryptology - EUROCRYPT 2023*. Ed. by Carmit Hazay and Martijn Stam. Vol. 14005. Lecture Notes in Computer Science. Springer, 2023, pp. 405–437. DOI: 10.1007/978-3-031-30617-4_14 (cit. on p. 30).

[BF23] Andrea Basso and Tako Boris Fouotsa. "New SIDH Countermeasures for a More Efficient Key Exchange". In: *Advances in Cryptology - ASIACRYPT 2023 - 29th International Conference on the Theory and Application of Cryptology and Information Security, Guangzhou, China, December 4-8, 2023, Proceedings, Part VIII*. Ed. by Jian Guo and Ron Steinfeld. Vol. 14445. Lecture Notes in Computer Science. Springer, 2023, pp. 208–233. ISBN: 978-981-99-8741-2. DOI: 10.1007/978-981-99-8742-9_7 (cit. on p. 30).

[BM25] Andrea Basso and Luciano Maino. "POKÉ: A Compact and Efficient PKE from Higher-Dimensional Isogenies". In: *Advances in Cryptology - EUROCRYPT 2025 - 44th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Madrid, Spain, May 4-8, 2025, Proceedings, Part II*. Ed. by Serge Fehr and Pierre-Alain Fouque. Vol. 15602. Lecture Notes in Computer Science. Springer, 2025, pp. 94–123. ISBN: 978-3-031-91123-1. DOI: 10.1007/978-3-031-91124-8_4 (cit. on p. 30).

[BMP23] Andrea Basso, Luciano Maino, and Giacomo Pope. "FESTA: Fast Encryption from Supersingular Torsion Attacks". In: *Advances in Cryptology – ASIACRYPT 2023*. Ed. by Jian Guo and Ron Steinfeld. Vol. 14444. Lecture Notes in Computer Science. Springer, 2023, pp. 98–126. DOI: 10.1007/978-981-99-8739-9_4 (cit. on p. 30).

[BJS14] Jean-François Biasse, David Jao, and Anirudh Sankar. "A Quantum Algorithm for Computing Isogenies between Supersingular Elliptic Curves". In: *Progress in Cryptology - INDOCRYPT 2014 - 15th International Conference on Cryptology in India, New Delhi,*

India, December 14-17, 2014, Proceedings. Ed. by Willi Meier and Debdeep Mukhopadhyay. Vol. 8885. Lecture Notes in Computer Science. Springer, 2014, pp. 428–442. ISBN: 978-3-319-13038-5. DOI: 10.1007/978-3-319-13039-2_25 (cit. on p. 30).

[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. 30).

[CLM+18] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. "CSIDH: An Efficient Post-Quantum Commutative Group Action". In: *Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2-6, 2018, Proceedings, Part III*. Ed. by Thomas Peyrin and Steven D. Galbraith. Vol. 11274. Lecture Notes in Computer Science. Springer, 2018, pp. 395–427. ISBN: 978-3-030-03331-6. DOI: 10.1007/978-3-030-03332-3_15 (cit. on p. 30).

[Cou06] Jean Marc Couveignes. "Hard Homogeneous Spaces". In: *IACR Cryptol. ePrint Arch.* (2006), p. 291. URL: http://eprint.iacr.org/2006/291 (cit. on p. 30).

[DEF+25] Pierrick Dartois, Jonathan Komada Eriksen, Tako Boris Fouotsa, Arthur Herlédan Le Merdy, Riccardo Invernizzi, Damien Robert, Ryan Rueger, Frederik Vercauteren, and Benjamin Wesolowski. "PEGASIS: Practical Effective Class Group Action using 4-Dimensional Isogenies". In: *Advances in Cryptology - CRYPTO 2025 - 45th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2025, Proceedings, Part I*. Ed. by Yael Tauman Kalai and Seny F. Kamara. Vol. 16000. Lecture Notes in Computer Science. Springer, 2025, pp. 67–99. ISBN: 978-3-032-01854-0. DOI: 10.1007/978-3-032-01855-7_3 (cit. on p. 30).

[DFP24] Luca De Feo, Tako Boris Fouotsa, and Lorenz Panny. "Isogeny Problems with Level Structure". 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. 181–204. ISBN: 978-3-031-58750-4. DOI: 10.1007/978-3-031-58754-2_7 (cit. on p. 30).

[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. 30).

[FFK+23] Luca De Feo, Tako Boris Fouotsa, Péter Kutas, Antonin Leroux, Simon-Philipp Merz, Lorenz Panny, and Benjamin Wesolowski. "SCALLOP: Scaling the CSI-FiSh". In: *Public-Key Cryptography - PKC 2023 - 26th IACR International Conference on Practice and Theory of Public-Key Cryptography, Atlanta, GA, USA, May 7-10, 2023, Proceedings, Part I*. Ed. by Alexandra Boldyreva and Vladimir Kolesnikov. Vol. 13940. Lecture Notes in Computer Science. Springer, 2023, pp. 345–375. ISBN: 978-3-031-31367-7. DOI: 10.1007/978-3-031-31368-4_13 (cit. on p. 30).

[FMP23] Tako Boris Fouotsa, Tomoki Moriya, and Christophe Petit. "M-SIDH and MD-SIDH: Countering SIDH Attacks by Masking Information". 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. 282–309. ISBN: 978-3-031-30588-7. DOI: 10.1007/978-3-031-30589-4_10 (cit. on p. 30).

[GPSV18] Steven D. Galbraith, Lorenz Panny, Benjamin Smith, and Frederik Vercauteren. "Quantum Equivalence of the DLP and CDHP for Group Actions". In: *IACR Cryptol. ePrint Arch.* (2018), p. 1199. URL: https://eprint.iacr.org/2018/1199 (cit. on p. 30).

[JD11] David Jao and Luca De Feo. "Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies". In: *Post-Quantum Cryptography - 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, November 29 - December 2, 2011. Proceedings*. Ed. by Bo-Yin Yang. Vol. 7071. Lecture Notes in Computer Science. Springer, 2011, pp. 19–34. ISBN: 978-3-642-25404-8. DOI: 10.1007/978-3-642-25405-5_2 (cit. on p. 30).

[MMP+23] Luciano Maino, Chloe Martindale, Lorenz Panny, Giacomo Pope, and Benjamin Wesolowski. "A Direct Key Recovery Attack on SIDH". In: *Advances in Cryptology – EUROCRYPT 2023. Part V*. Ed. by Carmit Hazay and Martijn Stam. Vol. 14008. Lecture Notes in Computer Science. Springer, 2023, pp. 448–471. DOI: 10.1007/978-3-031-30589-4_16 (cit. on p. 30).

[Rob23] Damien Robert. "Breaking SIDH in Polynomial Time". 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. Lec-

ture Notes in Computer Science. Springer, 2023, pp. 472–503. ISBN: 978-3-031-30588-7. DOI: 10.1007/978-3-031-30589-4_17 (cit. on p. 30).

[RS06] Alexander Rostovtsev and Anton Stolbunov. "Public-Key Cryptosystem Based on Isogenies". In: *IACR Cryptol. ePrint Arch.* (2006), p. 145. URL: http://eprint.iacr.org/2006/145 (cit. on p. 30).

[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. 30).