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 is 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 $\mathcal{O}$ of discriminant d, and two supersingular primitively $\mathcal{O}$-oriented elliptic curves (E, ω) and (E', ω') over

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

$\mathbb{F}_{p^2}$, *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 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 curves 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

[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. 2).

[CK20] Leonardo Colò and David Kohel. "Orienting supersingular isogeny graphs". In: *Journal of Mathematical Cryptology* 14.1 (2020), pp. 414–437 (cit. on p. 1).

[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. 1).

[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. 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. 2).

[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. 1).

[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/AE0FHBMO (cit. on p. 2).

[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. 2).

[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. 2).

[Onu21] Hiroshi Onuki. "On oriented supersingular elliptic curves". In: *Finite Fields and Their Applications* 69 (2021), p. 101777 (cit. on p. 2).

[RS06] Alexander Rostovtsev and Anton Stolbunov. *Public-key cryptosystem based on isogenies*. Cryptology ePrint Archive, Paper 2006/145. 2006. URL: https://eprint.iacr.org/2006/145 (cit. on p. 1).

[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. 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. 3).