SUPERSINGULAR ISOGENY GRAPHS IN CRYPTOGRAPHY
ARIZONA WINTER SCHOOL 2026
PROJECT DESCRIPTIONS

KIRSTEN EISENTRÄGER AND GABRIELLE SCULLARD

Last updated: January 26, 2026

1. Preparation for the Winter School

For almost all of our proposed projects, it is essential to have some experience with Magma. Magma has a free, limited use online calculator here

`http://magma.maths.usyd.edu.au/calc/`.

It is even better is to obtain a copy for your laptop. The Simons Foundation has made Magma freely available to mathematicians working in the US

`http://magma.maths.usyd.edu.au/magma/ordering/`.

The IT staff in your department should be able to help you obtain a copy of Magma through this agreement.

Several of the proposed projects deal with algorithms for computing endomorphism rings. We recommend looking at [ES26, EHL+20, BCNE+19, HW25, Tu11].

It is also helpful to have some familiarity with quaternion algebras (see [Voi21], especially Chapter 23 Section 5 on the Bruhat-Tits tree and Chapter 42 on supersingular elliptic curves).

2. Projects

The first two projects deal with aspects of computing endomorphism rings of supersingular elliptic curves. Beside being of intrinsic interest, computing the endomorphism ring of a supersingular elliptic curve has become a central problem in isogeny-based cryptography. There are several ways to compute endomorphism rings. Computing the endomorphism ring of a supersingular elliptic curve E was first studied by Kohel [Koh96, Theorem 75], who gave an approach for generating a subring of finite index of the endomorphism ring $\mathrm{End}(E)$. The algorithm is based on finding cycles in the ℓ-isogeny graph of supersingular elliptic curves in characteristic p and runs in time $O(p^{1+\varepsilon})$. In [ES26] we completed Kohel's approach by showing how to compute $\mathrm{End}(E)$ from a suborder. This algorithm runs in time polynomial in $\log p$, the logarithm of the degrees of the generators of the suborder and the largest prime and largest exponent in the factorization of the discriminant of the suborder. It built on [EHL+20] which gave a subexponential algorithm, under certain heuristics, if the input suborder was Bass. In [FIK+25], it is shown that under GRH, a Bass suborder of $\mathrm{End}(E)$ can be computed in $O(p^{1/2+\varepsilon})$ time. In a different direction, one can attempt to compute $\mathrm{End}(E)$ by constructing a generating set. Endomorphisms of E correspond to cycles through E in an isogeny graph. One example of a cycle-finding algorithm for

Date: January 26, 2026.

computing powersmooth endomorphisms with complexity $\tilde{O}(p^{1/2})$ and polynomial storage is given by Delfs and Galbraith [DG16]. In [GPS17] it is argued that heuristically one expects $O(\log p)$ calls to a cycle finding algorithm until the cycles generate $\mathrm{End}(E)$. In [FIK+25], a basis for $\mathrm{End}(E)$ is found that involves inseparable endomorphisms. Page and Wesolowski give an unconditional probabilistic algorithm for the computation of the full endomorphism ring whose complexity is $\tilde{O}(p^{1/2})$ [PW24].

2.1. **Computing the endomorphism ring of a supersingular curve from a subring.** The first project is to implement an example of the main algorithm, Algorithm 8.1, from [ES26]. This is a deterministic algorithm that computes the endomorphism ring of a supersingular elliptic curve, given two non-commuting endomorphisms and a factorization of the reduced discriminant of the order they generate.

In Section 8 of [ES26], an example is computed with the following setup: Let $p = 103$ and let E be the elliptic curve with j-invariant 69, given by the model $y^2 = x^3 + 37x + 38$. For this choice of p, $B_{p,\infty}$ has a $\mathbb{Q}$-basis of the form $\{1, i, j, ij\}$ with $i^2 = -1$ and $j^2 = -103$. The goal is to compute a maximal order $\tilde{\mathcal{O}} \subset B_{p,\infty}$ with $\tilde{\mathcal{O}} \cong \mathrm{End}(E)$, given a subring $\mathcal{O}_0$ of finite index. In the example in [ES26] we start with the order $\mathcal{O}_0 \subset B_{p,\infty}$ which is given by the basis

$$\left\{1, -11095 - \frac{21}{2}i - 11095j - \frac{7}{2}ij, -49 - \frac{49}{2}i - 49j - \frac{49}{2}ij, \frac{107653}{2} + \frac{107653}{2}ij\right\}.$$

This order can be shown to be contained in $\tilde{\mathcal{O}}$. Here, we are implicitly using an isomorphism of $\mathcal{O}_0$ into $\mathrm{End}(E) \otimes \mathbb{Q}$ for which j maps to the Frobenius π_p and $7i$ to an endomorphism of degree 7. This example was constructed completely on the quaternion side to have certain properties (in particular: for $q \mid \mathrm{discrd}(\mathcal{O}_0)$, one can easily describe an embedding $\mathcal{O}_0 \otimes \mathbb{Z}_q \to M_2(\mathbb{Z}_q)$).

The goal of the first project is to implement another example:

- The example in [ES26] is done almost entirely in terms of orders of $B_{p,\infty}$ rather than actual endomorphisms of the given curve E. It would be interesting to have an example set up on the endomorphism side, e.g. by constructing the basis endomorphisms as cycles in isogeny graphs. (See [BCNE+19, p. 57] for the supersingular isogeny graph with $p = 103$.)

  The starting point would be to generate an order $\mathcal{O}_0$ whose reduced discriminant is non-maximal by taking two noncommuting endomorphisms which are given by a composition of isogenies.
- Warm-Up: Let $p = 103$. Fix a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$. Construct an order $\mathcal{O}_0 \subset B_{p,\infty}$ such that $\mathcal{O}_0 \subset \mathrm{End}(E)$ and $\mathrm{discrd}(\mathcal{O}_0)$ is divisible by a few primes besides p. The example is most illustrative if $\mathcal{O}_0$ is Bass at some primes and not at others. One way to do this is to start by using Magma to construct a list of all maximal orders up to isomorphism in $B_{p,\infty}$ and determining an order $\mathcal{O}$ which is isomorphic to $\mathrm{End}(E)$. Then one can use Magma functions to construct suborders of specified index. Then run the algorithm [ES26, Algorithm 8.1] to compute the endomorphism ring. Here, checking that β/n is an endomorphism means checking that $\beta/n \in \mathcal{O}$.
- More Challenging: Rather than constructing the order on the quaternion side (which involved knowing $\mathrm{End}(E)$ already), construct a suborder $\mathcal{O}_0 \subset \mathrm{End}(E)$ by finding

two noncommuting nonbacktracking cycles in an isogeny graph. Cycles should be given as a composition of isogenies of prime or prime power degree. Again, the goal is to construct an order which is Bass at some primes and not at others. Then use the algorithm to compute the endomorphism ring. This will require embeddings $f_q : \mathcal{O}_0 \otimes \mathbb{Z}_q \to M_2(\mathbb{Q}_q)$ as described in [ES26, Appendix B].

2.2. **Magma implementation of endomorphism ring algorithm.** A second project would be a general Magma implementation of any cycle finding algorithm in an isogeny graph and of Algorithm 8.1 in [ES26]. Those two parts would give an algorithm for computing supersingular endomorphism rings. The main obstacle for an efficient implementation of Algorithm 8.1 is that computing higher-dimensional isogenies in the necessary generality (dimension 8) to determine if an endomorphism is a scalar multiple of another endomorphism is not yet implemented. Given an endomorphism β and an integer n we need to determine when β/n is an endomorphism. When the parameters ($\deg(\beta)$ and n) are small enough, one can determine if β/n is an endomorphism by evaluating β on $E[n]$ instead, but for the general case one would need higher-dimensional isogenies as in [ES26, Appendix A].

2.3. **Statistics on when a suborder of $B_{p,\infty}$ is Bass.** The third project deals with how often two noncommuting cycles in isogeny graphs generate a suborder of the endomorphism ring that has extra properties. This is of interest because the problem of computing the endomorphism ring of a supersingular elliptic curve from a finite index subring can be solved more efficiently if the input order has special properties that force more structure.

Here are several definitions of orders in quaternion algebras in which we will be interested. We say that $\mathcal{O}$ is an *Eichler order* if $\mathcal{O} \subseteq B$ is the intersection of two (not necessarily distinct) maximal orders. The *codifferent* of an order is defined as $\operatorname{codiff}(\mathcal{O}) = \{\alpha \in B : \operatorname{Trd}(\alpha\mathcal{O}) \subseteq \mathbb{Z}\}$. Following [Voi21, Definition 24.2.1], we say that $\mathcal{O}$ is *Gorenstein* if the lattice $\operatorname{codiff}(\mathcal{O})$ is invertible as a lattice as in [Voi21, 24.1.1]. An order $\mathcal{O}$ is *Bass* if every superorder $\mathcal{O}' \supseteq \mathcal{O}$ is Gorenstein.

We will be interested in the situtation when the input order Λ is locally a Bass order. The main property of local Bass orders that is interesting for us is that there are at most $e+1$ maximal orders containing a local Bass order $\Lambda \otimes \mathbb{Z}_q$, where $e = v_q(\operatorname{discrd}(\Lambda))$ is the valuation of the reduced discriminant of Λ (see [Brz83]). Let $\Lambda \otimes \mathbb{Z}_q \subseteq M_2(\mathbb{Q}_q)$ be a Bass $\mathbb{Z}_q$-order, and $e \coloneqq v_q(\operatorname{discrd}(\Lambda))$.

We can use the Bruhat-Tits tree $\mathcal{T}$ to compute the maximal superorders of $\Lambda \otimes \mathbb{Z}_q$. The vertices of $\mathcal{T}$ are in bijection with maximal orders in $M_2(\mathbb{Q}_q)$.

If $\Lambda \otimes \mathbb{Z}_q \subseteq M_2(\mathbb{Q}_q)$ is a Bass $\mathbb{Z}_q$-order, the subgraph of maximal orders containing $\Lambda \otimes \mathbb{Z}_q$ forms a path which can be recovered efficiently [EHL+20]. There it is shown that when $\Lambda \otimes \mathbb{Z}_q$ is Bass and Eichler, i.e. $\Lambda \otimes \mathbb{Z}_q = \mathcal{O} \cap \mathcal{O}'$ for local maximal orders $\mathcal{O}, \mathcal{O}'$, then the $e+1$ maximal orders containing $\Lambda \otimes \mathbb{Z}_q$ are exactly the vertices on the path from $\mathcal{O}$ to $\mathcal{O}'$. If $\Lambda \otimes \mathbb{Z}_q$ is Bass but not Eichler, then there are either 1 or 2 maximal orders containing $\Lambda \otimes \mathbb{Z}_q$ by [Brz83, Proposition 3.1, Corollary 3.2, and Corollary 4.3], and they form a path as well.

In [ES26, Algorithm 8.1], when the input order is Bass, one can find $\operatorname{End}(E) \otimes \mathbb{Z}_q$ with a binary search on orders in the path. In this case, one can find $\operatorname{End}(E) \otimes \mathbb{Z}_q$ in $O(\log_2(e))$ applications of the division algorithm, which is an improvement on $O(eq)$ applications in the non-Bass case.

For some large primes p and orders generated by 100 pairs of noncommuting endomorphisms in a specific cycle-finding algorithm in 2-isogeny graph for characteristic p, [EHL$^+$20, Section 5.3] summarizes the number of those orders which are Bass. This project would be to generate more data and try to prove that a certain proportion of orders generated will be Bass. In [FIK$^+$25], another case is considered where a Bass order is created using inseparable endomorphisms, but we would like to focus on using separable endomorphisms.

References

[BCNE$^+$19] Efrat Bank, Catalina Camacho-Navarro, Kirsten Eisenträger, Travis Morrison, and Jennifer Park. Cycles in the supersingular ℓ-isogeny graph and corresponding endomorphisms. In *Research directions in number theory—Women in Numbers IV*, volume 19 of *Assoc. Women Math. Ser.*, pages 41–66. Springer, Cham, [2019] ©2019.

[Brz83] Juliusz. Brzeziński. On orders in quaternion algebras. *Comm. Algebra*, 11(5):501–522, 1983.

[DG16] Christina Delfs and Steven D. Galbraith. Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$. *Des. Codes Cryptography*, 78(2):425–440, February 2016.

[EHL$^+$20] Kirsten Eisenträger, Sean Hallgren, Chris Leonardi, Travis Morrison, and Jennifer Park. Computing endomorphism rings of supersingular elliptic curves and connections to path-finding in isogeny graphs. In *ANTS XIV—Proceedings of the Fourteenth Algorithmic Number Theory Symposium*, volume 4 of *Open Book Ser.*, pages 215–232. Math. Sci. Publ., Berkeley, CA, 2020.

[ES26] Kirsten Eisenträger and Gabrielle Scullard. Connecting Kani's lemma and path-finding in the Bruhat-Tits tree to compute supersingular endomorphism rings, 2026. Expanded and revised preprint, `https://arxiv.org/pdf/2402.05059`.

[FIK$^+$25] Jenny Fuselier, Annamaria Iezzi, Mark Kozek, Travis Morrison, and Changningphaabi Namoijam. Computing supersingular endomorphism rings using inseparable endomorphisms. *J. Algebra*, 668:145–189, 2025.

[GPS17] Steven D. Galbraith, Christophe Petit, and Javier Silva. Identification protocols and signature schemes based on supersingular isogeny problems. In *Advances in cryptology—ASIACRYPT 2017. Part I*, volume 10624 of *Lecture Notes in Comput. Sci.*, pages 3–33. Springer, 2017.

[HW25] Arthur Herlédan Le Merdy and Benjamin Wesolowski. The supersingular endomorphism ring problem given one endomorphism. *IACR Communications in Cryptology*, 2(1), 2025.

[Koh96] David Kohel. *Endomorphism rings of elliptic curves over finite fields*. PhD thesis, University of California, Berkeley, 1996.

[PW24] Aurel Page and Benjamin Wesolowski. The supersingular endomorphism ring and one endomorphism problems are equivalent. *Advances in cryptology—EUROCRYPT 2024. Part VI*, 2024.

[Tu11] Fang-Ting Tu. On orders of $M(2, K)$ over a non-Archimedean local field. *Int. J. Number Theory*, 7(5):1137–1149, 2011.

[Voi21] John Voight. *Quaternion algebras*, volume 288 of *Graduate Texts in Mathematics*. Springer, Cham, [2021] ©2021.