AWS 2026 – SUPERSINGULAR ISOGENY GRAPHS IN CRYPTOGRAPHY

KIRSTEN EISENTRÄGER
PROJECT ASSISTANT: GABRIELLE SCULLARD

1. Course Introduction

Cryptosystems based on supersingular isogenies are one viable option for use in post-quantum cryptography. These systems rely on the hardness of computing isogenies between supersingular elliptic curves. The purpose of this lecture series is to present recent advances in this field, with a particular emphasis on the graph-theoretic perspective and reductions to other computational problems. One central related problem on which we will focus is the supersingular endomorphism ring problem.

Cryptographic applications based on the hardness of computing isogenies between supersingular elliptic curves were first given in [CGL09], which constructed a hash function from the ℓ-isogeny graph of supersingular elliptic curves. In the construction of the hash function, finding preimages was connected to finding certain ℓ-power isogenies (for ℓ a small prime) between supersingular elliptic curves.

Proposals for post-quantum key-exchange, signature and encryption schemes based on computing isogenies of supersingular elliptic curves were given by De Feo, Jao and Plût in [DFJP14a]. This scheme, referred to as SIDH (Supersingular isogeny Diffie-Hellman), was the only isogeny-based system submitted to the initial NIST Post-quantum cryptography standardization call. In SIDH, the underlying hard problem is finding paths in the isogeny graph when certain torsion-point information is revealed. It was broken in July 2022 [CD23, MMP$^+$23, Rob23a]. The groundbreaking idea for the break of SIDH relied on moving this problem into a more flexible framework using isogenies between products of elliptic curves, via Kani's Lemma. Since the break, these techniques have been applied to more general problems like computing supersingular endomorphism rings [ES25, HLMW23, PW23]. They have also been exploited in the construction of other post-quantum signature schemes, such as SQISignHD [DLRW24].

For distinct primes p and ℓ, we can define the supersingular isogeny graph $G(p, \ell)$ as follows:

Definition. *The graph $G(p, \ell)$ is a directed graph whose vertex set and edges are defined as follows:*

1. *The vertex set is the set of isomorphism classes of supersingular elliptic curves over the finite field $\overline{\mathbb{F}}_p$.*
2. *The directed edges are isogenies of degree ℓ. Here, edges from a given vertex are defined up to $\overline{\mathbb{F}}_p$-isomorphism of the codomain.*

The graph $G(p, \ell)$ is connected and $(\ell + 1)$-regular for outgoing edges, while the existence of curves of j-invariant 0 or 1728 with additional automorphisms implies a reduced number of

incoming edges at these vertices if either j-invariant is supersingular. Most importantly, these graphs are Ramanujan graphs, which means that random walks quickly reach the uniform distribution. Given two arbitrary supersingular elliptic curves E and E' it is believed to be hard to find a path in $G(p, \ell)$ connecting them. This is the ℓ-isogeny Path-finding problem, and it is the underlying hardness assumption for many of the isogeny-based systems that have been proposed.

Problem 1 (**ℓ-isogeny Path-Finding Problem).** *Given a prime p and two supersingular curves E, E' defined over $\mathbb{F}_{p^2}$, find a path from E to E' in the supersingular ℓ-isogeny graph.*

Under the generalized Riemann hypothesis, it can be shown that this problem is equivalent to the following:

Problem 2 (**The Supersingular Endomorphism Ring Problem).** *Given a prime p and a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$, find four endomorphism of E, given in an efficient representation, that generate* $\mathrm{End}(E)$ *as a lattice.*

2. Course outline

Here is a tentative outline of lectures.

Lecture 1: Introduction to isogeny-based cryptography and overview. Supersingular endomorphism rings, Deuring correspondence, supersingular isogeny graphs and their properties. References: [Deu41, Piz90, Piz98, dFJP14b], [Voi21, Chapter 42.4].

Lecture 2: Pathfinding in isogeny graphs and the endomorphism ring problem. Reductions. References: [EHL$^+$18, Wes21].

Lecture 3: Solving the endomorphism ring problem locally. Finding local solutions in the Bruhat-Tits tree. References: [Tu11, Voi13, ES25, PW24].

Lecture 4: Divisibility tests using higher-dimensional isogenies. Approaches for computing endomorphism rings from subrings. References: [Rob23b, EHL$^+$20, HLMW23, ES25].

3. Projects

Gabrielle Scullard will be the project assistant. We will have projects that involve the global side, i.e. vertices in the the supersingular ℓ-isogeny graph and their endomorphism rings, and corresponding local information obtained from the Bruhat-Tits tree at a prime q and certain subtrees. We will post lecture notes and more details about projects several weeks before the Winter School. Students in this project group should prepare by reading the lecture notes ahead of time.

References

[CD23] Wouter Castryck and Thomas Decru. An efficient key recovery attack on SIDH. In *Advances in cryptology—EUROCRYPT 2023. Part V*, volume 14008 of *Lecture Notes in Comput. Sci.*, pages 423–447. Springer, Cham, 2023.

[CGL09] Denis X. Charles, Eyal Z. Goren, and Kristin Lauter. Cryptographic hash functions from expander graphs. *J. Cryptology*, 22(1):93–113, 2009.

[Deu41] Max Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Univ. Hamburg*, 14(1):197–272, 1941.

[DFJP14a] Luca De Feo, David Jao, and Jérôme Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *J. Math. Cryptol.*, 8(3):209–247, 2014.

[dFJP14b] Luca de Feo, David Jao, and Jérôme Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *J. Math. Cryptol.*, 3(3):209–247, 2014.

[DLRW24] Pierrick Dartois, Antonin Leroux, Damien Robert, and Benjamin Wesolowski. SQIsignHD: new dimensions in cryptography. In *Advances in cryptology—EUROCRYPT 2024. Part I*, volume 14651 of *Lecture Notes in Comput. Sci.*, pages 3–32. Springer, Cham, [2024] ©2024.

[EHL+18] Kirsten Eisenträger, Sean Hallgren, Kristin Lauter, Travis Morrison, and Christophe Petit. Supersingular isogeny graphs and endomorphism rings: reductions and solutions. In *Advances in cryptology—EUROCRYPT 2018. Part III*, volume 10822 of *Lecture Notes in Comput. Sci.*, pages 329–368. Springer, Cham, 2018.

[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.

[ES25] Kirsten Eisenträger and Gabrielle Scullard. Connecting Kani's lemma and path-finding in the Bruhat-Tits tree to compute supersingular endomorphism rings, 2025. Preprint.

[HLMW23] Arthur Herlédan Le Merdy and Benjamin Wesolowski. The supersingular endomorphism ring problem given one endomorphism. Cryptology ePrint Archive, Paper 2023/1448, 2023. `https://eprint.iacr.org/2023/1448`.

[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*, volume 14008 of *Lecture Notes in Comput. Sci.*, pages 448–471. Springer, Cham, [2023] ©2023.

[Piz90] Arnold K. Pizer. Ramanujan graphs and Hecke operators. *Bull. Amer. Math. Soc. (N.S.)*, 23(1):127–137, 1990.

[Piz98] Arnold K. Pizer. Ramanujan graphs. In *Computational perspectives on number theory (Chicago, IL, 1995)*, volume 7 of *AMS/IP Stud. Adv. Math.*, pages 159–178. Amer. Math. Soc., Providence, RI, 1998.

[PW23] Aurel Page and Benjamin Wesolowski. The supersingular endomorphism ring and one endomorphism problems are equivalent. Cryptology ePrint Archive, Paper 2023/1399, 2023. `https://eprint.iacr.org/2023/1399`.

[PW24] Aurel Page and Benjamin Wesolowski. The supersingular endomorphism ring and one endomorphism problems are equivalent. In *Advances in cryptology—EUROCRYPT 2024. Part VI*, volume 14656 of *Lecture Notes in Comput. Sci.*, pages 388–417. Springer, Cham, [2024] ©2024.

[Rob23a] Damien Robert. Breaking SIDH in polynomial time. In *Advances in cryptology—EUROCRYPT 2023. Part V*, volume 14008 of *Lecture Notes in Comput. Sci.*, pages 472–503. Springer, Cham, [2023] ©2023.

[Rob23b] Damien Robert. Some applications of higher dimensional isogenies to elliptic curves, Preprint, 2023.

[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.

[Voi13] John Voight. Identifying the matrix ring: algorithms for quaternion algebras and quadratic forms. In *Quadratic and higher degree forms*, volume 31 of *Dev. Math.*, pages 255–298. Springer, New York, 2013.

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

[Wes21] Benjamin Wesolowski. The supersingular isogeny path and endomorphism ring problems are equivalent. *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1100–1111, 2021.