A Survey of Literature on Supersingular Isogeny Graphs

Sarah Arpin
Graduate Student at the University of Colorado Boulder
Sarah.Arpin@colorado.edu

1 Classical Literature

1.1 Deuring

[Deu41]

- The "Deuring Correspondence": The endomorphism ring of a supersingular elliptic curve over $\mathbb{F}_{p^2}$ is isomorphic to a maximal order in the quaternion algebra which ramifies precisely at p and ∞.

1.2 Waterhouse

[Wat69]

- General reference for abelian varieties over finite fields. Includes many proofs of foundations.

1.3 Pizer

[Piz80]

- Pizer wrote down the generators for the quaternion algebra ramified at p and ∞ for the different congruence classes of $p \pmod 8$.

1.4 Ibukiyama

[Ibu82]

- Gives a classification of the maximal orders of a definite quaternion algebra ramified at m which contain an element with minimal polynomial $x^2 + m$.
- This is particularly interesting for $m = p$, as it classifies the orders which correspond to endomorphism rings of elliptic curves defined over $\mathbb{F}_p$.

1.5 Kohel

[Koh96]

- Kohel thoroughly covers both ordinary and supersingular elliptic curves in his thesis.

2 Initial Proposals

2.1 Hash Functions – Charles, Goren, Lauter

[CGL06]

- Using the hard problem of path-finding in Ramanujan graphs to construct cryptographic hash functions.

2.2 Key Exchange – De Feo, Jao, Plût

[FJP11]

- A key-exchange protocol using the supersingular elliptic curve isogeny graph.

3 Research based on the above

3.1 On the Correspondence between Supersingular Elliptic Curves and maximal quaternionic Orders – Cerviño

[Cer04]

- This paper connects three different ways of considering the endomorphism rings of supersingular elliptic curves: Endomorphism rings, orders in quaternion algebras, and ternary quadratic forms. This connection is used to compute endomorphism rings of elliptic curves.

- The main result is an algorithm for going from a prime number p to a list of supersingular j-invariants over $\overline{\mathbb{F}}_p$ together with a 4-tuple that forms a $\mathbb{Z}$-basis for the maximal order of $B(p, \infty)$ that corresponds to $\mathrm{End}(E_j)$.

3.2 Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$ – Delfs & Galbraith

[DG13]

- This paper primarily focuses on the supersingular ℓ-isogeny graph where the isomorphism classes and isogenies are all defined over $\mathbb{F}_p$. These graphs are not a priori connected, and Delfs and Galbraith show that if you add isogenies of prime degree up to $6\log(|d|)^2$, where d is the discriminant of the $\mathbb{F}_p$-endomorphism ring. This is discussed at the bottom of page 8, in section 3: The supersingular isogeny problem.

- This paper collects information about the $\mathbb{F}_p$-endomorphism rings of supersingular elliptic curves. The $\mathbb{F}_p$-endomorphism ring is an order in the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$, so there are only two possibilities: $\mathrm{End}_{\mathbb{F}_p}(E) \cong \mathbb{Z}[\sqrt{-p}]$ or $\mathrm{End}_{\mathbb{F}_p}(E) \cong \mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$, with the latter option only possible for $p \equiv 3 \pmod 4$.

- Determining the possible endomorphism rings means much is known about the structure of the $\mathbb{F}_p$-supersingular ℓ-isogeny graph: there can only be at most two "levels", for example (see the definition on page 4).

- This paper is also a good reference for the class number formulas.

- Includes pictures and worked out examples of the isogeny graphs defined over $\mathbb{F}_p$.

3.3 Explicit representation of the endomorphism rings of supersingular elliptic curves – Lauter & McMurdy

[LM], [McM14]

- The first paper was 2004 work with both Lauter and McMurdy, and the second one expands upon this work.

- The paper includes explicit isomorphisms between the endomorphism ring of a supersingular elliptic curve and the corresponding maximal order in a quaternion algebra. They do this for one representative elliptic curve for every congruence class of p, and then they demonstrate how to use the isogenies to determine the maximal orders of isogenous elliptic curves.

- The end result is a method to simultaneously generate the entire supersingular isogeny graph at the same time as the corresponding graph of maximal orders in a quaternion algebra.

3.4 Cycles in the supersingular ℓ-isogeny graph and corresponding endomorphisms – Bank, Camacho-Navarro, Eisentraeger, Morrison, Park

[BCE$^+$18]

- This is a paper from WIN-4.
- From their abstract: *We prove a necessary and sufficient condition for the two endomorphisms corresponding to two cycles to be linearly independent, expanding on the work in Kohel's thesis. We also give a criterion under which the order generated by two cycles is not a maximal order.*
- Includes lots of pictures of examples, and examples of the correspondence of the endomorphism rings with maximal orders in a quaternion algebra.

3.5 Supersingular Isogeny Graphs and Endomorphism Rings: Reductions and Solutions – Eisentraeger, Hallgren, Lauter, Morrison, Petit

[EHL$^+$18]

- This paper provides a good summary of what the hard problems are and the relationships are between them. It also proves new reductions of some of the hard problems, for example: in section 5 the three hard problems listed below are reduced to each other:
  1. a constructive version of Deuring's correspondence from j-invariants of supersingular elliptic curves over $\overline{\mathbb{F}}_p$ to maximal orders in the quaternion algebra ramified at p and ∞.
  2. the endomorphism ring computation problem
  3. the preimage and collision resistance of the hash function from [CGL06], for a randomly chosen initial vertex.
- In section 6, they show that constructing paths in the ℓ-isogeny graph reduces to a computation of the maximal order corresponding to the endomorphism ring, as well as knowing how the generators of that order act on the ℓ-torsion of the curve.
- In section 7, there are heuristics on one direction of the Deuring correspondence (from quaternion orders to j-invariants)
- In section 8, they define what a "compact representation" of an endomorphism ring is, and show that endomorphisms rings can be expressed with bases of compactly represented endomorphisms.

3.6 On isogeny graphs of supersingular elliptic curves over finite fields – Adj, Ahmadi, Menezes

[AAM18]

- This paper consider the supersingular ℓ-isogeny graph where the vertex isomorphism classes and isogenies are both defined over $\mathbb{F}_{p^2}$, as opposed to $\overline{\mathbb{F}}_p$.
- They look at subgraphs with vertices representing elliptic curves of specific traces: $t = 0, -p, p, -2p, 2p$. For $t = 0, -p, p$, the subgraphs are small enough that the structures can be completely described. For $t = 2p, -2p$ these graphs are larger and there are some issues with $j = 0$ and $j = 1728$.
- I am a little confused here - I think normally the vertex isomorphism class is $\overline{\mathbb{F}}_p$, so each vertex is an isomorphism class of curves with different traces? I need to do a little more background reading on this topic again. I remember being confused about this before.

3.7 Ramanujan graphs in cryptography– Costache, Feigon, Lauter, Massierer, Puskas

[CFL$^+$18]

- Another WIN-4 paper!
- [CGL06] originally proposed two types of expander graphs to work on: Lubotzky-Phillips-Sarnak (LPS) graphs and supersingular isogeny graphs (Pizer). The LPS graphs were quickly attacked, but not the supersingular isogeny graphs. This paper explores whether the attacks on LPS graphs can be used adjusted for use on supersingular isogeny graphs.
- This paper also compares the hard problems used to ensure the security of [FJP11] and [CGL06]. In particular, Theorem 3.2 shows that the security of the key exchange proposed in [FJP11] depends on the hardness of the path-finding problem in supersingular isogeny graphs stated in [CGL06].
- This paper has thorough background and historical information.
- This paper also goes through how to construct supersingular isogeny graphs and LPS graphs as graphs on double cosets.

3.8 Li, Ouyang, Xu Subgraph Work

[LOX19b], [LOX19a]

- In these two works, the authors describe the number of $\mathbb{F}_p$-vertices which are ℓ-isogenous to $\mathbb{F}_p$-vertices, for any prime ℓ.
- The first work deals with $j = 0, 1728$, and the second work generalizes from there.
- Both works (but especially the second) make use of Ibukiyama's classification of the maximal orders of a definite quaternion algebra ramified at p. In particular, the maximal orders which represent endomorphism rings of $\mathbb{F}_p$ curves can always be written down in one of two forms, $\mathcal{O}(q)$ or $\mathcal{O}'(q)$.

3.9 How Not To Break SIDH – Chloe Martindale and Lorenz Panny

[MP19]

- Recent paper reviewing attack algorithms and why they don't work. Excellent summary article.
- Failed attempts that don't use auxiliary points:
  - $\mathbb{F}_p$-subgraph 'compass'
  - Lifting to characteristic 0
  - Weil restrictions
- Failed attempts that use the auxiliary points:
  - Interpolation
  - Group-theoretic approaches
  - Petit's attack, from "Faster algorithms for isogeny problems using torsion point images"

3.10 Adventures in Supersingularland - Sarah Arpin, Catalina Camacho-Navarro, Kristin Lauter, Joelle Lim, Kristina Nelson, Travis Scholl, Jana Sotáková

[ACNL+19]

- Authors explore four main attributes of the graph:
  - How does the $\mathbb{F}_p$-graph fit into the $\overline{\mathbb{F}_p}$-graph?
  - How many paths pass through $\mathbb{F}_p$-points of the graph?
  - How far are conjugate j-invariants?
  - What is the actual diameter of these graphs?

References

[AAM18] Gora Adj, Omran Ahmadi, and Alfred Menezes. On isogeny graphs of supersingular elliptic curves over finite fields. Cryptology ePrint Archive, Report 2018/132, 2018. https://eprint.iacr.org/2018/132.

[ACNL+19] Sarah Arpin, Catalina Camacho-Navarro, Kristin Lauter, Joelle Lim, Kristina Nelson, Travis Scholl, and Jana Sotáková. Adventures in supersingularland, 2019.

[BCE+18] E. Bank, C. Camacho-Navarro, K. Eisentraeger, T. Morrison, and J. Park. Cycles in the supersingular ℓ-isogeny graph and corresponding endomorphisms. *ArXiv e-prints*, April 2018. http://adsabs.harvard.edu/abs/2018arXiv180404063B.

[Cer04] Juan Marcos Cerviño. On the Correspondence between Supersingular Elliptic Curves and maximal quaternionic Orders. *ArXiv e-prints*, April 2004. https://arxiv.org/abs/math/0404538.

[CFL+18] Anamaria Costache, Brooke Feigon, Kristin Lauter, Maike Massierer, and Anna Puskas. Ramanujan graphs in cryptography. Cryptology ePrint Archive, Report 2018/593, 2018. https://eprint.iacr.org/2018/593.

[CGL06] Denis Charles, Eyal Goren, and Kristin Lauter. Cryptographic hash functions from expander graphs. Cryptology ePrint Archive, Report 2006/021, 2006. https://eprint.iacr.org/2006/021.

[Deu41] Max Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkorper. *Abh. Math. Sem. Hansischen Univ.*, 14:197–272, 1941.

[DG13] C. Delfs and S. D. Galbraith. Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$. *ArXiv e-prints*, October 2013. https://arxiv.org/pdf/1310.7789.pdf.

[EHL+18] Kirsten Eisentraeger, Sean Hallgren, Kristin Lauter, Travis Morrison, and Christophe Petit. Supersingular isogeny graphs and endomorphism rings: reductions and solutions. Cryptology ePrint Archive, Report 2018/371, 2018. https://eprint.iacr.org/2018/371.

[FJP11] Luca De Feo, David Jao, and Jérôme Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. Cryptology ePrint Archive, Report 2011/506, 2011. https://eprint.iacr.org/2011/506.

[Ibu82] Tomoyoshi Ibukiyama. On maximal orders of division quaternion algebras over the rational number field with certain optimal embeddings. *Nagoya Math. J.*, 88:181–195, 1982.

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

[LM] Kristin Lauter and Ken McMurdy. Explicit generators for endomorphism rings of supersingular elliptic curves. https://phobos.ramapo.edu/~kmcmurdy/research/ss_endomorphisms.pdf.

[LOX19a] Songsong Li, Yi Ouyang, and Zheng Xu. Endomorphism rings of supersingular elliptic curves over $\mathbb{F}_p$, 2019.

[LOX19b] Songsong Li, Yi Ouyang, and Zheng Xu. Neighborhood of the supersingular elliptic curve isogeny graph at $j = 0$ and 1728, 2019.

[McM14] Ken McMurdy. Explicit representation of the endomorphism rings of supersingular elliptic curves, August 2014. https://pdfs.semanticscholar.org/5de9/19a374a9676dcd63ad426415d276e22a2d69.pdf.

[MP19] Chloe Martindale and Lorenz Panny. How to not break sidh. Cryptology ePrint Archive, Report 2019/558, 2019. https://eprint.iacr.org/2019/558.

[Piz80] Arnold Pizer. An algorithm for computing modular forms on $\gamma_0(n)$. *Journal of Algebra*, Vol. 64, Issue 2, June 1980. https://www.sciencedirect.com/science/article/pii/0021869380901519.

[Wat69] William C. Waterhouse. Abelian varieties over finite fields. *Ann. Sci. Ecole Norm. Sup.*, 2:521–560, 1969.