

1163-11-847

Sarah Arpin* (sarah.arpin@colorado.edu), **Catalina Camacho-Navarro**, **Kristin Lauter**,
Joelle Lim, **Kirstina Nelson**, **Travis Scholl** and **Jana Sotáková**. *Adventures in
Supersingularland: An investigation into the Structure of Supersingular Isogeny Graphs.*

In this work we study isogeny graphs of supersingular elliptic curves. Supersingular isogeny graphs were introduced as a hard problem into cryptography by Charles, Goren, and Lauter for the construction of cryptographic hash functions [CGL06]. We consider two related graphs that help us understand the structure: the ‘spine’ S , which is the subgraph of the usual l -isogeny graph given by the j -invariants in \mathbb{F}_p , and the graph in which both curves and isogenies must be defined over \mathbb{F}_p . We show how to pass from the latter to the former. The graph S is relevant for cryptanalysis because routing between vertices in \mathbb{F}_p is easier than in the full isogeny graph. We provide an analysis of the distances of connected components of S . We study the involution on the l -isogeny graph that is given by the Frobenius of \mathbb{F}_p and give heuristics on how often shortest paths between two conjugate j -invariants are preserved by this involution (mirror paths). We also study the related question of what proportion of conjugate j -invariants are l -isogenous for $l=2,3$. This data is related to later work of Eisentraeger, Hallgren, Leonardi, Morrison, and Park. (Received September 13, 2020)