Orienting supersingular isogeny graphs

Leonardo Colò and David Kohel

Supersingular isogeny graphs have been used in the Charles–Goren–Lauter cryptographic hash function and the supersingular isogeny Diffie–Hellman (SIDH) protocol of De Feo and Jao. A recently proposed alternative to SIDH is the commutative supersingular isogeny Diffie–Hellman (CSIDH) protocol, in which the isogeny graph is first restricted to $\mathbb{F}_p$-rational curves E and $\mathbb{F}_p$-rational isogenies then oriented by the quadratic subring $\mathbb{Z}[\pi] \subset \mathrm{End}(E)$ generated by the Frobenius endomorphism $\pi : E \to E$.

We introduce a general notion of orienting supersingular elliptic curves and their isogenies, and use this as the basis to construct a general oriented supersingular isogeny Diffie-Hellman (OSIDH) protocol. We describe the structure of this oriented isogeny graph and its navigation using isogeny chains and modular curve equations.