1135-VS-2593 **Kirsten Eisentraeger**, **Sean Hallgren** and **Travis Morrison*** (txm950@psu.edu), Penn State University, Mathematics Department, University Park, PA 16802. *Computing isogenies and endomorphism rings of supersingular elliptic curves.*

NIST is currently soliciting submissions of post-quantum cryptographic protocols, meaning cryptosystems which would be secure even against a quantum computer. Some suggested cryptosystems are believed secure due to the hardness of computing isogenies between supersingular elliptic curves. Breaking these systems reduces to the problems of either computing an isogeny of prime-power degree between two given supersingular elliptic curves, or computing the endomorphism ring $End(E)$ (meaning return a maximal order of a quaternioin algebra isomorphic to $End(E)$) of a supersingular elliptic curve E. These problems are deeply related, and are often referred to as equivalent problems. In joint work with Kirsten Eisentraeger and Sean Hallgren, we study the size of these objects, which is necessary to have meaningful reductions. Additionally, we give a reduction from the problem of computing a ℓ-power isogeny between supersingular curves for a prime ℓ to the problem of, given a supersingular curve E, computing both the maximal order isomorphic to $End(E)$ along with its action on $E[\ell]$. Thus we reduce the problem of computing isogenies to a problem of computing endomorphism rings, meaning knowing $End(E)$ algebraically along with a little bit of its geometric information. (Received September 26, 2017)