1176-11-252 **Annamaria Iezzi**, **Jenny Fuselier**, **Mark Kozek**, **Travis Morrison*** (tmo@vt.edu) and **Changningphaabi Namoijam**. *Computing the endomorphism ring of a supersingular elliptic curve.* Preliminary report.

A large-scale quantum computer will render our currently deployed public-key cryptosystems insecure, due to Shor's algorithm for factoring and solving discrete logarithms. Post-quantum cryptosystems, on the other hand, run on classical computers (like smartphones, laptops, or servers), but are based on problems conjectured to be hard even for quantum computers. One such family of cryptosystems, isogeny-based cryptography, bases its security on the supposed difficulty of computing an isogeny between two given supersingular elliptic curves. The isogeny problem can be solved given an algorithm which computes the endomorphism ring of a given supersingular elliptic curve. In this talk, I will discuss various approaches to computing the endomorphism ring of a supersingular elliptic curve. (Received January 24, 2022)