1147-11-480 **Travis Morrison*** (travis.morrison@uwaterloo.ca). *Computing isogenies and endomorphism rings of supersingular elliptic curves.*

A sufficiently large quantum computer will break our currently deployed public key cryptosystems, like RSA and elliptic curve cryptography. Some proposed cryptosystems, believed to be secure even against quantum computers, base their security on the hardness of computing isogenies between supersingular elliptic curves. In this talk, I will discuss how endomorphism rings of supersingular elliptic curves can be used to compute isogenies. I will also discuss a new algorithm for computing supersingular endomorphism rings. (Received January 24, 2019)