1163-00-1550 **Aaron Hutchinson*** (a5hutchi@uwaterloo.ca). *Optimizations of the CSIDH Key Exchange Protocol.*

The Commutative Supersingular Isogeny-based Diffie-Hellman (CSIDH) protocol was proposed in 2018 as a post-quantum key exchange algorithm analogous to the original Diffie-Hellman algorithm. To perform the exchange, CSIDH makes use of isogenies between supersingular elliptic curves defined over a finite field $\mathbb{F}_p$, where $p = 4\ell_1 \cdots \ell_n - 1$ with $\ell_1, \ldots, \ell_n$ being distinct small odd primes. In this talk, we give an overview of the CSIDH algorithm and detail optimization methods which reduce the computational cost associated to computing the isogenies required within the protocol for both parties. In particular, we see how optimal strategies proposed for SIDH can be adapted for use in CSIDH, and we examine how permuting the primes ℓ_i within the protocol can yield increased performance. (Received September 15, 2020)