1163-11-1608 **Kristin E Lauter*** (klauter@microsoft.com), **Travis Morrison**, **Christophe Petit**, **Kirsten Eisentraeger** and **Sean Hallgren**. *Supersingular isogeny graphs and endomorphism rings.*

Progress on developing quantum computers at scale forces us to consider what hard problems in mathematics our next generation of cryptographic systems will be based on. Supersingular Isogeny Graphs were proposed for use in cryptography in 2006 by Charles, Goren, and Lauter. The hard problem is finding paths in these graphs, i.e. routing. There are no known subexponential algorithms to solve this problem, either classically or on a quantum computer. For this reason, cryptosystems based on the hardness of problems on Supersingular Isogeny Graphs are currently under consideration for standardization in the NIST Post-Quantum Cryptography (PQC) Competition. This talk will introduce these graphs, explain how the security of the Key Exchange protocol depends on the hardness of the path-finding problem, and show an equivalence with the problem of computing endomorphism rings of supersingular elliptic curves. (Received September 15, 2020)