1125-11-1129 **Kristin Estella Lauter*** (klauter@microsoft.com). *Supersingular Isogeny Graphs and Quantum Arithmetic.*

The National Institute of Standards and Technology (NIST) will be running an international competition over the next few years to select a new system for Post-Quantum Cryptography (PQC). One of the possible candidates is based on the hardness of finding isogenies between supersingular elliptic curves. This hard problem was first proposed by Charles-Goren-Lauter in 2006 as the basis for a new cryptographic hash function construction. The isogeny graph of supersingular elliptic curves can be interpreted in terms of Brandt matrices representing Hecke operators acting on spaces of modular forms. The idea behind the cryptographic applications is to use the hardness of finding paths in these Ramanujan graphs (or inverting random walks) as a way to construct a one-way function. The hard problem is then to find paths in the graph, given the starting and ending point. In this talk, we will discuss an algorithm for path-finding in the related Ramanujan graphs constructed by Lubotzky-Phillips-Sarnak, and highlight a surprising connection with quantum arithmetic. (Received September 15, 2016)