1161-11-296 **Kristin E Lauter*** (klauter@microsoft.com), **Brooke Feigon**, **Anamaria Costache**, **Maike Massierer** and **Anna Puskas**. *Ramanujan Graphs in Cryptography.*

Quantum computers force us to consider what hard problems in mathematics our next generation of cryptographic systems can be based on. Supersingular Isogeny Graphs were proposed for use in cryptography in 2006 by Charles, Goren, and Lauter. Supersingular Isogeny Graphs are examples of Ramanujan graphs, which are optimal expander graphs. These graphs have the property that relatively short walks on the graph approximate the uniform distribution, and for this reason, walks on expander graphs are often used as a good source of randomness in computer science. But the reason these graphs are important for cryptography is that finding paths in these graphs, i.e. routing, is hard: 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 and explain how the security of the Key Exchange protocol depends on the hardness of the routing problem. It will also explain an alternate description of these graphs in terms of quaternion algebras, and in terms of Bruhat-Tits trees. (Received August 18, 2020)