Supersingular Isogeny Graphs in Cryptography

Kristin Lauter, Microsoft Research

Abstract: As we move towards a world where quantum computers can be built at scale, we are forced to consider the question of 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. 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, and have advanced to the second round of the competition. This talk will introduce these graphs, the cryptographic applications, and the various algorithmic approaches which have been tried to attack these systems.