1147-11-920 **Anamaria Costache** (anamaria.costache@bristol.ac.uk), **Brooke Feigon** (bfeigon@ccny.cuny.edu), **Kristin E Lauter*** (klauter@microsoft.com), **Maike Massierer** (maike.massierer@gmail.com) and **Anna Puskas** (puskas@math.umass.edu). *Ramanujan Graphs In Cryptography.*

This talk will address the security of a proposal for Post-Quantum Cryptography from both a number theoretic and cryptographic perspective. Charles–Goren–Lauter in 2006 [CGL06] proposed two hash functions based on the hardness of finding paths in Ramanujan graphs. One is based on Lubotzky–Phillips–Sarnak (LPS) graphs and the other one is based on Supersingular Isogeny Graphs. A 2008 paper by Petit–Lauter–Quisquater breaks the hash function based on LPS graphs. On the Supersingular Isogeny Graphs proposal, recent work has continued to build cryptographic applications on the hardness of finding isogenies between supersingular elliptic curves. A 2011 paper by De Feo–Jao–Plut proposed SIDH, a cryptographic system based on Supersingular Isogeny Diffie–Hellman as well as a set of five hard problems. In this paper we show that the security of the SIDH proposal relies on the hardness of the SIG path-finding problem introduced in [CGL06]. In addition, similarities between the number theoretic ingredients in the LPS and Pizer constructions suggest that the hardness of the path-finding problem in the two graphs may be linked. By viewing both graphs from a number theoretic perspective, we identify the similarities and differences between the Pizer and LPS graphs. (Received January 29, 2019)