1035-11-1953 **Kristin E Lauter*** (klauter@microsoft.com), One Microsoft Way, Redmond, WA 98052.

Applications of Ramanujan graphs in Cryptography.

This talk will explain a new construction of secure cryptographic hash functions from Ramanujan graphs with a certain property. We propose constructing provable collision resistant hash functions from expander graphs in which finding cycles is hard. As examples, we give two specific families of optimal expander graphs for provable collision resistant hash function constructions: the families of Ramanujan graphs constructed by Lubotzky-Phillips-Sarnak and Pizer respectively. When the hash function is constructed from one of Pizer's Ramanujan graphs, (the set of supersingular elliptic curves over $\mathbb{F}_{p^2}$ with ℓ-isogenies, ℓ a prime different from p), then collision resistance follows from hardness of computing isogenies between supersingular elliptic curves. For the LPS graphs, the underlying hard problem is a representation problem in group theory. Constructing the hash functions from optimal expander graphs implies that the outputs closely approximate the uniform distribution. This property is useful for arguing that the output is indistinguishable from random sequences of bits. Joint work with Denis Charles and Eyal Goren (Received September 20, 2007)