1024-68-146 **Denis Charles*** (cdx@microsoft.com), One Microsoft Way, Redmond, WA 98052, and **Eyal Goren** and **Kristin Lauter**. *Cryptographic hash functions from families of Ramanujan graphs.*

Collision resistant hash functions have many applications in cryptography. We show that one can construct provably collision resitant hash functions from certain families of Ramanujan graphs. Two such families are the Pizer graphs of supersingular j-invariants over finite fields and the Lubotzky-Phillips-Sarnak graphs. In both cases we show that finding a collision in the hash function reduces to solving a hard number theoretic or group theoretic problem. (Received January 06, 2007)