1026-68-195 **Ramarathnam Venkatesan*** (venkie@microsoft.com), One Microsoft Way, Redmond, WA 98052. *Cryptographic applications involving Spectral Analysis of Rapid mixing.*

In this talk we survey three results that involve spectral analysis to prove rapid mixing some random walks on some expander graphs that naturally occur in some applciations. One relates to the expected convergence time of classic Pollard Rho for solving discrete log on abelian groups. Another one seeks a formalization of the question if the standard practice of picking elliptic curves based essentially on the number of points on it (over a finite field) is the right one?. The final one is related to the analysis and design of stream cipher. We shall survey the proofs and briefly look at other applications.

Based on papers co-written with Steve Miller (Rutgers), David Jao (Waterloo) Ilya Miranov (Microsoft Research) and Nathan Keller (Hebrew) (Received February 26, 2007)