Probability on graphs and groups with applications to group-based cryptanalysis

Date Tuesday, February 2

Time 3 pm

Location 303 Mudd

Abstract: We introduce the notion of the mean-set (expectation) of a graph-(group-) valued random element ξ, generalize the strong law of large numbers to graphs and groups, and consider Chebyshev and Chernoff type bounds. In addition, we discuss several results about configurations of mean-sets in graphs and reflect on an algorithm for computing sample mean-sets. Finally, we show that our new theoretical tools provide a framework for practical applications; in particular, they have implications for cryptanalysis of group-based authentication protocols. In this talk, we will, among other things, look at the idea of such analysis for a certain existing identification protocol, using our results, and conclude that this protocol is not, in fact, secure. Results of actual experiments supporting our conclusions will be provided. (joint work with A. Ushakov)