Title: Counting Number of Solutions to a Bi-Variate System of Equations

Abstract

In this talk, I will present a lower bound on the number of solutions (P1, P2, ..., P_2q) to a given a system of q bi-variate equations over a finite abelian group G=({0,1}^n, \oplus) of the form P_{2i-1} \oplus P_{2i} = \lambda_i, where \lambda_i \in {0,1}^n \ {0^n}. This result is popularly known as Mirror Theory, which has been proven to be a powerful tool to provide a high security guarantee of many cryptographic constructions.

By : Avijit Dutta