Are There Efficient Secret Sharing Schemes?

Amos Beimel

Abstract

Secret-sharing schemes are an important tool used in many cryptographic protocols. In these schemes, a dealer holding a secret string distributes shares to the parties such that only pre-defined authorized subsets of participants can reconstruct the secret from their shares. For example, if the authorized sets are all the sets whose size is greater than some threshold, then there is an efficient secret-sharing scheme. However, for many other collections of authorized sets no efficient schemes are known and it is conjectured that no such efficient schemes exist.

In this talk I will survey the known results on secret sharing and discuss a few approaches for proving lower bounds for them. I will then show limitations of a promising approach of using non-Shannon information inequalities: All information inequalities in 4 and 5 variables and all known information inequalities in more than 5 variables cannot prove super-linear lower bounds.