World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:8, No:07, 2014

A New Bound on the Average Information Ratio of Perfect Secret-Sharing Schemes for Access Structures Based on Bipartite Graphs of Larger Girth

Authors : Hui-Chuan Lu

Abstract : In a perfect secret-sharing scheme, a dealer distributes a secret among a set of participants in such a way that only qualified subsets of participants can recover the secret and the joint share of the participants in any unqualified subset is statistically independent of the secret. The access structure of the scheme refers to the collection of all qualified subsets. In a graph-based access structures, each vertex of a graph G represents a participant and each edge of G represents a minimal qualified subset. The average information ratio of a perfect secret-sharing scheme realizing a given access structure is the ratio of the average length of the shares given to the participants to the length of the secret. The infimum of the average information ratio of all possible perfect secret-sharing schemes realizing an access structure is called the optimal average information ratio of that access structure. We study the optimal average information ratio of the access structures based on bipartite graphs. Based on some previous results, we give a bound on the optimal average information ratio for all bipartite graphs of girth at least six. This bound is the best possible for some classes of bipartite graphs using our approach.

Keywords : secret-sharing scheme, average information ratio, star covering, deduction, core cluster
Conference Title : ICIT 2014 : International Conference on Information Theory
Conference Location : Singapore, Singapore
Conference Dates : July 05-06, 2014