Informatics Research Institute of Toulouse

Within the framework of
IRIT@UT1

Thursday 6 October 2016
12h30 – 14h00
Manufacture des Tabacs, Salle ME302

Arkadii SLINKO
University of Auckland (Nouvelle-Zélande)

Access Structures of Weighted Threshold Ideal Secret Sharing Schemes

Seminar

Abstract: One of the most important challenges of the theory of secret sharing is to characterize access structures that can carry an ideal secret sharing scheme. Finding such a description appeared to be quite difficult. A result that generated much hope in this direction was the paper by Brickell and Davenport (1991) who showed that all ideal secret sharing schemes can be obtained from matroids. Not all matroids, however, define ideal schemes so the problem was reduced to classifying those matroids that do. There was little further progress, if any, in this direction.

In his pioneering paper Shamir (1979) introduced the notion of weighted threshold access structure. In such a structure every agent is given a weight and a coalition is authorised if their combined weight is at least a certain predefined threshold.

Beimel, Tassa and Weinreb (2008) and Farras and Padro (2010) partially characterized access structures of ideal weighted threshold secret sharing schemes in terms of the operation of composition introduced by Shapley (1962). They proved that any weighted threshold ideal access structure is a composition of indecomposable ones. Farras and Padro gave a list of seven classes of access structures---one unipartite, three bipartite and three tripartite---to which all weighted threshold ideal indecomposable access structures may belong. Hameed and Slinko determine exactly which access structures from those classes are indecomposable. They also determined which compositions of indecomposable weighted threshold access structures are again weighted threshold and obtained an if and only if characterization of ideal weighted threshold secret sharing schemes. They used game-theoretic techniques to achieve this. In my talk I will summarize the aforementioned developments and give a complete characterization of weighted threshold access structures.

05 61 55 65 10
info@irit.fr
www.irit.fr