Mutual information and secret key agreement

Andrei Romashchenko*[1]

[1]Laboratoire d'Informatique de Robotique et de Microélectronique de Montpellier (LIRMM) – Université Montpellier II - Sciences et techniques, CNRS : UMR5506 – CC 477, 161 rue Ada, 34095 Montpellier Cedex 5, France

Résumé

The description complexity (a.k.a. Kolmogorov complexity) of a string, C(x), is defined as the length of the shortest program that prints this string x. Given a pair of strings x and y, we define the mutual information between them as the difference between C(x)+C(y) and C(x,y). Intuitively, the mutual information is a measure of correlation between two strings: the closer the correlation is, the bigger the mutual information.
We discuss an operational interpretation of the mutual information that can be explained in terms of a communication protocol. It is a protocol with two parties, one having x and the other one having y, with interaction on a public channel. The aim is to establish the longest shared secret key without revealing any information on this key to the eavesdropper. It turns out that for every pair of inputs the optimal size of the key is equal to the mutual information between x and y. This statement can be extended to the settings with more than two parties.
The talk is based on joint works with Marius Zimand and Emirhan Gürpinar.

*Intervenant