Le problème d'agrément de clé secrète et une caractérisation de l'information mutuelle. // The problem of secret key agreement and a characterization of the mutual information.

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

We show that the mutual information, in the sense of Kolmogorov complexity, of any pair of strings X and Y is equal to the length of the longest shared secret key that two parties, one having X and the other one having Y, can establish via a probabilistic protocol with interaction on a public channel. This result is also extended to the protocols with more than two parties. (A joint work with Marius Zimand.)

*Intervenant