Title : The optimal secret key agreement and information inequalities.

Encadrant : Andrei ROMASHCHENKO (LIRMM)
email : andrei.romashchenko@lirmm.fr

Keywords : common secret key agreement, Kolmogorov complexity, information inequalities, communication complexity

Prerequisites : The candidate should have some basic knowledge of classical information theory. The knowledge of Kolmogorov complexity and communication complexity is a big plus.

Abstract : Suppose that each of two parties (two persons, two computers, any two electronic devices) called Alice and Bob holds some piece of information A and B respectively, and these pieces of information are correlated with each other. Alice and Bob can interact with each other via a public communication channel. The aim of Alice and Bob is to agree on a common secret key Z so that the eavesdropper (who does not know A and B but who can intercept the communication between Alice and Bob) gets no information on this key. The question is how large this common secret key can be made (how much information it can contain). This problem has an elegant solution : it can be shown that in some natural setting the maximal size of the common secret key Z is equal to the value of the mutual information between A and B (defined in terms of Kolmogorov complexity.)

We propose to generalize this problem to the case of $k > 2$ interacting parties. Though several partial results on this generalization are known, many natural questions remain open. We suggest to focus on two types of questions :

1. *Quantitative questions :* compute the size of the maximal value of the common secret key given all mutual information quantities for the input data.

2. *Algorithmic questions :* construct efficient (poly-time computable) communication protocols of the secret key agreement for some natural types of correlation between the initial pieces of information given to the parties involved in the protocol.

To attack the first type of questions we propose to employ the bounds based on information inequalities. In the questions of the second type we suppose to use the technique of coding theory and different methods of hashing.

Bibliography :

[1] Alexander Shen et al., Kolmogorov Complexity and Algorithmic Randomness. AMS 2017. The draft : `http://www.lirmm.fr/~ashen/kolmbook-eng.pdf`

[2] Andrei Romashchenko and Marius Zimand, An operational characterization of mutual information in algorithmic information theory. (2017) arXiv : 1710.05984
`https://arxiv.org/abs/1710.05984`

[3] Daniyar Chumbalov and Andrei Romashchenko, On the Combinatorial Version of the Slepian-Wolf Problem. (2015) arXiv : 1511.02899
`https://arxiv.org/abs/1511.02899`

[4] Imre Csiszar and Prakash Narayan, Secrecy capacities for multiple terminals. IEEE Trans. Information Theory, 50(12) : 3047–3061, 2004.