Universal codes achieving the capacity of fading and MIMO channels

In the last decade, algebraic tools have proven to be very useful to design high-performance codes exploiting the spatial and temporal diversity of MIMO channels, some of which have been adopted in 3G and 4G communication standards, including WiMAX and terrestrial Digital Video Broadcasting. The activity in this area focused at first on the characterization of the diversity-multiplexing gain trade-off (DMT) of space-time codes. Our approach is based on the relation between the DMT and the growth of elements of a bounded norm in discrete subgroups of Lie groups [hal-00822339] and led to a complete classification of the DMT of space-time block codes [hal-01740506]. Surprisingly, little attention has been given so far to the question of whether algebraic space-time codes can also approach ergodic capacity when encoding and decoding over a growing number of fading blocks. In our recent work [hal-01586936], we give a partial answer by showing that the normalized minimum determinant can be used to measure the gap to the capacity of a given family of multi-block lattice codes. Moreover, we propose a new construction of codes based on number field towers, which achieve capacity up to a constant gap universally over a wide class of fading models. The universality property guarantees robustness with respect to imperfect channel estimation at the transmitter

Lattice codes achieve semantic security

Physical layer security is a new paradigm which exploits the randomness inherent in wireless propagation to provide an additional level of protection. The notion of semantic security allows combining the requirements of cryptography and information theory. In [hal-0784077], we showed that lattice codes achieve semantic security over the Gaussian wiretap channel, and we proposed a fundamental design criterion for secrecy, the flatness factor. This work has been highly cited within the physical layer security community. More recently, we generalized this approach to wireless and MIMO channels, leading to a simple code design criterion: the product of the minimum determinant of the code and of its dual should be minimized [hal-01420943]. Moreover, it turns out that universal codes from number field towers also achieve semantic security. We also considered the problem of generating secret keys from correlated Gaussian sources in the presence of an

eavesdropper, and proposed a new hash function based on lattices [hal-00861654].

Covert Communication

While the goal of the wiretap channel coding is to hide the transmitted message, covert communication refers to scenarios where the communicating parties try to hide their activity of communication from a potential eavesdropper or "warden". This approach is based on physical layer security and offers quantum resistance (information theoretic security). This setting also called communication with a low probability of detection, the eavesdropper's goal is to "detect" communication, not to learn the message. The first information-theoretic characterization of the performance limit for covert communication was provided in [hal-01345907]. This paper has stimulated much interest in the Information Theory community and is already highly cited. This characterization was subsequently extended in various directions such as classical-quantum channels in [hal-01390568] and channel-state information in [hal-01556729].

Coordination of autonomous devices in decentralized networks

Future 5G networks will be characterized by the rise of direct device-to-device communication. Among the many challenges that must be addressed to develop distributed systems, a key aspect is to understand the interplay between coordination and communication. A novel approach in Information Theory consists in modeling the actions performed by the devices as random variables, and in measuring the level of coordination by the distance between their joint distribution and a target behavior

- It is then possible to characterize the minimum rates of communication that are required for coordination according to different metrics (empirical or strong coordination). This topic is developed in the PhD thesis of Giulia Cervia, co-supervised by Laura Luzzi and M. Le Treust. We propose an application of polar codes for coordination over a noisy channel, where the input and output signals have to be coordinated with the source and the reconstruction [hal-01368551], [hal-01718146]
- We provide the first inner and outer bounds for strong coordination in this scenario [hal-01522450]
- The limit performances of empirical coordination were characterized in [LeTreustITW2014], [LeTreustISIT2015a], [LeTreustISIT2015b], [hal-01531949], and extended to the case of secure coordination in [hal-01361207]. When the network is decentralized, the autonomous devices are considered as players that maximize their own utility functions. By using tools from Game Theory, we investigate the problem of strategic coordination and establish a connection with the economics literature on "Bayesian Persuasion" [hal-01383923], [LeTreustTomalaECMA2017], [hal-01633603], [hal-01724109].