Abstract

A new coding scheme is proposed to establish a lower bound on the strong secrecy capacity of stochastic code over the general arbitrarily varying wiretap channel. Moreover, the lower bound is the secrecy capacity when the main channel is less noisy than the wiretap channel. The main idea is to construct secure partitions over the “good” codebook by extending Csiszár’s almost independent coloring scheme. This new scheme provides a fundamental tool to deal with the strong secrecy problems of wiretap channels.