CCIT Report #854 March 2014

Exact Correct–Decoding Exponent of the Wiretap Channel Decoder [*]

Neri Merhav

Department of Electrical Engineering
Technion - Israel Institute of Technology
Technion City, Haifa 32000, ISRAEL
E–mail: merhav@ee.technion.ac.il

Abstract

The security level of the achievability scheme for Wyner's wiretap channel model is examined from the perspective of the probability of correct decoding, P_c, at the wiretap channel decoder. In particular, for finite–alphabet memoryless channels, the exact random coding exponent of P_c is derived as a function of the total coding rate R_1 and the rate of each sub–code R_2. Two different representations are given for this function and its basic properties are provided. We also characterize the region of pairs of rates (R_1, R_2) of full security in the sense of the random coding exponent of P_c, in other words, the region where the exponent of this achievability scheme is the same as that of blind guessing at the eavesdropper side. Finally, an analogous derivation of the correct–decoding exponent is outlined for the case of the Gaussian channel.

Index Terms: Wiretap channel, random coding exponent, information–theoretic security, secrecy.

[*] This research was supported by the Israel Science Foundation (ISF), grant no. 412/12.