CCIT Report #892 January 2016

Exact Random Coding Secrecy Exponents for the Wiretap Channel

Mani Bastani Parizi, *Student Member, IEEE,* Emre Telatar, *Fellow, IEEE,* and Neri Merhav, *Fellow, IEEE*

Abstract

We analyze the exact exponential decay rate of the expected amount of information leaked to the wiretapper in Wyner's wiretap channel setting using wiretap channel codes constructed from both i.i.d. and constant-composition random codes. Our analysis for those sampled from i.i.d. random coding ensemble shows that the previously-known achievable secrecy exponent using this ensemble is indeed the exact exponent for an average code in the ensemble. Furthermore, our analysis on wiretap channel codes constructed from the ensemble of constant-composition random codes, leads to an exponent which, in addition to being the exact exponent for an average code, is larger than the achievable secrecy exponent that has been established so far in the literature for this ensemble (which in turn was known to be smaller than that achievable by wiretap channel codes sampled from i.i.d. random coding ensemble). We also show examples where the exact secrecy exponent for the wiretap channel codes constructed from random constant-composition codes is larger than that of those constructed from i.i.d. random codes.

Index Terms

Wiretap channel, Channel resolvability, Secrecy exponent, Resolvability exponent

I. Introduction

The problem of communication in presence of an eavesdropper wiretapping the signals sent to the legitimate receiver (see Figure 1) was first studied by Wyner [1] and later, in a broader context, by Csiszár and Körner [2], where it was shown (among others) that as long as the eavesdropper's channel is weaker than that of the legitimate receiver, reliable and *secure* communication at positive rates is feasible. More precisely, it was shown that, given any distribution on the common input alphabet of the channels, P_X, for which the mutual information developed across the legitimate receiver's channel is higher than that developed across the wiretapper's channel, that is, $I(X;Y) > I(X;Z)$, with $(X,Y,Z) \sim P_X(x)W_{\mathrm{M}}(y|x)W_{\mathrm{E}}(z|x)$ (where X, Y, and Z represent the common

The work of M. Bastani Parizi and E. Telatar was supported by the Swiss National Science Foundation (SNSF) grant no. 200020_146832. The work of N. Merhav was supported by the Israel Science Foundation (ISF), grant no. 412/12.

The material in this paper will be submitted in part to 2016 IEEE International Symposium on Information Theory (ISIT 2016).

M. Bastani Parizi and E. Telatar are with the Information Theory Laboratory (LTHI), Swiss Federal Institute of Technology (EPFL), Lausanne 1015, Switzerland (email: mani.bastaniparizi@epfl.ch, emre.telatar@epfl.ch)

N. Merhav is with the Department of Electrical Engineering, Technion - Israel Institute of Technology, Haifa 32000, Israel (email: merhav@ee.technion.ac.il)