Information Theoretic Security

Fall semester, 2013

Assignment 3

Assigned: Thursday, October 3, 2013

Due: Wednesday, October 16, 2013 Somayeh Salimi

Problems

Problem 1.1:

Show that the secrecy capacity equals $\max_{P_X}[I(X;Y) - I(X;Z)]$ in the case where the main channel is more capable than the eavesdropper's channel.

Problem 1.2:

Prove Csiszar sum identity $H(Y^n) - H(Z^n) = \sum_{i=1}^{n}[H(Y_i|Y^{i-1}, Z_{i+1}^n) - H(Z_i|Y^{i-1}, Z_{i+1}^n)]$ and consequently show that

$$I(M;Y^n) - I(M;Z^n) = \sum_{i=1}^{n}[I(M;Y_i|Y^{i-1}, Z_{i+1}^n) - I(M;Z_i|Y^{i-1}, Z_{i+1}^n)].$$

Problem 1.3:

Find the secrecy capacity in the cases where the eavesdropper's channel is either more capable or less noisy than the main channel as well as the case where the main channel is physically degraded compared to the eavesdropper's channel (reversely degraded wiretap channel).

Problem 1.4:

Assume that the main channel and the eavesdropper's channel are binary-erasure and binary-symmetric as in Fig.1. Prove that for $0 < \epsilon \leq 2p$, Z is a stochastically degraded version of Y but not physically degraded (Hint: take a look at Fig. 22.6 of Network Information Theory book).

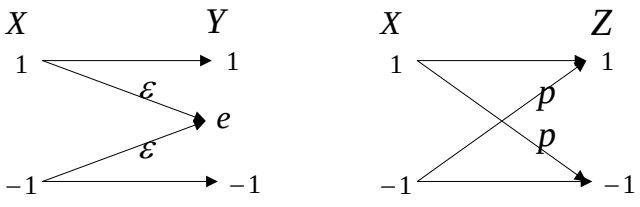

Fig. 1: BEC and BSC

Problem 1.5:

Prove the converse part of Theorem 3 of Lecture#3.

Problem 1.6:

Problem 22.7 of Network Information Theory book.

Problem 1.7 (extra problem)[1]:

Consider the physically degraded discrete memoryless wiretap channel $p(yz|x) = p(y|x)p(z|y)$. Assume that there is noiseless causal secure feedback from the receiver to the sender. Show that the secrecy capacity is

$$C_s = \max_{p(x)} \min\{I(X;Y|Z) + H(Y|X,Z), I(X;Y)\}.$$

Does the same result hold for the reversely degraded channel, i.e., $p(yz|x) = p(z|x)p(y|z)$?

(Hint: Give the achievability scheme assuming that the receiver is not allowed to make randomization, i.e., sending an independent key and he is only allowed to use the channel output. Due to the secure noiseless feedback, the sender and the receiver can agree on a secret key of rate $H(Y|X,Z)$ independent of the message and the transmitted random codeword. Using block Markov coding, this key can be used to increase the secrecy capacity for the next transmission block as in Theorem 3 of Lecture#3.

Remark: This result is due to Theorem 1 of Ahlswede and Cai's paper "Transmission, Identification and Common Randomness Capacities for Wire-Tape Channels with Secure Feedback from the Decoder", 2007.)

[1]Doing an extra problem is not mandatory but it has extra point