Information Theoretic Security

Fall semester, 2013

Assignment 4

Assigned: Friday, October 11, 2013

Due: Thursday, October 31, 2013 Somayeh Salimi

Problems

Problem 1.1:

Show that in Maurer's example (in lecture#4), by computing $Z \oplus W$, Eve does not lose any information about V, i.e., with access to Z and W, $Z \oplus W$ is the sufficient statistic of V.

Problem 1.2:

Show that in the basic channel model of key agreement with the channel distribution $P_{YZ|X}$ (in the general q-round public channel communication case), the upper bound $I(X;Y|Z)$ is tight and the secret key capacity equals $C_K = \max_{P_X} I(X;Y) - I(Y;Z)$ if Markov chain $Y - X - Z$ holds between the channel input and outputs.

Problem 1.3:

Find the forward and the backward secret key capacity ($q = 1$) of the source model when the joint conditional pmf $P_{X_1X_2Z}$ is defined in Fig.1.

Problem 1.4:

Change the proof of the outer bound on p. 567 of Network Information Theory book to the case where the secret keys generated at the users are stochastic functions of the available information, i.e., $H(K_1|X_1^n, M_q) \neq 0, H(K_2|X_2^n, M_q) \neq 0$ but instead we have $K_1 - (X_1^n, M_q) - (X_2^n, Z^n, K_2)$ and $K_2 - (X_2^n, M_q) - (X_1^n, Z^n, K_1)$.

Problem 1.5: Problem 22.6 of Network Information Theory book.

Problem 1.6: Problem 22.8 of Network Information Theory book.

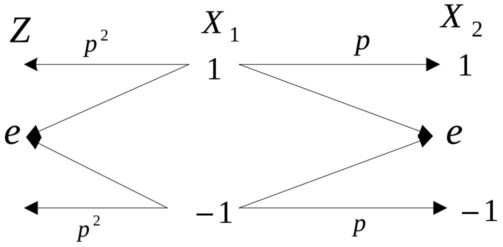

Fig. 1: joint pmf of problem 1.3

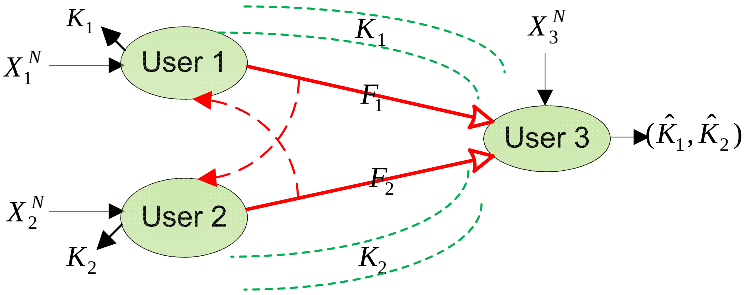

Fig. 2: Source model key agreement with forward public channel

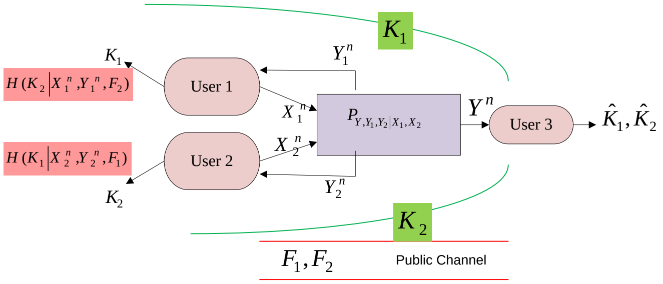

Fig. 3: Source model key agreement with forward public channel

Problem 1.7: Problem 22.9 of Network Information Theory book.

Problem 1.8:

Show that in the source model of secret key agreement scheme with two secret keys (Fig.2), if the sources X_1, X_2 and X_3 (with distribution $P_{X_1X_2X_3}$) form Markov chain in any order, then the secret key capacity region is deduced.

Problem 1.9:

Prove the following explicit outer bound of the secret key capacity region in the channel model of Fig.3:

$$0 \leq R_1 \leq I(X_1, Y_1; Y|X_2, Y_2), \qquad 0 \leq R_2 \leq I(X_2, Y_2; Y|X_1, Y_1)$$

over all distribution of the form $p(x_1, x_2, y, y_1, y_2) = p(x_1)p(x_2)p(y, y_1, y_2|x_1, x_2)$.

Problem 1.10:

Prove that when the inputs and outputs of the generalized multiple access channel in Fig.3 form a Markov chain as $(X_1, X_2) - Y_2 - Y - Y_1$, the secret key capacity region is as follows:

$$0 \leq R_1 \leq I(Y_1; Y|Y_2), \qquad 0 \leq R_2 \leq I(X_2, Y_2; Y|X_1, Y_1)$$

over all distribution of the form $p(x_1, x_2, y, y_1, y_2) = p(x_1)p(x_2)p(y, y_1, y_2|x_1, x_2)$. Describe intuitively how the secret key sharing is performed in this case.