Mathematical Problems of Computer Science 36, 79–90, 2012.

Random Coding Bound for Secrecy E-capacity Region of the Broadcast Channel With Two Confidential Messages

Nasrin Afshar, Evgueni Haroutunian and Mariam Haroutunian

Institute for Informatics and Automation Problems of NAS of RA
e-mail: evhar@ipia.sci.am

Abstract

We study secrecy E-capacity region of the discrete memoryless broadcast channel with two independent confidential messages sent to two receivers (BC-2CM). The system involves two sources, one encoder, two discrete memoryless channels and two receivers. Each private message is sent to the corresponding receiver while keeping the other receiver in total ignorance of it. The level of ignorance is measured by the equivocation rate. E-capacity region is the set of rate pairs R_1, R_2 of codes with given error probability exponents (reliabilities) E_1, E_2 at respective receivers. We derived a random coding bound for secrecy E-capacity region of the BC-2CM. When error probability exponents are going to zero, this bound coincides with the inner bound of secrecy capacity region of the BC-2CM obtained by R. Liu, I. Maric, P. Spasojevic and R. Yates.

Key words: Broadcast channel with confidential messages, secrecy E-capacity, equivocation rate, error probability exponent, method of types, random coding bound.

1. Introduction

The broadcast channel with confidential messages (BCC) which is a generalization of the Wyner's wiretap channel [17] was first investigated by Csiszár and Körner [3]. M. Hayashi and R. Matsumoto obtained universally attainable error exponents for the BCC [12]. Random coding bound for the E- capacity region of the wiretap channel was found in [10].

In this paper, we study discrete memoryless broadcast channel with two independent confidential messages (BC-2CM). Each private message is transmitted to the respective receiver while ensuring the eavesdropping receiver to be kept in total ignorance of it. The model of BC-2CM is depicted in Fig.1. Bounds for the secrecy capacity region of the BC-2CM were found in [14]. Y. Cao and B. Chen proposed an inner bound on the capacity region of the broadcast channel with one common message and two confidential messages [18]. We construct a single-letter characterization of random coding bound for secrecy E-capacity region of the BC-2CM.

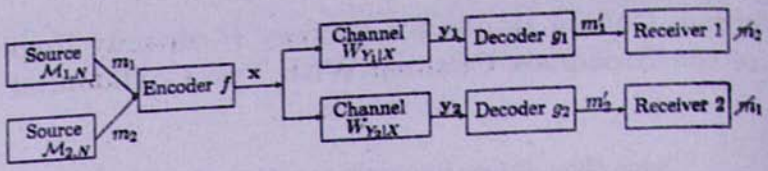

Figure 1. The BC-2CM.

The reminder of the paper is organized as follows. In Section II, the problem and result are formulated. Section III and Appendix are dedicated to proofs.

2. Preliminaries, Problem and Result Formulation

We denote finite sets by script capitals. For finite set $\mathcal{X}$ the cardinality is denoted by $|\mathcal{X}|$. Capital letters $X, \dots$, represent random variables (RVs) with values in $\mathcal{X}, \dots$, and specific realizations of them are denoted by the corresponding lower case letters $x, \dots$. Respective vectors of length N are denoted by bold-face letters $\mathbf{X}, \dots$, and $\mathbf{x}, \dots$.

The discrete memoryless BC-2CM is with an input alphabet $\mathcal{X}$, and output alphabets $\mathcal{Y}_1$ and $\mathcal{Y}_2$, correspondingly, on the first and second receivers. The vector $\mathbf{x} = (x_1, \dots, x_N) \in \mathcal{X}^N$ is the input, $\mathbf{y}_1 = (y_{1,1}, \dots, y_{1,N}) \in \mathcal{Y}_1^N$ and $\mathbf{y}_2 = (y_{2,1}, \dots, y_{2,N}) \in \mathcal{Y}_2^N$ are the output vectors after N uses of channels. $\mathcal{M}_{1,N}$ and $\mathcal{M}_{2,N}$ are message sets at the first and the second sources, respectively. We introduce some additional finite sets $\mathcal{U}_0$, $\mathcal{U}_1$, $\mathcal{U}_2$. RVs $M_{1,N}$, $M_{2,N}$, U_0, U_1, U_2, X, Y_1, Y_2 take values, correspondingly, in $\mathcal{M}_{1,N}$, $\mathcal{M}_{2,N}$, $\mathcal{U}_0$, $\mathcal{U}_1$, $\mathcal{U}_2$, $\mathcal{X}$, $\mathcal{Y}_1$, $\mathcal{Y}_2$.

Let $P_0 = \{P_0(u_0),\ u_0 \in \mathcal{U}_0\}$ be PD of RV U_0, $P_{i|0} = \{P_{i|0}(u_i|u_0),\ u_0 \in \mathcal{U}_0,\ u_i \in \mathcal{U}_i\}$ be conditional PD of RV U_i for given value u_0 of RV U_0 and $P_i = \{P_i(u_i) = \sum_{u_0} P_{i|0}(u_i|u_0)P_0(u_0),\ u_i \in \mathcal{U}_i\}$ be a marginal PD of RV U_i, $i = 1, 2$. We define conditional joint PD of pair of RVs U_1, U_2 for given value u_0 of RV U_0 by

$$P_{1,2|0} \triangleq P_{1|0} \circ P_{2|1,0} \triangleq \{P(u_1, u_2|u_0) = P_{1|0}(u_1|u_0)P_{2|1,0}(u_2|u_1, u_0),\ u_0 \in \mathcal{U}_0,\ u_i \in \mathcal{U}_i,\ i = 1, 2\}.$$

Let

$$P_{X|U_1,U_2} = \{P_{X|U_1,U_2}(x|u_1, u_2),\ x \in \mathcal{X},\ u_i \in \mathcal{U}_i, i = 1, 2\},$$

$$V_{Y_i|X} = \{V_{Y_i|X}(y_i|x),\ x \in \mathcal{X},\ y_i \in \mathcal{Y}_i\},\ i = 1, 2.$$

We use joint PDs of RVs U_0, U_1, U_2, X, Y_1, Y_2,

$$P_0 \circ P_{1,2|0} \circ P_{X|U_1,U_2} \circ V_{Y_i|X} =$$

$$\{P_0 \circ P_{1,2|0} \circ P_{X|U_1,U_2} \circ V_{Y_i|X}(u_0, u_1, u_2, x, y_i) = P_0(u_0)P_{1,2|0}(u_1, u_2|u_0)P(x|u_1, u_2)V_{Y_i|X}(y_i|x),$$

$$u_0 \in \mathcal{U}_0, u_1 \in \mathcal{U}_1, u_2 \in \mathcal{U}_2, x \in \mathcal{X}, y_i \in \mathcal{Y}_i\}, i = 1, 2. \quad (1)$$

So we have Markov chains $U_0 \to (U_1, U_2) \to X \to Y_1$ and $U_0 \to (U_1, U_2) \to X \to Y_2$. The memoryless broadcast channel is characterized by the conditional PDs.

$$W_{Y_i|X} = \{W_{Y_i|X}(y_i|x),\ x \in \mathcal{X},\ y_i \in \mathcal{Y}_i\},\ i = 1, 2.$$

and by products for N uses of the channel

$$W^N_{Y_i|X}(\mathbf{y}_i|\mathbf{x}) \triangleq \prod_{n=1}^{N} W_{Y_i|X}(y_{i_n}|x_n)),\ i = 1, 2.$$

Messages $m_1 \in \mathcal{M}_{1,N}$, $m_2 \in \mathcal{M}_{2,N}$ should be transmitted, correspondingly, to receivers 1 and 2 while ensuring to be kept secret from the unintended receiver. The level of secrecy is measured by the equivocation rate at the eavesdropping receiver.

To increase secrecy the stochastic encoding is applied [3]. A *stochastic encoder* f for the BC-2CM is specified by conditional probabilities $f(\mathbf{x}|m_1, m_2)$, where $\mathbf{x} \in \mathcal{X}^N$, $m_i \in \mathcal{M}_{i,N}$, $i = 1, 2$, and $\sum_{\mathbf{x}\in\mathcal{X}^N} f(\mathbf{x}|m_1, m_2) = 1$.

A *code* is a triple (f, g_1, g_2), where f is a stochastic encoder and $g_i : \mathcal{Y}_i^N \to \mathcal{M}_{i,N}$, $i = 1, 2$, are deterministic decoders.

The quality of transmission is estimated by the probabilities of erroneous receipt of messages $m_1 \in \mathcal{M}_{1,N}$ and $m_2 \in \mathcal{M}_{2,N}$ by channels $W_{Y_1|X}$ and $W_{Y_2|X}$ using a code (f, g_1, g_2)

$$e_i(f, g_i, W_{Y_i|X}, m_1, m_2) \triangleq \sum_{\mathbf{x}\in\mathcal{X}^N} f(\mathbf{x}|m_1, m_2) W^N_{Y_i|X}((g_i^{-1}(m_i))^c|\mathbf{x}),\ i = 1, 2,$$

where $g_i^{-1}(m_i)$ is the set of $\mathbf{y}_i \in \mathcal{Y}_i^N$, which are decoded to m_i.

The maximal probabilities of error of the code (f, g_1, g_2) are

$$e_i(f, g_i, W_{Y_i|X}) \triangleq \max_{m_1\in\mathcal{M}_{1,N}, m_2\in\mathcal{M}_{2,N}} e_i(f, g_i, W_{Y_i|X}, m_1, m_2),\ i = 1, 2, \tag{2}$$

and the average error probabilities, assuming that random messages $M_{1,N}$, $M_{2,N}$ are uniformly distributed over $\mathcal{M}_{1,N}$ and $\mathcal{M}_{2,N}$, are

$$\bar{e}_i(f, g_i, W_{Y_i|X}) \triangleq (|\mathcal{M}_{1,N}| \times |\mathcal{M}_{2,N}|)^{-1} \sum_{m_1\in\mathcal{M}_{1,N}, m_2\in\mathcal{M}_{2,N}} e_i(f, g_i, W_{Y_i|X}, m_1, m_2), i = 1, 2. \tag{3}$$

Evidently

$$\bar{e}_i(f, g_i, W_{Y_i|X}) \le e_i(f, g_i, W_{Y_i|X}),\ i = 1, 2.$$

A code (f, g_1, g_2) is characterized also by coding rates and equivocation rates (the functions log and exp are taken to the base 2)

$$R_i \triangleq \frac{1}{N} \log |\mathcal{M}_{i,N}|,$$

$$R_{i,e} \triangleq \frac{1}{N} H_{P_{0,1,2},W_{Y_{3-i}|X}}(M_{i,N}|Y_{3-i}),\ i = 1, 2, \tag{4}$$

where conditional entropy $H_{P_{0,1,2},W_{Y_{3-i}|X}}(M_{i,N}|Y_{3-i})$ is the uncertainty at receiver i with respect to private messages m_{3-i}, $i = 1, 2$.

The E-capacity [9] presents dependence between rate R and reliability E (error probability exponent) of optimal codes. The function denoted by $R(E)$ (and also $C(E)$) [6] [9] is inverse to the Shannon's reliability function $E(R)$.

Let $E = (E_1, E_2)$. A rates pair (R_1, R_2) is called *E-achievable* for the BC-2CM iff there exists a codes sequence such that

$$\lim_{N\to\infty} \frac{1}{N} \log |\mathcal{M}_{i,N}| \ge R_i,\ i = 1, 2. \tag{5}$$

the reliability requirements

$$e_i(f, g_i, W_{Y_i|X}) \le \exp\{-NE_i\}, \ i = 1, 2. \tag{6}$$

and the secrecy constraints

$$\lim_{N\to\infty} \frac{1}{N} H_{P_{0,1,2},W_{Y_{3-i}|X}}(M_{i,N}|\mathbf{Y}_{3-i}) \ge R_i, \ i = 1, 2, \tag{7}$$

are valid.

Secrecy E-capacity region $C(E)$ for maximal error probabilities is defined as the set of all E-achievable rates (R_1, R_2). We denote $\overline{C}(E)$ for secrecy E-capacity region when average error probabilities are applied. Evidently

$$C(E) \subseteq \overline{C}(E).$$

In this paper, we construct an inner bound for $C(E)$. To this end, we apply the method of types [4]. For the definitions and properties of type and conditional type we refer to [4], [9].

Let P_0 be a type of a vector $\mathbf{u}_0 \in \mathcal{U}_0^N$ and $P_{i|0}$, $i = 1, 2$, $P_{1,2|0}$, $P_{X|U_1,U_2}$ and $V_{Y_i|X}$, $i = 1, 2$, be conditional types.

For $i = 1, 2$, we define conditional PDs $P^1_{Y_i|U_i,U_0}$ and $P_{Y_i|U_i,U_0}$ as follows,

$$P_{Y_i|U_i,U_0}(y_i|u_i, u_0) \triangleq \sum_{u_{3-i},x} P_{U_{3-i}|U_i,U_0}(u_{3-i}|u_i, u_0) P_{X|U_1,U_2}(x|u_1, u_2) W_{Y_i|X}(y_i|x), \tag{8}$$

$$P^1_{Y_i|U_i,U_0}(y_i|u_i, u_0) \triangleq \sum_{u_{3-i},x} P_{U_{3-i}|U_i,U_0}(u_{3-i}|u_i, u_0) P_{X|U_1,U_2}(x|u_1, u_2) V_{Y_i|X}(y_i|x), \tag{9}$$

Let $\mathcal{V}_N(P_{0,i}, \mathcal{Y}_i)$ be the set of all conditional types $P^1_{Y_i|U_i,U_0}$ of $\mathbf{y}_i \in \mathcal{Y}_i^N$, $i = 1, 2$. The notations $I_{P_{0,i},P^1_{Y_i|U_i,U_0}}(U_1 \wedge Y_1|U_0)$ and $I_{P_{0,i},P_{Y_i|U_i,U_0}}(U_1 \wedge Y_2, U_2|U_0)$ are used for the conditional mutual information of RVs U_1, Y_1 and U_1, Y_2, U_2, respectively, relative to RV U_0. $H_{P_{0,1,2},W_{Y_2|X}}(M_{1,N}|Y_2)$ is conditional entropy of RV $M_{1,N}$ relative to RV Y_2. The notations $I_{P_{0,1},P^1_{Y_1|U_1,U_0}}(U_1 \wedge Y_1|U_0)$ and $I_{P_{0,1},P_{Y_1|U_1,U_0}}(U_1 \wedge Y_2, U_2|U_0)$ are used for the conditional mutual information of RVs U_1, Y_1 and U_1, Y_2, U_2, respectively, relative to RV U_0. $H_{P_{0,1,2},W_{Y_2|X}}(M_{1,N}|Y_2)$ is conditional entropy of RV $M_{1,N}$ relative to RV Y_2.

The divergence $\mathrm{D}(P^1_{Y_i|U_i,U_0}\|P_{Y_i|U_i,U_0}|P_{0,i})$, $i = 1, 2$, is defined as

$$\mathrm{D}(P^1_{Y_i|U_i,U_0}\|P_{Y_i|U_i,U_0}|P_{0,i}) \triangleq \sum_{u_0,u_i,y_i} P_{0,i}(u_0, u_i) P^1_{Y_i|U_i,U_0}(y_i|u_i, u_0) \log \frac{P^1_{Y_i|U_i,U_0}(y_i|u_i, u_0)}{P_{Y_i|U_i,U_0}(y_i|u_i, u_0)}.$$

If $P^1_{Y_i|U_i,U_0}$, $i = 1, 2$, are the conditional types of $\mathbf{y}_i$ for given $(\mathbf{u}_0, \mathbf{u}_i) \in \mathcal{T}^N_{P_{0,i}}(U_0U_i)$, then according to Lemma 1.2.6 in [4] for $\mathbf{y}_i \in \mathcal{T}^N_{P_{0,i},P^1_{Y_i|U_i,U_0}}(Y_i|\mathbf{u}_i, \mathbf{u}_0)$ we have

$$P^N_{Y_i|U_i,U_0}(\mathbf{y}_i|\mathbf{u}_i, \mathbf{u}_0) =$$

$$\exp\{-N[\mathrm{D}(P^1_{Y_i|U_i,U_0}\|P_{Y_i|U_i,U_0}|P_{0,i}) + H_{P_{0,i},P^1_{Y_i|U_i,U_0}}(Y_i|U_i, U_0)]\}, \ i = 1, 2. \tag{10}$$

We consider RVs X, Y_1, Y_2 and auxiliary RVs U_0, U_1, U_2 with joint PDs

$$P_0 \circ P_{1,2|0} \circ P_{X|U_1,U_2} \circ V_{Y_i|X} = \{P_0 \circ P_{1,2|0} \circ P_{X|U_1,U_2} \circ V_{Y_i|X}(u_0, u_1, u_2, x, y_i) =$$

$P_0(u_0)P_{1,2|0}(u_1,u_2|u_0)P(x|u_1,u_2)V_{Y_i|X}(y_i|x), u_0 \in \mathcal{U}_0, u_1 \in \mathcal{U}_1, u_2 \in \mathcal{U}_2, x \in \mathcal{X}, y_i \in \mathcal{Y}_i\},$

$$i = 1, 2. \quad (11)$$

Let us define the following set of distributions

$$\mathcal{D}_i(E_i) = \{P^1_{Y_i|U_i,U_0} \in \mathcal{V}_N(P_{0,i}, \mathcal{Y}_i) : \mathrm{D}(P^1_{Y_i|U_i,U_0}\|P_{Y_i|U_i,U_0}|P_{0,i}) \le E_i\}.$$

To formulate the inner bound of secrecy E-capacity region of the BC-2CM, we define the following region of rates R_1, R_2:

$0 \le R_1 \le$

$$\min_{P^1_{Y_1|U_1,U_0}: \mathrm{D}(P^1_{Y_1|U_1,U_0}\|P_{Y_1|U_1,U_0}|P_{0,1}) \le E_1} \left| I_{P_{0,1},P^1_{Y_1|U_1,U_0}}(U_1 \wedge Y_1|U_0) + \mathrm{D}(P^1_{Y_1|U_1,U_0}\|P_{Y_1|U_1,U_0}|P_{0,1}) - E_1 \right|^+$$

$$- I_{P_{0,1},P_{Y_2|U_2,U_0}}(U_1 \wedge Y_2|U_2, U_0) - I_{P_{0,1,2}}(U_1 \wedge U_2|U_0), \quad (12)$$

$0 \le R_2 \le$

$$\min_{P^1_{Y_2|U_2,U_0}: \mathrm{D}(P^1_{Y_2|U_2,U_0}\|P_{Y_2|U_2,U_0}|P_{0,2}) \le E_2} \left| I_{P_{0,2},P^1_{Y_2|U_2,U_0}}(U_2 \wedge Y_2|U_0) + \mathrm{D}(P^1_{Y_2|U_2,U_0}\|P_{Y_2|U_2,U_0}|P_{0,2}) - E_2 \right|^+$$

$$- I_{P_{0,2},P_{Y_1|U_1,U_0}}(U_2 \wedge Y_1|U_1, U_0) - I_{P_{0,1,2}}(U_1 \wedge U_2|U_0). \quad (13)$$

We define the inner bound $\mathcal{R}^*(E)$ of secrecy E-capacity region $C(E)$ as follows

$$\mathcal{R}^*(P_{0,1,2}, E) \triangleq \{(R_1, R_2) : (12), (13) \text{ take place for some}$$

$$\text{Markov chains } U_0 \to (U_1, U_2) \to X \to Y_i,\ i = 1, 2\},$$

$$\mathcal{R}^*(E) \triangleq \bigcup_{P_{0,1,2}} R^*(P_{0,1,2}, E).$$

Let us define the following set of distributions

Theorem. For all $E_1 > 0, E_2 > 0$, the region $\mathcal{R}^*(E)$ is an inner bound for secrecy E-capacity region of the BC-2CM:

$$\mathcal{R}^*(E) \subseteq C(E).$$

Corollary. If $E = (E_1, E_2) \to 0$, the achievable region given in the Theorem coincides with the inner bound for the secrecy capacity region of the BC-2CM of [14].

3. Proof of the Theorem

We shall prove that there exists a code $\mathcal{C}$ such that for each $\delta > 0$, $\epsilon > 0$ and N large enough $M_i = |\mathcal{M}_{i,N}|$

$$= \exp\left\{N\left[\min_{P^1_{Y_i|U_i,U_0} \in \mathcal{D}_i(E_i)} \left| I_{P_{0,i},P_{Y_i|U_i,U_0}}(U_i \wedge Y_i|U_0) + \mathrm{D}(P^1_{Y_i|U_i,U_0}\|P_{Y_i|U_i,U_0}|P_{0,i}) - E_i \right|^+ \right.\right.$$

$$\left.\left. - I_{P_{0,i},P_{Y_{3-i}|U_{3-i},U_0}}(U_i \wedge Y_{3-i}|U_{3-i}, U_0) - I_{P_{0,1,2}}(U_1 \wedge U_2|U_0) - \delta\right]\right\},\ i = 1, 2, \quad (14)$$

(5) and (7) hold.

Let us introduce the following numbers

$$J_1 = \exp\{N(I_{P_{0,1},P_{Y_2|U_2,U_0}}(U_1 \wedge Y_2|U_2,U_0) - \delta)\}, \tag{15}$$

$$J_2 = \exp\{N(I_{P_{0,2},P_{Y_1|U_1,U_0}}(U_2 \wedge Y_1|U_1,U_0) - \delta)\}, \tag{16}$$

$$K = \exp\{N(I_{P_{0,1,2}}(U_1 \wedge U_2|U_0) + \delta)\}, \tag{17}$$

$$R_i' = \frac{1}{N}\log J_i,\ R^+ = \frac{1}{N}\log K,\ i = 1, 2. \tag{18}$$

Without loss of generality M_1, M_2, J_1, J_2 and K are considered to be integers. The following sets will be used

$$\mathcal{J}_i = \{1, 2, ..., J_i\},\ i = 1, 2, \text{ and } \mathcal{K} = \{1, 2, ..., K\}.$$

We randomly generate a vector $\mathbf{u}_0 \in \mathcal{T}^N_{P_0}(U_0)$, $M_i \times J_i \times K$ vectors $\mathbf{u}_i(m_i, j_i, k_i)$ from $\mathcal{T}^N_{P_{0,P_{i|0}}}(U_i|\mathbf{u}_0)$, $m_i \in \mathcal{M}_{i,N}$, $j_i \in \mathcal{J}_i$, $k_i \in \mathcal{K}$ $i = 1, 2$. It is assumed that both decoders are informed about $\mathbf{u}_0$. Let us denote

$$\mathcal{C}_i \triangleq \{\mathbf{u}_i(m_i, j_i, k_i),\ m_i \in \mathcal{M}_i,\ j_i \in \mathcal{J}_i,\ k_i \in \mathcal{K}\},\ \ i = 1, 2,$$

The set $\mathcal{C}_i$ is composed by M_i bins, and the m_ith bin is

$$\mathcal{C}_i(m_i) \triangleq \{\mathbf{u}_i(m_i, j_i, k_i),\ j_i \in \mathcal{J}_i,\ k_i \in \mathcal{K}\}.$$

Every bin $\mathcal{C}_i(m_i)$ is divided into J_i sub-bins, and the (m_i, j_i)th sub-bin is

$$\mathcal{C}_i(m_i, j_i) \triangleq \{\mathbf{u}_i(m_i, j_i, k_i),\ k_i = 1, 2, ..., K\},\ i = 1, 2.$$

We encode message pair (m_1, m_2) as follows. First, we take randomly sub-bins $\mathcal{C}_1(m_1, j_1)$ and $\mathcal{C}_2(m_2, j_2)$. Next, we choose such k_1, k_2 that $\mathbf{u}_1(m_1, j_1, k_1)$ and $\mathbf{u}_2(m_2, j_2, k_2)$ have joint type $P_{1,2|0}$, i.e.

$$(\mathbf{u}_1(m_1, j_1, k_1), \mathbf{u}_2(m_2, j_2, k_2)) \in \mathcal{T}^N_{P_{1,2|0}}(U_1, U_2|\mathbf{u}_0).$$

Then a codeword $\mathbf{x}(m_1, m_2, j_1, j_2, k_1, k_2)$ is chosen randomly from

$$\mathcal{T}^N_{P_{0,1,2},P_{X|U_1,U_2}}(X|\mathbf{u}_0, \mathbf{u}_1(m_1, j_1, k_1), \mathbf{u}_2(m_2, j_2, k_2)).$$

The codeword $\mathbf{x}(m_1, m_2, j_1, j_2, k_1, k_2)$ is transmitted through the channels and the channel outputs $\mathbf{y}_1$, $\mathbf{y}_2$ must be decoded. We apply the following minimum divergence decoding: decoder $g_i : \mathcal{Y}_i^N \to \mathcal{M}_{i,N}$, $i = 1, 2$, finds m_i such that for some $P^1_{Y_i|U_i,U_0}$ and j_i, k_i,

$$\mathbf{y}_i \in \mathcal{T}^N_{P_{0,i},P^1_{Y_i|U_i,U_0}}(Y_i|\mathbf{u}_0, \mathbf{u}_i(m_i, j_i, k_i))$$

and

$$D(P^1_{Y_i|U_i,U_0}\|P_{Y_i|U_i,U_0}|P_{0,i}) \text{ is minimal.}$$

For $i = 1, 2$, decoder g_i makes an error if message m_i is transmitted but there exists $m_i' \neq m_i$ such that for some j_i, j_i', k_i, k_i' and $P^{1'}_{Y_i|U_i,U_0}$:

$$\mathbf{y}_i \in \mathcal{T}^N_{P_{0,i},P^1_{Y_i|U_i,U_0}}(Y_i|\mathbf{u}_0, \mathbf{u}_i(m_i, j_i, k_i)) \bigcap \mathcal{T}^N_{P_0,P^{1'}_{Y_i|U_i,U_0}}(Y_i|\mathbf{u}_0, \mathbf{u}_i(m_i', j_i', k_i')),$$

bound

$$D(P^{1'}_{Y_i|U_i,U_0}\|P_{Y_i|U_i,U_0}|P_{0,i}) \le D(P^{1}_{Y_i|U_i,U_0}\|P_{Y_i|U_i,U_0}|P_{0,i}).$$

We consider the following sets $\mathcal{B}_i(P^{1'}_{Y_i|U_i,U_0})$, which are defined as the sets of all vectors $y_i \in \mathcal{Y}_i^N$ which can lead to error at receiver i,

$$B_i(P^{1'}_{Y_i|U_i,U_0}) \triangleq T^N_{P_{0,i},P^{1}_{Y_i|U_i,U_0}}(Y_i|\mathbf{u}_0, \mathbf{u}_i(m_i, j_i, k_i))$$

$$\bigcap \bigcup_{m_i' \neq m_i} \bigcup_{j_i' \in \mathcal{J}_i, k_i' \in \mathcal{K}_i} T^N_{P_{0,i},P^{1'}_{Y_i|U_i,U_0}}(Y_i|\mathbf{u}_0, \mathbf{u}_i(m_i', j_i', k_i')), \ i = 1, 2, \tag{19}$$

Let us define the following set of distributions $\mathcal{D}_i'(P^{1}_{Y_i|U_i,U_0}) = \{P^{1'}_{Y_i|U_i,U_0} \in \mathcal{V}_N(P_{0,i}, \mathcal{Y}_i) :$

$$\mathrm{D}(P^{1'}_{Y_i|U_i,U_0}\|P_{Y_i|U_i,U_0}|P_{0,i}) \le \mathrm{D}(P^{1}_{Y_i|U_i,U_0}\|P_{Y_i|U_i,U_0}|P_{0,i})\}, \ i = 1, 2.$$

Lemma 1. For the constructed code and N large enough the following inequalities are valid

$$|B_i(P^{1'}_{Y_i|U_i,U_0})| \le$$

$$\exp\{NH_{P_{0,i},P^{1}_{Y_i|U_i,U_0}}(Y_i|U_i, U_0)\} \exp\{-N|D(P^{1}_{Y_i|U_i,U_0}\|P_{Y_i|U_i,U_0}|P_{0,i}) - E_i|^+\}, \ i = 1, 2. \tag{20}$$

Proof. Proof is exposed in Appendix.

Now we prove that for any E_1, E_2, error probabilities of the code are decreasing exponentially. Let $i = 1, 2$, the encoder makes an error when there is no such a pair $(\mathbf{u}_1(m_1, j_1, k_1), \mathbf{u}_2(m_2, j_2, k_2))$ that have joint type $P_{1,2|0}$. Define for some j_1, j_2, k_1, k_2 the set

$$\mathcal{A} \triangleq \{(\mathbf{u}_1(m_1, j_1, k_1), \mathbf{u}_2(m_2, j_2, k_2)) : (\mathbf{u}_1(m_1, j_1, k_1), \mathbf{u}_2(m_2, j_2, k_2)) \in T^N_{P_{1,2|0}}(U_1, U_2|\mathbf{u}_0)\},$$

then probability of encoding error is

$$e(f) \triangleq \Pr\{\mathcal{A}^c\}.$$

So probability of error at receiver i to find m_i is

$$e_i(f, g_i, W_{Y_i|X}, m_1, m_2) \le e(f) + \Pr\{\bigcup_{P^{1}_{Y_i|U_i,U_0}} \bigcup_{P^{1'}_{Y_i|U_i,U_0} \in \mathcal{D}_i'(P^{1}_{Y_i|U_i,U_0})} \mathcal{B}_i(P^{1'}_{Y_i|U_i,U_0})|\mathbf{u}_i(m_i, j_i, k_i), \mathbf{u}_0\}.$$

Maximal probability of error at receiver i to find m_i is

$$e_i(f, g_i, W_{Y_i|X})$$

$$\le \max_{m_1 \in \mathcal{M}_{1,N}, m_2 \in \mathcal{M}_{2,N}} \left\{e(f) + \Pr\{\bigcup_{P^{1}_{Y_i|U_i,U_0}} \bigcup_{P^{1'}_{Y_i|U_i,U_0} \in \mathcal{D}_i'(P^{1}_{Y_i|U_i,U_0})} \mathcal{B}_i(P^{1'}_{Y_i|U_i,U_0})|\mathbf{u}_i(m_i, j_i, k_i), \mathbf{u}_0\}\right\}$$

$$\le^{(a)} \max_{m_1 \in \mathcal{M}_{1,N}, m_2 \in \mathcal{M}_{2,N}} \left\{e(f) + P_{Y_i|U_i,U_0}(\mathbf{y}_i|\mathbf{u}_i(m_i, j_i, k_i), \mathbf{u}_0) \times \right.$$

$$\left. |\bigcup_{P^{1}_{Y_i|U_i,U_0}} \bigcup_{P^{1'}_{Y_i|U_i,U_0} \in \mathcal{D}_i'(P^{1}_{Y_i|U_i,U_0})} \mathcal{B}_i(P^{1'}_{Y_i|U_i,U_0})|\right\}$$

$$\leq^{(b)} \epsilon_N + \max_{m_1 \in \mathcal{M}_{1,N}, m_2 \in \mathcal{M}_{2,N}} \sum_{P^1_{Y_i|U_i,U_0}} \sum_{P^{1'}_{Y_i|U_i,U_0} \in \mathcal{D}'_i(P^1_{Y_i|U_i,U_0})} P_{Y_i|U_i,U_0}(\mathbf{y}_i|\mathbf{u}_i(m_i, j_i, k_i)) \times |\mathcal{B}_i(P^{1'}_{Y_i|U_i,U_0})|$$

$$\leq^{(c)} \epsilon_N + \sum_{P^1_{Y_i|U_i,U_0}} \sum_{P^{1'}_{Y_i|U_i,U_0} \in \mathcal{D}'_i(P^1_{Y_i|U_i,U_0})} \exp\Big\{ - N[\mathrm{D}(P^1_{Y_i|U_i,U_0} \| P_{Y_i|U_i,U_0}|P_{0,i}) + H_{P_0,P^1_{Y_i|U_i,U_0}}(Y_i|U_i,U_0)]\Big\} \times \max_{m_i \in \mathcal{M}_{i,N}} |\mathcal{B}_i(P^{1'}_{Y_i|U_i,U_0})|, \tag{21}$$

where (a) follows from the definition of sets for decoding error (19); taking into account that $e(f) \leq \epsilon_N$, $\epsilon_N \to 0$ [11] and $P_{Y_i|U_i,U_0}(\mathbf{y}_i|\mathbf{u}_i, \mathbf{u}_0)$ is constant for fixed P_0, $P^1_{Y_i|U_i,U_0}$, we conclude (b); and (c) is consequence of (10).

By substituting (20) in (21) we obtain

$e_i(f, g_i, W_{Y_i|X}) \leq \epsilon_N +$

$$\sum_{P^1_{Y_i|U_i,U_0}} \sum_{P^{1'}_{Y_i|U_i,U_0} \in \mathcal{D}'_i(P^1_{Y_i|U_i,U_0})} \exp\Big\{ - N[\mathrm{D}(P^1_{Y_i|U_i,U_0} \| P_{Y_i|U_i,U_0}|P_{0,i}) + H_{P_0,P^1_{Y_i|U_i,U_0}}(Y_i|U_i,U_0)]\Big\}$$

$$\times \exp\Big\{ N[H_{P_0,P^1_{Y_i|U_i,U_0}}(Y_i|U_i,U_0) + \mathrm{D}(P^1_{Y_i|U_i,U_0} \| P_{Y_i|U_i,U_0}|P_{0,i}) - E_i]\Big\}$$

$$\leq \exp\{-N(E_i - \epsilon')\},$$

where ϵ' is a small positive number for N large enough.

Now we prove that the secrecy requirements (7) hold for BC-2CM.For brevity of notations we write $H(...)$ and $I(...)$ instead of $H_{P_{0,1,2},W_{Y_2|X}}(...)$ and $I_{P_{0,1,2},W_{Y_2|X}}(...)$, respectively.

$$H(M_{1,N}|\mathbf{Y}_2) \geq H(M_{1,N}|\mathbf{Y}_2, \mathbf{U}_2, \mathbf{U}_0) = H(M_{1,N}, \mathbf{Y}_2|\mathbf{U}_2, \mathbf{U}_0) - H(\mathbf{Y}_2|\mathbf{U}_2, \mathbf{U}_0)$$

$$= H(M_{1,N}, \mathbf{U}_1, \mathbf{Y}_2|\mathbf{U}_2, \mathbf{U}_0) - H(\mathbf{U}_1|\mathbf{Y}_2, \mathbf{U}_2, \mathbf{U}_0, M_{1,N}) - H(\mathbf{Y}_2|\mathbf{U}_2, \mathbf{U}_0)$$

$$= H(M_{1,N}, \mathbf{U}_1|\mathbf{U}_2, \mathbf{U}_0) - H(\mathbf{U}_1|\mathbf{Y}_2, \mathbf{U}_2, \mathbf{U}_0, M_{1,N}) - H(\mathbf{Y}_2|\mathbf{U}_2, \mathbf{U}_0) + H(\mathbf{Y}_2|\mathbf{U}_1, \mathbf{U}_2, \mathbf{U}_0, M_{1,N}) \tag{22}$$

Based on the random code construction, we can show that

$$I(M_{1,N} \wedge \mathbf{Y}_2|\mathbf{U}_0, \mathbf{U}_1, \mathbf{U}_2) = 0. \tag{23}$$

Hence, from (22) and (23), we obtain

$$H(M_{1,N}|\mathbf{Y}_2) \geq H(M_{1,N}, \mathbf{U}_1|\mathbf{U}_2, \mathbf{U}_0) - H(\mathbf{U}_1|\mathbf{Y}_2, \mathbf{U}_2, \mathbf{U}_0, M_{1,N}) - H(\mathbf{Y}_2|\mathbf{U}_2, \mathbf{U}_0) + H(\mathbf{Y}_2|\mathbf{U}_1, \mathbf{U}_2, \mathbf{U}_0)$$

$$\geq H(\mathbf{U}_1|\mathbf{U}_2, \mathbf{U}_0) - H(\mathbf{U}_1|\mathbf{Y}_2, \mathbf{U}_2, \mathbf{U}_0, M_{1,N}) - I(\mathbf{U}_1 \wedge \mathbf{Y}_2|\mathbf{U}_2, \mathbf{U}_0). \tag{24}$$

We estimate three terms in (24) separately. Note that given $\mathbf{U}_0 = \mathbf{u}_0$, $\mathbf{U}_1$ has $M_{1,N} \times J_1 \times K_1$ equiprobable possible values. So

$$H(\mathbf{U}_1|\mathbf{U}_0, \mathbf{U}_2) = H(\mathbf{U}_1|\mathbf{U}_0) - I(\mathbf{U}_1 \wedge \mathbf{U}_2|\mathbf{U}_0)$$

$$= \log(M_{1,N} \times J_1 \times K_1) - I(\mathbf{U}_1 \wedge \mathbf{U}_2|\mathbf{U}_0). \tag{25}$$

Lemma 2.

$$I(\mathrm{U}_1 \wedge \mathrm{Y}_2|\mathrm{U}_2, \mathrm{U}_0) \le NI(U_1 \wedge Y_2|U_2, U_0), \tag{26}$$

$$I(\mathrm{U}_1 \wedge \mathrm{U}_2|\mathrm{U}_0) \le NI(U_1 \wedge U_2|U_0). \tag{27}$$

Lemma 3.

$$\frac{1}{N} \lim_{N\to\infty} H(\mathrm{U}_1|\mathrm{Y}_2, \mathrm{U}_2, \mathrm{U}_0, M_{1,N}) = 0. \tag{28}$$

The proof is similar to the proof of lemma 3 in [14].

The proof is exposed in the Appendix.

By substituting (25), (26), (27) and (28) in (24) we achieve (7).

4. Conclusion

We derived a random coding bound for secrecy E-capacity region of the BC-2CM. The inner bound rate region is achieved by random binning techniques. When $E \to 0$, the random coding bound coincides with the inner bound for secrecy capacity region of the BC-2CM obtained by R. Liu, I. Maric, P. Spasojevic and R. Yates.

5. Appendix

Proof of Lemma 1. Let us note that if the collection of vectors

$$\{(\mathrm{u}_0, \mathrm{u}_i(m_i, j_i, k_i))\}_{m_i \in \mathcal{M}_{i,N}, j_i \in \mathcal{J}_i, k_i \in \mathcal{K}_i}$$

satisfy (20) for any $P^1_{Y_i|U_i,U_0}$, $P^{1'}_{Y_i|U_i,U_0}$, $i = 1, 2$, then $(\mathrm{u}_0, \mathrm{u}_i(m_i', j_i', k_i')) \ne (\mathrm{u}_0, \mathrm{u}_i(m_i, j_i, k_i))$ for $(m_1', m_2') \ne (m_1, m_2)$. To prove that, it is enough to choose $P^1_{Y_i|U_i,U_0} = P^{1'}_{Y_i|U_i,U_0}$ and $\mathrm{D}(P^{1'}_{Y_i|U_i,U_0}\|P_{Y_i|U_i,U_0}|P_{0,i}) < E_i$, $i = 1, 2$.

If $P^{1'}_{Y_i|U_i,U_0}$ is such that $\mathrm{D}(P^{1'}_{Y_i|U_i,U_0}\|P_{Y_i|U_i,U_0}|P_{0,i}) \ge E_i$ then

$$\exp\{-N|E_i - \mathrm{D}(P^{1'}_{Y_i|U_i,U_0}\|P_{Y_i|U_i,U_0}|P_{0,i})|^+\} = 1,$$

and (20) is valid for any $M_{i,N}$, J_i, K_i. It remains to prove inequality (20) for $P^{1'}_{Y_i|U_i,U_0}$ such that $\mathrm{D}(P^{1'}_{Y_i|U_i,U_0}\|P_{Y_i|U_i,U_0}|P_{0,i}) \le E_i, i = 1, 2$.

To prove (20), it is sufficient to prove the following inequality for the code generated and N large enough

$$\sum_{i=1,2} \sum_{P^1_{Y_i|U_i,U_0} \in \mathcal{V}_N(P_{0,i},\mathcal{Y}_i)} \sum_{P^{1'}_{Y_i|U_i,U_0} \in \mathcal{D}_i(E_i)} \mathrm{E}(|\mathcal{T}^N_{P_{0,i},P^1_{Y_i|U_i,U_0}}(Y|\mathrm{u}_0, \mathrm{u}_i(m_i, j_i, k_i))$$

$$\bigcap \bigcup_{m_i' \ne m_i} \bigcup_{j_i' \in \mathcal{J}_i, k_i' \in \mathcal{K}_i} \mathcal{T}^N_{P_{0,i},P^{1'}_{Y_i|U_i,U_0}}(Y_i|\mathrm{u}_0, \mathrm{u}_i(m_i', j_i', k_i'))|)$$

$$\times \exp\{-N[H_{P_{0,i},P^1_{Y_i|U_i,U_0}}(Y_i|U_i, U_0) - D(P^1_{Y_i|U_i,U_0}\|P_{Y_i|U_i,U_0}|P_{0,i}) + E_i]\} \le 1. \tag{29}$$

The expectations in summation (29) are estimated as follows,

$$\mathrm{E}(|\mathcal{T}^N_{P_{0,i},P^1_{Y_i|U_i,U_0}}(Y|\mathrm{u}_0, \mathrm{u}_i(m_i, j_i, k_i)) \bigcap \bigcup_{m_i' \ne m_i} \bigcup_{j_i' \in \mathcal{J}_i, k_i' \in \mathcal{K}_i} \mathcal{T}^N_{P_{0,i},P^{1'}_{Y_i|U_i,U_0}}(Y_i|\mathrm{u}_0, \mathrm{u}_i(m_i', j_i', k_i'))|)$$

$$\leq \sum_{\mathbf{y}\in\mathcal{T}^N_{P_{0,i},P^1_{Y_i|U_i,U_0}}} \sum_{(Y_i)\,m'\neq m} \Pr\{\mathbf{y}_i \in \mathcal{T}^N_{P_{0,i},P^1_{Y_i|U_i,U_0}}(Y|\mathbf{u}_0,\mathbf{u}_i(m_i,j_i,k_i))\}$$

$$\times \Pr\{\mathbf{y}_i \in \bigcup_{j_i'\in\mathcal{J}_i,k_i'\in\mathcal{K}_i} \mathcal{T}^N_{P_{0,i},P^{1'}_{Y_i|U_i,U_0}}(Y_i|\mathbf{u}_0,\mathbf{u}_i(m_i',j_i',k_i'))\}, \tag{30}$$

because the events in the brackets are independent.

The first probability in (30) is different from zero iff $\mathbf{y}_i \in \mathcal{T}^N_{P_{0,i},P^1_{Y_i|U_i,U_0}}(Y_i)$, then for N large enough

$$\Pr\{\mathbf{y}_i \in \mathcal{T}^N_{P_{0,i},P^1_{Y_i|U_i,U_0}}(Y_i|\mathbf{u}_0,\mathbf{u}_i(m_i,j_i,k_i))\}$$

$$= \frac{|\mathcal{T}^N_{P_{0,i},P^1_{Y_i|U_i,U_0}}(U_i|\mathbf{y}_i,\mathbf{u}_0)|}{|\mathcal{T}^N_{P_i}(U_i)|}$$

$$\leq (N+1)^{|\mathcal{Y}_i|}\exp\{-NI_{P_{0,i},P^1_{Y_i|U_i,U_0}}(Y_i\wedge U_i|U_0)\}$$

$$\leq \exp\{-N(I_{P_{0,i},P^1_{Y_i|U_i,U_0}}(Y_i\wedge U_i)-\delta/2)\}. \tag{31}$$

The second probability in (30) can be estimated as follows

$$\Pr\{\mathbf{y}_i \in \bigcup_{j_i'\in\mathcal{J}_i,k_i'\in\mathcal{K}_i} \mathcal{T}^N_{P_{0,i},P^{1'}_{Y_i|U_i,U_0}}(Y_i|\mathbf{u}_0,\mathbf{u}_i(m_i',j_i',k_i'))\}$$

$$\leq \sum_{j_i'\in\mathcal{J}_i,k_i'\in\mathcal{K}_i} \Pr\{\mathbf{y}_i \in \mathcal{T}^N_{P_{0,i},P^{1'}_{Y_i|U_i,U_0}}(Y_i|\mathbf{u}_0,\mathbf{u}_i(m_i',j_i',k_i'))\}$$

$$= \sum_{j_i'\in\mathcal{J}_i,k_i'\in\mathcal{K}_i} \frac{|\mathcal{T}^N_{P_{0,i},P^{1'}_{Y_i|U_i,U_0}}(U_i|\mathbf{u}_0,\mathbf{y}_i)|}{|\mathcal{T}^N_{P_i}(U_i)|}$$

$$\leq \sum_{j_i'\in\mathcal{J}_i,k_i'\in\mathcal{K}_i} \exp\{-N[I_{P_{0,i},P^{1'}_{Y_i|U_i,U_0}}(Y_i\wedge U_i|U_0)-\delta/4]\}$$

$$\leq \exp\{NI_{P_{0,i},P_{Y_{3-i}|U_{3-i},U_0}}(U_i\wedge Y_{3-i},U_{3-i}|U_0)\}\exp\{-N[I_{P_{0,i},P^{1'}_{Y_i|U_i,U_0}}(Y_i\wedge U_i|U_0)-\delta/4]\}, \tag{32}$$

where the last inequality is concluded from (15), (16) and (17). For some $P^{1'}_{Y_i|U_i}\in\mathcal{V}_N(P,\mathcal{Y}_i)$ from (14) we have

$$|\mathcal{M}_{i,N}| = \exp\{N[|I_{P_{0,i},P^{1'}_{Y_i|U_i,U_0}}(U_i\wedge Y_i|U_0)+\mathrm{D}(P^{1'}_{Y_i|U_i,U_0}\|P_{Y_i|U_i,U_0}|P_{0,i})-E_i|^+$$

$$-I_{P_{0,i},P_{Y_{3-i}|U_{3-i},U_0}}(U_i\wedge Y_{3-i},U_{3-i}|U_0)-\delta]\}. \tag{33}$$

Thus by substituting (33) in (30) and from (31), (32) taking into account the fact that the number of all $P^{1'}_{Y_i|U_i,U_0}$, $P^1_{Y_i|U_i,U_0}$, $i=1,2$, does not exceed $(N+1)^{2|\mathcal{Y}_i|(|\mathcal{Y}_1|+|\mathcal{Y}_2|)}$, for N large enough we conclude

$$\sum_{i=1,2}\sum_{V_{Y_i|U_i,U_0}\in\mathcal{V}_N(P_{0,i},\mathcal{Y}_i)}\sum_{P^{1'}_{Y_i|U_i,U_0}\in\mathcal{D}_i(E_i)} \mathbf{E}(|\mathcal{T}^N_{P_{0,i},P^1_{Y_i|U_i,U_0}}(Y|\mathbf{u}_0,\mathbf{u}_i(m_i,j_i,k_i))$$

$$\cap \bigcup_{m_i'\neq m_i,\,j_i'\in\mathcal{J}_i,k_i'\in\mathcal{K}_i} \mathcal{T}^N_{P_{0,i},P^{1'}_{Y_i|U_i,U_0}}(Y_i|\mathbf{u}_0,\mathbf{u}_i(m_i',j_i',k_i'))|)$$

$$\times \exp\{-N[H_{P_{0,i},P^1_{Y_i|U_i,U_0}}(Y_i|U_i,U_0) - D(P^1_{Y_i|U_i,U_0}\|P_{Y_i|U_i,U_0}|P_{0,i}) + E_i]\} \le 1.$$

Proof of Lemma 3. Let $P_e(W_{Y_2|X}, j_1, k_1)$ denote the probability of decoding error of (j_1, k_1) at receiver 2. From Fano's inequality we have

$$\frac{1}{N}H(\mathbf{U}_1|\mathbf{Y}_2, \mathbf{U}_2, \mathbf{U}_0, M_{1N}) \le \frac{1}{N}[1 + P_e(W_{Y_2|X}, j_1, k_1) \times \log(J_1 \times K_1)].$$

We prove that

$$P_e(W_{Y_2|X}, j_1, k_1) \to 0, \text{ when } N \to \infty.$$

For a given typical sequences pair $(\mathbf{u}_0, \mathbf{u}_2(m_2, j_2, k_2))$, let $\mathcal{A}_{\epsilon_N}(P_{U_1,Y_2|U_2,U_0}$ denote the set of jointly typical sequences $\mathbf{u}_1(m_1, j_1, k_1)$ and $\mathbf{y}_2$ with respect to $P_{U_1,Y_2|U_2,U_0}$. For a given $M_{1,N} = m_1$, decoder 2 chooses (j_1, k_1) so that

$$(\mathbf{u}_1(m_1, j_1, k_1), \mathbf{y}_2) \in \mathcal{A}_{\epsilon_N}(P_{U_1,Y_2|U_2,U_0}),$$

if such (j_1, k_1) exists and is unique. If there is no such a pair an error is declared. Similar to the proof of Lemma 2 [14] we can prove that $P_e(W_{Y_2|X}, j_1, k_1) \le \epsilon_N$, where $\epsilon_N \to 0$. So

$$\frac{1}{N}\lim_{N\to\infty} H(\mathbf{U}_1|\mathbf{Y}_2, \mathbf{U}_2, \mathbf{U}_0, M_{1,N}) = 0.$$

References

[1] T. M. Cover, "Broadcast channels", *IEEE Trans. Inf. Theory*, vol. IT-18, no. 1, pp. 2-14, 1972.

[2] T. M. Cover and J. A. Thomas, "*Elements of Information Theory*", 2nd edition, A Wiley-Interscience Publication, 2006.

[3] I. Csiszár and J. Körner, "Broadcast channel with confidential messages", *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339-348, 1978.

[4] I. Csiszár and J. Körner, "*Information Theory: Coding Theorems for Discrete Memoryless Systems*", New York, Wiley, 1981.

[5] S. I. Gelfand and M. S. Pinsker, "Capacity of broadcast channel with one deterministic component", *Probl. Pered. Inf.*, vol. 16, no. 1, pp. 17-25, 1980.

[6] E. A. Haroutunian, "Upper estimate of transmission rate for memoryless channel with countable number of output signals under given error probability exponent", (in Russian) *3rd All Union Conference on Theory of Information Transmission and Coding, Uzhgorod, Publishing House of the Uzbek Academy of Sciences*, pp. 83-86, 1967.

[7] E. A. Haroutunian, B. Belbashir, "Lower bound of the optimal transmission rate depending on given error probability exponent for discrete memoryless channel and for asymmetric broadcast channel", (in Russian), *Abstracts of Papers of 6th Int. Symp. Inf. Theory, Tashkent, USSR*, vol. 1, pp. 19-21, 1984.

[8] E. A. Haroutunian, "On Bounds for E-Capacity of DMC", *IEEE Trans. Inf. Theory*, vol. IT-53, no. 11, pp. 4210-4220, 2007.

[9] E. A. Haroutunian, M. E. Haroutunian and A. N. Harutyunyan, "Reliability criteria in information theory and in statistical hypothesis testing", *Foundations and Trends in Communications and Information Theory*, vol. 4, nos. 2-3, 2008.

[10] E. A. Haroutunian, M. E. Haroutunian and N. Afshar, "Random Coding Bound for E-capacity Region of the Wiretap Channel", *8th International Conference of Computer Science and Information Technologies, Yerevan*, pp. 121-124, 2011.

[11] M. E. Haroutunian, "Random coding bound for E-capacity region of the broadcast channel". *Mathematical Problems of Computer Science*, no. 21, pp. 50-60, 2000.

[12] M. Hayashi , R. Matsumoto, "Universally attainable error and information exponents for the broadcast channels with confidential messages", *Arxiv:1104.4285v2 [cs.IT]*, 24 April 2011.
[13] Y. Liang, H. V. Poor and S. Shamai, "Information theoretic security", *Foundations and Trends in Communications and Information Theory*, vol. 5, nos. 4-5, 2009.
[14] R. Liu, I. Maric, P. Spasojevic and R. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: secrecy rate regions", *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2493-2507, 2008.
[15] K. Marton, "A coding theorem for the discrete memoryless broadcast channel", *IEEE Trans. Inf. Theory*, vol. IT-25, no. 3, pp. 306-311, 1979.
[16] C. E. Shannon, "A mathematical theory of communication", *Bell Syst. Tech. J.*, – vol. 27, no. 3, pp. 379-423, 1948. 38, no. 5, pp. 611-659, 1959.
[17] A. D. Wyner, "The wire-tap channel", *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355-1387, 1975.
[18] J. Xu, Y. Cao and B. Chen, "Capacity bound for broadcast channels with confidential messages", *IEEE Trans. Inf. Theory*, vol. 55, no. 10, pp. 4529-4542, 2009.

Երկու գաղտնի հաղորդագրություններով լայնասփյուռ կապուղու գաղտնիության E-ունակության տիրույթի պատահական կոդավորման գնահատականը

Ն. Ավշար, Ե. Հարությունյան և Մ. Հարությունյան

Ամփոփում

Մ"նք հետազոտում ենք երկու անկախ գաղտնի հաղորդագրություններով ընդհատ առանց հիշողության լայնասփյուռ կապուղու գաղտնիության E-ունակության տիրույթը: Գաղտնիության մակարդակը չափվում է անորոշության արագությամբ: Կառուցված է գաղտնիության E-ունակության տիրույթի պատահական կոդավորման գնահատականը:

Граница случайного кодирования области E-пропускной способности секретности широковещательного канала с двумя секретными сообщениями

Н.Афшар, Е.Арутюнян и М. Арутюнян

Аннотация

Мы изучаем область секретной -пропускной способности дискретного широковещательного канала без памяти с двумя независимыми секретными сообщениями, посылаемыми двум адресатам. Уровень секретности измеряется скоростью неопределенности. Мы строим границу случайного кодирования для области секретной E-пропускной способности широковещательного канала с двумя секретными сообщениями.