Communications in Information and Systems
Vol. 12, No. 2, pp. 131-156, 2012

001

# RANDOM CODING BOUND FOR $E$-CAPACITY REGION OF THE BROADCAST CHANNEL WITH CONFIDENTIAL MESSAGES

NASRIN AFSHAR*, EVGUENI HAROUTUNIAN*, AND MARIAM HAROUTUNIAN*

**Abstract.** We study the discrete memoryless broadcast channel with confidential messages (BC-C). It involves two discrete memoryless channels with two sources, one encoder and two receivers. A common message must be transmitted at rate $R_0$ to both receivers and a private message to the intended receiver at rate $R_1$ while keeping the other receiver ignorant of it with equivocation rate $R_e$. We consider error probability exponents (reliabilities) $E_1$, $E_2$, $E_3$, of exponentially decrease of error probability, respectively, of the first decoder, the second decoder and of the decoder trying to find the confidential message. For $E = (E_1, E_2, E_3)$ the $E$-capacity region is the set of all achievable rate triples $R_0$, $R_1$, $R_e$ of codes with given reliabilities $E_1$, $E_2$, $E_3$. We construct a random coding bound for $E$-capacity region of the BCC. When error probability exponents are going to zero, the limit of this bound coincides with the capacity region of the BCC obtained by Csiszár and Körner. Meanwhile the attainable error probability exponents as a function of given rate triple proposed by Hayashi and Matsumoto are positive in the region which can be smaller than the capacity region of the BCC.

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

**1. Introduction.** The information theoretic security of multiterminal systems has attracted great attention last years [18]. One of the important objects of investigation is the broadcast channel with confidential messages (BCC) first studied by Csiszár and Körner [3]. The BCC involves two discrete memoryless channels with two sources, two receivers but one encoder. The model is depicted in Fig.1. One source sends common message to both receivers at rate $R_0$. The private message of the second source must be communicated to receiver 1 at rate $R_1$ while receiver 2 should be kept ignorant of it with equivocation rate greater than $R_e$.

Csiszár and Körner found the capacity region of the BCC [3]. Liu et al proposed bounds of the secrecy capacity region of the BCC with two confidential messages [19]. Xu et al obtained an inner bound for the capacity region of the BCC with one common message and two confidential messages [24]. Hayashi and Matsumoto constructed universally attainable error exponents for the BCC [15].

The $E$-capacity (rate-reliability function) is an important concept in information theory for channel coding, it is a generalization of the Shannon's channel capacity, presenting the dependence of optimal code rate $R$ on given reliability (error probability exponent) $E$. $E$-capacity denoted by $R(E)$ (or $C(E)$) is an inverse function to the Shannon's reliability function $E(R)$. For history of investigation of estimates

*Laboratory of Information Theory and Applied Statistics, Institute for Informatics and Automation Problems, Armenian National Academy of Sciences.E-mail: eghishe@sci.am

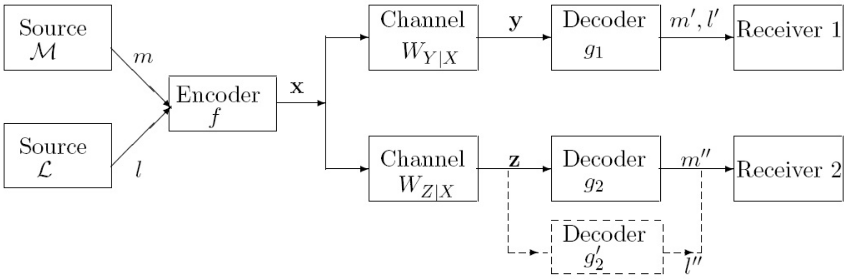

FIG. 1. *The discrete memoryless broadcast channel with confidential messages.*

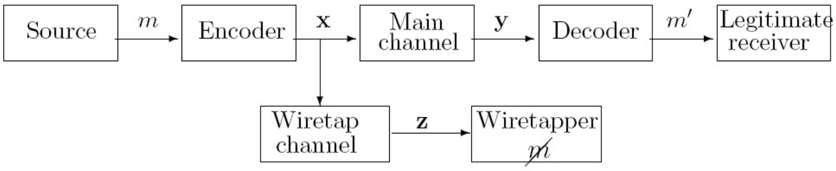

FIG. 2. *The generalized wiretap channel.*

for reliability function we refer to monographs of Gallager [5], Csiszár and Körner [4] and also [13]. The commonly accepted expression for the sphere packing bound of reliability function for two-terminal channels was introduced by Haroutunian [9]. Sphere packing bound for $E$-capacity of two-terminal channels was first constructed in [7], see also [9], [12]. Random coding bound for $E$-capacity of DMC was considered in [11], [12]. Random coding bound for $E$-capacity region of the broadcast channel with one common message and two private messages was found by M. Haroutunian [14]. The present paper is devoted to a single letter characterization of random coding bound for $E$-capacity region of the BCC.

Another problem concerned secure communication over a wiretap channel was first investigated by Wyner [23]. The wiretap channel considered by Csiszár and Körner [3] is a generalization (Fig.2) of the wiretap channel of Wyner. The secrecy capacity of the generalized wiretap channel was found in [3]. Random coding bound for $E$-capacity region of the generalized wiretap channel, where probability of the wiretapper's error decreases not exponentially, was studied in [13]. As a consequence of our result for the BCC we obtain a random coding bound for $E$-capacity region of the generalized wiretap channel when wiretapper's error probability decreases exponentially.

It should be noted, that the consideration of the $E$-capacity upper bound of secrecy leakage (see Proposition 1 in section 4) is a non-standard approach in the BCC and the wiretap channel's equivocation rate lower bound construction.

**2. Preliminaries and Problem Formulation.** Throughout this work, capital letters $X$, $Y$, ... represents random variables (RVs), and specific realizations of them are denoted by the corresponding lower case letters $x$, $y$, ... . Respective random vectors of length $N$ will be denoted by bold-faced letters $\mathbf{X}$, $\mathbf{Y}$, ... and $\mathbf{x}$, $\mathbf{y}$, ... . We denote all sets by script capitals. The cardinality of finite set $\mathcal{X}$ is denoted by $|\mathcal{X}|$.

We investigate a discrete memoryless BCC with an input alphabet $\mathcal{X}$ and output alphabets $\mathcal{Y}$ and $\mathcal{Z}$, correspondingly, on the first and second receivers. Vector $\mathbf{x} = (x_1, ..., x_N) \in \mathcal{X}^N$ is the input codeword, $\mathbf{y} = (y_1, ..., y_N) \in \mathcal{Y}^N$ and $\mathbf{z} = (z_1, ..., z_N) \in \mathcal{Z}^N$ are the output vectors. Let $\mathcal{U}_0$ and $\mathcal{U}_1$ be some additional finite sets and $U_0$, $U_1$, $X$, $Y$ and $Z$ be RVs with values, correspondingly, in $\mathcal{U}_0$, $\mathcal{U}_1$, $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$.

Let $Q_0 = \{Q_0(u_0),\, u_0 \in \mathcal{U}_0\}$ be the probability distribution (PD) of RV $U_0$, $Q_{1|0} = \{Q_{1|0}(u_1|u_0),\, u_0 \in \mathcal{U}_0,\, ,u_1 \in \mathcal{U}_1\}$ be conditional PD of RV $U_1$ for given value $u_0$ of RV $U_0$ and $Q_1 = \{Q_1(u_1) = \sum\limits_{u_0} Q_{1|0}(u_1|u_0)Q_0(u_0),\, u_1 \in \mathcal{U}_1\}$ be a PD of RV $U_1$.

We denote the joint PD of RVs $U_0$ and $U_1$ by

$$Q \triangleq Q_0 \circ Q_{1|0} \triangleq \{Q(u_0, u_1) = Q_0(u_0)Q_{1|0}(u_1|u_0),\, u_0 \in \mathcal{U}_0,\, u_1 \in \mathcal{U}_1\}$$

and use conditional PD $P_1 = \{P_1(x|u_1),\, x \in \mathcal{X},\, u_1 \in \mathcal{U}_1\}$ and marginal PD $P = \{P(x) = \sum\limits_{u_1} P_1(x|u_1)Q_1(u_1), x \in \mathcal{X}\}$. Let

$$V_{Y|X} = \{V_{Y|X}(y|x),\, x \in \mathcal{X},\, y \in \mathcal{Y}\} \text{ and } V_{Z|X} = \{V_{Z|X}(z|x),\, x \in \mathcal{X},\, z \in \mathcal{Z}\}$$

be some conditional PDs and $U_0 \to U_1 \to X \to (Y, Z)$ be a Markov chain.

The memoryless broadcast channel is defined by the conditional PDs $W_{Y|X} = \{W_{Y|X}(y|x),\ x \in \mathcal{X},\, y \in \mathcal{Y}\}$, $W_{Z|X} = \{W_{Z|X}(z|x),\, x \in \mathcal{X},\, z \in \mathcal{Z}\}$ and by products

$$W^N_{Y|X}(\mathbf{y}|\mathbf{x}) \triangleq \prod_{n=1}^{N} W_{Y|X}(y_n|x_n), \quad W^N_{Z|X}(\mathbf{z}|\mathbf{x}) \triangleq \prod_{n=1}^{N} W_{Z|X}(z_n|x_n).$$

The entropy of RV $X$ with PD $P$ is denoted by $H_P(X)$, and the conditional entropy of RV $Y$ relative to RV $X$ is $H_{P,V_{Y|X}}(Y|X)$. In this paper, log and exp are taken to the base 2. The notations $I_{P,V_{Y|X}}(X \wedge Y)$ and $I_{Q,P_1,V_{Y|X}}(X \wedge Y|U_0)$ are used for the mutual information of RVs $X$, $Y$ and the conditional mutual information of RVs $X$, $Y$ relative to RV $U_0$, respectively.

The divergence $D(V_{Y|X}\|W_{Y|X}|Q_1, P_1)$ is defined as

$$D(V_{Y|X}\|W_{Y|X}|Q_1, P_1) \triangleq \sum_{u_1,x,y} Q_1(u_1)P_1(x|u_1)V_{Y|X}(y|x) \log \frac{V_{Y|X}(y|x)}{W_{Y|X}(y|x)}.$$

Let $\mathcal{M}_N$ be the set of common messages, which should be sent to both receivers, and $\mathcal{L}_N$ be the set of private messages, which should be sent to receiver 1.

A block length $N$ *stochastic encoder* $f : \mathcal{M}_N \times \mathcal{L}_N \to \mathcal{X}^N$ for the BCC is specified by conditional probabilities $f(\mathbf{x}|m, l)$, $\mathbf{x} \in \mathcal{X}^N$, $m \in \mathcal{M}_N$, $l \in \mathcal{L}_N$, $\sum\limits_{\mathbf{x}\in\mathcal{X}^N} f(\mathbf{x}|m,l) = 1$.

A *code* is a triple $(f,\, g_1,\, g_2)$, where $f$ is a stochastic encoder, $g_1 : \mathcal{Y}^N \to \mathcal{M}_N \times \mathcal{L}_N$ and $g_2 : \mathcal{Z}^N \to \mathcal{M}_N$ are deterministic decoders.

The probabilities of erroneous transmission of the pair of messages $(m,\, l)$ by the channels $W_{Y|X}$ and $W_{Z|X}$ using a code $(f,\, g_1,\, g_2)$ are defined, respectively, as follows:

$$e_1(f,\, g_1,\, W_{Y|X},\, m,\, l) \triangleq \sum_{\mathbf{x}\in\mathcal{X}^N} f(\mathbf{x}|m,l) W^N_{Y|X}((g_1^{-1}(m,l))^c|\mathbf{x}),$$

$$e_2(f,\, g_2,\, W_{Z|X},\, m,\, l) \triangleq \sum_{\mathbf{x}\in\mathcal{X}^N} f(\mathbf{x}|m,l) W^N_{Z|X}((g_2^{-1}(m))^c|\mathbf{x}).$$

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

$$e_1(f,\, g_1,\, W_{Y|X}) \triangleq \max_{m\in\mathcal{M}_N, l\in\mathcal{L}_N} e_1(f,\, g_1,\, W_{Y|X},\, m,\, l), \tag{1a}$$

$$e_2(f,\, g_2,\, W_{Z|X}) \triangleq \max_{m\in\mathcal{M}_N, l\in\mathcal{L}_N} e_2(f,\, g_2,\, W_{Z|X},\, m,\, l), \tag{1b}$$

and the average error probabilities, assuming that random messages $M_N$, $L_N$ are uniformly distributed over $\mathcal{M}_N$ and $\mathcal{L}_N$, respectively, are:

$$\overline{e}_1(f,\, g_1,\, W_{Y|X}) \triangleq (|\mathcal{M}_N| \times |\mathcal{L}_N|)^{-1} \sum_{m\in\mathcal{M}_N, l\in\mathcal{L}_N} e_1(f,\, g_1,\, W_{Y|X},\, m,\, l), \tag{2a}$$

$$\overline{e}_2(f,\, g_2,\, W_{Z|X}) \triangleq (|\mathcal{M}_N| \times |\mathcal{L}_N|)^{-1} \sum_{m\in\mathcal{M}_N, l\in\mathcal{L}_N} e_2(f,\, g_2,\, W_{Z|X},\, m,\, l). \tag{2b}$$

Evidently

$$\overline{e}_1(f,\, g_1,\, W_{Y|X}) \leq e_1(f,\, g_1,\, W_{Y|X}), \quad \overline{e}_2(f,\, g_2,\, W_{Z|X}) \leq e_2(f,\, g_2,\, W_{Z|X}).$$

A code $(f, g_1,\, g_2)$ is characterized also by coding rates

$$R_0 \triangleq \lim_{N\to\infty} \frac{1}{N} \log|\mathcal{M}_N|\,, \quad R_1 \triangleq \lim_{N\to\infty} \frac{1}{N} \log|\mathcal{L}_N|. \tag{3}$$

The equivocation $H_{Q,P_1,W_{Z|X}}(L_N|\mathbf{Z})$ is the uncertainty of receiver 2 with respect to the private message. We also consider equivocation rate $(1/N)H_{Q,P_1,W_{Z|X}}(L_N|\mathbf{Z})$. Denoting by $R_e$ the lower bound for equivocation rate, we introduce the notion of *secrecy leakage* rate $R_s \triangleq R_1 - R_e$ as the rate of accessible information about private message $l$ at receiver 2. Let the private message set $\mathcal{L}_N$ be arranged in a matrix of dimension $A \times J$. It is supposed that $A$ is the information which can not be found by receiver 2. Let define the set $\mathcal{J} \triangleq \{1, ..., J\}$. We define another decoder $g_2' : \mathcal{Z}^N \to \mathcal{J}$, with which receiver 2 tries to find information about private message $l$. Maximal and average error probabilities at receiver 2 to determine $l$ are the following:

$$e_3(f,g_2',W_{Z|X}) \triangleq \max_{m\in\mathcal{M}_N, l\in\mathcal{L}_N} \sum_{\mathbf{x}\in\mathcal{X}^N} f(\mathbf{x}|m,l)W^N_{Z|X}((g_2^{'-1}(j))^c|\mathbf{x}). \tag{4}$$

$$\overline{e}_3(f,g_2',W_{Z|X}) \triangleq (|\mathcal{M}_N| \times |\mathcal{L}_N|)^{-1} \sum_{m\in\mathcal{M}_N, l\in\mathcal{L}_N} \sum_{\mathbf{x}\in\mathcal{X}^N} f(\mathbf{x}|m,l)W^N_{Z|X}((g_2^{'-1}(j))^c|\mathbf{x}). \tag{5}$$

Let $E=(E_1,E_2,E_3)$, $E_1>0$, $E_2>0$, $E_3>0$, and $\min(E_1,\, E_2,\, E_3)>\delta>0$. A rate-equivocation triple $R_0$, $R_1$, $R_e$ is called *$E$-achievable* for the BCC iff for $N$ large enough and every $\delta$

$$|\mathcal{M}_N| \geq \exp\{N(R_0-\delta)\}, \quad |\mathcal{L}_N| \geq \exp\{N(R_1-\delta)\}, \tag{6}$$

$$\liminf_{N\to\infty} \frac{1}{N} H_{Q,P_1,W_{Z|X}}(L_N|\mathbf{Z}) \geq R_e, \tag{7}$$

$$e_1(f,\, g_1,\, W_{Y|X}) \leq \exp\{-N(E_1-\delta)\}\,, \quad e_2(f,\, g_2,\, W_{Z|X}) \leq \exp\{-N(E_2-\delta)\}, \tag{8}$$

$$e_3(f,g_2',W_{Z|X}) \leq \exp\{-N(E_3-\delta)\}. \tag{9}$$

For the definition and bounds of the $E$-capacity of DMC we refer to [7], [9]-[12]. The $E$-capacity region $\mathcal{C}(E)$ of the BCC for maximal error probabilities is defined as the set of all $E$-achievable rate-equivocation tuples $(R_0,\, R_1,\, R_e)$. We denote by $\overline{\mathcal{C}}(E)$ the $E$-capacity region of the BCC when average error probabilities are applied in (8) and (9). Remark, that the problem of lower bounding the equivocation rate is equivalent to upper bounding of secrecy leakage rate. The upper bound for $E_3$-capacity of secrecy leakage will be inquired in Proposition 1.

Some definitions from the method of types follow (see [2], [4], [12]). Let $N(u_0|\mathbf{u}_0)$ be the number of occurrences of symbol $u_0$ in vector $\mathbf{u}_0 \in \mathcal{U}_0^N$ and $N(u_0,x|\mathbf{u}_0,\mathbf{x})$ be the number of repetitions of pair $(u_0,\,x)$ in vector pair $(\mathbf{u}_0,\,\mathbf{x}) \in \mathcal{U}_0^N \times \mathcal{X}^N$. The *type* of a vector $\mathbf{u}_0 \in \mathcal{U}_0^N$ is the empirical PD $Q_0$ on $\mathcal{U}_0$

$$Q_0 = \Big\{Q_0(u_0) = N(u_0|\mathbf{u}_0)/N, \;\; u_0 \in \mathcal{U}_0\Big\}.$$

The set of all $\mathbf{u}_0 \in \mathcal{U}_0^N$ with type $Q_0$ is denoted by $\mathcal{T}^N_{Q_0}(U_0)$. The conditional type of $\mathbf{x} \in \mathcal{X}^N$ given $\mathbf{u}_0 \in \mathcal{T}^N_{Q_0}(U_0)$ is the empirical conditional PD $P_0$ defined as

$$P_0(x|u_0) \triangleq \begin{cases} N(u_0,x|\mathbf{u}_0,\mathbf{x})/N(u_0|\mathbf{u}_0), & (u_0,x) \in \mathcal{U}_0 \times \mathcal{X},\; N(u_0|\mathbf{u}_0)>0, \\ 0, & N(u_0|\mathbf{u}_0)=0. \end{cases}$$

We denote the set of all $\mathbf{x} \in \mathcal{X}^N$ of conditional type $P_0$ with respect to $\mathbf{u}_0 \in \mathcal{T}^N_{Q_0}(U_0)$ by $\mathcal{T}^N_{Q_0,P_0}(X|\mathbf{u_0})$. Similarly to the definition of conditional type $P_0$ we define the conditional types $V_{Y|X}$ and $V_{Z|X}$ of $\mathbf{y}$ and $\mathbf{z}$ given $\mathbf{x}$ from $\mathcal{T}^N_{Q_0,P_0}(X|\mathbf{u}_0)$, respectively. The set of all $\mathbf{y}$ with conditional type $V_{Y|X}$ is denoted by $\mathcal{T}^N_{Q_0,P_0,V_{Y|X}}(Y|\mathbf{u}_0,\mathbf{x})$ and is called $V_{Y|X}$-*shell* of $\mathbf{u}_0$ and $\mathbf{x}$. Let $\mathcal{P}_N(\mathcal{X})$ be the set of all possible types of vectors of $\mathcal{X}^N$ and $\mathcal{V}_N(Q_0,P_0,\mathcal{Y})$ be the set of all conditional type of $\mathbf{y}$ given $\mathbf{x}$ from $\mathcal{T}^N_{Q_0,P_0}(X|\mathbf{u}_0)$. Similarly, $\mathcal{V}_N(Q_0,P_0,\mathcal{Z})$ and $\mathcal{T}^N_{Q_0,P_0,V_{Z|X}}(Z|\mathbf{u}_0,\mathbf{x})$ are defined.

Useful properties of types are the following [4]:

$$(10)\qquad |\mathcal{P}_N(\mathcal{X})| \leq (N+1)^{|\mathcal{X}|},\quad |\mathcal{V}_N(Q_0,P_0,\mathcal{Y})| < (N+1)^{|\mathcal{U}_0||\mathcal{X}||\mathcal{Y}|}.$$

If $V_{Y|X}$ and $V_{Z|X}$ are conditional types of, respectively, $\mathbf{y}$ and $\mathbf{z}$ given $\mathbf{x} \in \mathcal{T}^N_{Q_0,P_0}(X)$, then for $\mathbf{y} \in \mathcal{T}_{Q_0,P_0,V_{Y|X}}(Y|\mathbf{x})$ and for $\mathbf{z} \in \mathcal{T}_{Q_0,P_0,V_{Z|X}}(Z|\mathbf{x})$ we have

$$(11)\qquad W^N_{Y|X}(\mathbf{y}|\mathbf{x}) = \exp\{-N[D(V_{Y|X}\|W_{Y|X}|Q_0,P_0) + H_{Q_0,P_0,V_{Y|X}}(Y|X)]\},$$

$$(12)\qquad W^N_{Z|X}(\mathbf{z}|\mathbf{x}) = \exp\{-N[D(V_{Z|X}\|W_{Z|X}|Q_0,P_0) + H_{Q_0,P_0,V_{Z|X}}(Z|X)]\}.$$

For types $Q_0, P_0$

$$(13)\qquad (N+1)^{-|\mathcal{X}|}\exp\{NH_{Q_0,P_0}(X)\}\} < |\mathcal{T}^N_{Q_0,P_0}(X)| \leq \exp\{NH_{Q_0,P_0}(X)\},$$

and for every conditional type $V_{Y|X}$ and $\mathbf{x} \in \mathcal{T}^N_{Q_0,P_0}(X)$ if $\mathcal{T}_{Q_0,P_0,V_{Y|X}}(Y|\mathbf{x}) \neq \emptyset$, then

$$(14)\quad (N+1)^{-|\mathcal{X}||\mathcal{Y}|}\exp\{NH_{Q_0,P_0,V_{Y|X}}(Y|X)\}\} < |\mathcal{T}^N_{Q_0,P_0,V_{Y|X}}(Y|\mathbf{x})| \leq \exp\{NH_{Q_0,P_0,V_{Y|X}}(Y|X)\}.$$

**3. Result Formulation.** Consider RVs $X$, $Y$, $Z$ and auxiliary RVs $U_0$, $U_1$ with joint PDs:

(15)

$$Q\circ P_1\circ V_{Y|X} = \{Q\circ P_1\circ V_{Y|X}(u_0,u_1,x,y) = Q_0(u_0)Q_{1|0}(u_1|u_0)P_1(x|u_1)V_{Y|X}(y|x)\},$$

(16)

$$Q\circ P_1\circ V_{Z|X} = \{Q\circ P_1\circ V_{Z|X}(u_0,u_1,x,z) = Q_0(u_0)Q_{1|0}(u_1|u_0)P_1(x|u_1)V_{Z|X}(z|x)\}.$$

We define the following functions appearing in our inner estimates of $E$-capacity region:

$R^*_0(Q,P_1,E_1,E_2) \triangleq$

$$\min\left\{\min_{V_{Y|X}:D(V_{Y|X}\|W_{Y|X}|Q_1,P_1)\leq E_1}\left|I_{Q,P_1,V_{Y|X}}(U_0\wedge Y)+D(V_{Y|X}\|W_{Y|X}|Q_1,P_1)-E_1\right|^+,\right.$$

(17)

$$\left.\min_{V_{Z|X}:D(V_{Z|X}\|W_{Z|X}|Q_1,P_1)\leq E_2}\left|I_{Q,P_1,V_{Z|X}}(U_0\wedge Z)+D(V_{Z|X}\|W_{Z|X}|Q_1,P_1)-E_2\right|^+\right\},$$

$$R_1^*(Q,P_1,E_1) \triangleq$$

(18)
$$\min_{V_{Y|X}:D(V_{Y|X}\|W_{Y|X}|Q_1,P_1)\leq E_1} \left| I_{Q,P_1,V_{Y|X}}(U_1\wedge Y|U_0) + D(V_{Y|X}\|W_{Y|X}|Q_1,P_1) - E_1 \right|^+,$$

$$R_e^*(Q,P_1,E_1,E_3) \triangleq$$

$$\min_{V_{Y|X}:D(V_{Y|X}\|W_{Y|X}|Q_1,P_1)\leq E_1} \left| I_{Q,P_1,V_{Y|X}}(U_1\wedge Y|U_0) + D(V_{Y|X}\|W_{Y|X}|Q_1,P_1) - E_1 \right|^+ -$$

(19)
$$\min_{V_{Z|X}:D(V_{Z|X}\|W_{Z|X}|Q_1,P_1)\leq E_3} I_{Q,P_1,V_{Z|X}}(U_1\wedge Z|U_0).$$

Let us consider the following bounds of rates $R_0$, $R_1$, $R_e$:

(20a) $$0 \leq R_0 + R_1 \leq R_0^*(Q,P_1,E_1,E_2) + R_1^*(Q,P_1,E_1),$$

(20b) $$0 \leq R_0 \leq R_0^*(Q,P_1,E_1,E_2),$$

(20c) $$0 \leq R_e \leq R_e^*(Q,P_1,E_1,E_3),$$

(20d) $$R_e \leq R_1.$$

The main result of the paper is formulated in the following

THEOREM 1. *For* $E_1 > 0$, $E_2 > 0$, $E_3 > 0$, *the region*

(21) $$\mathcal{R}^*(E) \triangleq \bigcup_{Q,P_1} \{(R_0,\, R_1,\, R_e) : (20) \text{ take place for } U_0 \to U_1 \to X \to (Y,\, Z)\}$$

*is an inner bound for $E$-capacity region $\mathcal{C}(E)$ of the BCC*:

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

*Proof*: We expose the proof of Theorem 1 in section 4 and in Appendices. Concerning the ranges of $\mathcal{U}_0$ and $\mathcal{U}_1$, we can assert that they are the same as in Theorem 1 of [3].

The condition $R_e = R_1$ implies *perfect secrecy. Secrecy E-capacity* region $\mathcal{C}_s(E)$ of the BCC for the maximal error probabilities is the set of all $E$-achievable rate triples $(R_0,\, R_1,\, R_1)$.

COROLLARY 1. *The inner bound for secrecy $E$-capacity region $\mathcal{C}_s(E)$ consists of $(R_0,\, R_1,\, R_1)$ for which there exists a Markov chain $U_0 \to U_1 \to X \to (Y,\, Z)$ and*

$$0 \leq R_0 \leq R_0^*(Q,P_1,E_1,E_2),$$

$$0 \leq R_1 \leq R_e^*(Q,P_1,E_1,E_3).$$

Now we pass to consideration of the model of wiretap channel introduced by Csiszár and Körner (Fig. 2) and will find the random coding bound for $E$-capacity region of that.

Note the source message set by $\widehat{\mathcal{M}}_N$. We split $\widehat{\mathcal{M}}_N$ into two parts, one part is represented by $\mathcal{M}_N$ which must be sent to the legitimate receiver and can be received also by the eavesdropper. We denote the remaining part of messages by $\mathcal{L}_N$, which must be sent to the legitimate receiver, while keeping it secret from the eavesdropper. So message $\widehat{m}$ is splitted into two components: $m \in \mathcal{M}_N = \{1, ..., \exp\{NR_0\}\}$ and $l \in \mathcal{L}_N = \{1, ..., \exp\{NR_1\}\}$, and hence the transmission rates for $m$ and $l$ are $R_0$ and $R_1$, respectively. The channel input $\mathbf{x}$ is transmitted as outputs $\mathbf{y}$ and $\mathbf{z}$ to the legitimate receiver and the eavesdropper, respectively. Therefore, the wiretap channel can be considered as a special case of the BCC with $R = R_0 + R_1$.

COROLLARY 2. *The inner bound for $E$-capacity region $\mathcal{C}_W(E)$ of the generalized wiretap channel is:*

$$R^*_W(E) = \bigcup_{Q,P_1} \Big\{ (R,\, R_e) : \ \textit{for} \ \ U_0 \to U_1 \to X \to (Y,Z)$$

$$0 \le R \le R^*_0(Q,P_1,E_1,E_2) + R^*_1(Q,P_1,E_1),$$
$$0 \le R_e \le R^*_e(Q,P_1,E_1,E_3),$$
$$R_e \le R \Big\}.$$

COROLLARY 3. *If $E = (E_1,\, E_2,\, E_3) \to 0$, the achievable region* (21) *of Theorem 1 tends to the region, which coincides with the capacity region of the BCC from* [3], *determined by*

$$\mathcal{C} = \Big\{ (R_0, R_1, R_e) : \quad \textit{for}\ U_0 \to U_1 \to X \to (Y,Z),$$

$$0 \le R_0 + R_1 \le \min\Big\{ I_{Q,P_1,W_{Y|X}}(U_0 \wedge Y),\ I_{Q,P_1,W_{Z|X}}(U_0 \wedge Z) \Big\}$$

$$+\, I_{Q,P_1,W_{Y|X}}(U_1 \wedge Y|U_0), \tag{22a}$$

$$0 \le R_0 \le \min\Big\{ I_{Q,P_1,W_{Y|X}}(U_0 \wedge Y),\ I_{Q,P_1,W_{Z|X}}(U_0 \wedge Z) \Big\}, \tag{22b}$$

$$0 \le R_e \le I_{Q,P_1,W_{Y|X}}(U_1 \wedge Y|U_0) - I_{Q,P_1,W_{Z|X}}(U_1 \wedge Z|U_0), \tag{22c}$$

$$R_e \le R_1 \Big\}. \tag{22d}$$

In the following corollaries we compare the particular cases of our result with the achievable regions found in [14], [16] and [17].

When $R_e = 0$ in the BCC, the secrecy requirement is removed and the coding problem relates to the broadcast channel with degraded message sets, which was considered by Körner and Marton [16]. The capacity region of the broadcast channel with degraded message sets is given by the set of rates $R_0$, $R_1$ such that there exists a Markov chain $U_0 \to X \to (Y,\, Z)$ and

$$\begin{aligned} 0 \leq & R_0 + R_1 \leq I_{Q,P_1,W_{Y|X}}(X \wedge Y|U_0) \\ & \qquad + \min\{I_{Q,P_1,W_{Y|X}}(U_0 \wedge Y),\, I_{Q,P_1,W_{Z|X}}(U_0 \wedge Z)\}, \end{aligned} \tag{23a}$$

$$0 \leq R_0 \leq \min\{I_{Q,P_1,W_{Y|X}}(U_0 \wedge Y),\, I_{Q,P_1,W_{Z|X}}(U_0 \wedge Z)\}. \tag{23b}$$

Corollary 4. *When $R_e = 0$ and $E \to 0$, with* (17)-(19) *we see that the achievable region* (21) *converges to the capacity region of the broadcast channel with degraded message sets* (23).

Corollary 5. *When $R_e = 0$, then* (20c) *and* (20d) *are removed and we obtain the inner bound for $E$-capacity region of the broadcast channel with degraded message sets. This bound coincides with the random coding bound of the $E$-capacity region of the broadcast channel obtained by M. Haroutunian in* [14] *when* $R_2 = 0$.

Consider now the broadcast channel with degraded message sets, defined by $W_{Y|X} : \mathcal{X} \to \mathcal{Y}$, $W_{Z|X} : \mathcal{X} \to \mathcal{Z}$. Körner and Sgarro [17] introduced the bounds of pair of attainable error exponents $(E_1,\, E_2)$ for given rates $R_0$, $R_1$:

$$\begin{aligned} & 0 \leq E_1 \leq \min_{V_{Y|X}} \Big\{ D(V_{Y|X} \| W_{Y|X}|Q_1, P_1) \\ & \quad + \min\{|I_{Q,P_1,V_{Y|X}}(U_0, X \wedge Y) - (R_0 + R_1)|^+, |I_{Q,P_1,V_{Y|X}}(X \wedge Y|U_0) - R_1|^+\} \Big\}, \end{aligned} \tag{24a}$$

$$0 \leq E_2 \leq \min_{V_{Z|X}} \Big\{ D(V_{Z|X} \| W_{Z|X}|Q_1, P_1) + |I_{Q,P_1,V_{Z|X}}(U_0 \wedge Z) - R_0|^+ \Big\}. \tag{24b}$$

We deduced the following bounds for rates $R_0$, $R_1$ as a function of exponents

$E_1$, $E_2$ as inverse to relations defined by (24):

(25a)
$$
\begin{aligned}
0 \le R_0 + R_1 \le \min\Big\{ &\min_{V_{Y|X}: D(V_{Y|X}\|W_{Y|X}|Q_1,P_1)\le E_1} |I_{Q,P_1,V_{Y|X}}(U_0 \wedge Y) \\
&+ D(V_{Y|X}\|W_{Y|X}|Q_1,P_1) - E_1|^+, \\
\min_{V_{Z|X}: D(V_{Z|X}\|W_{Z|X}|Q_1,P_1)\le E_2} &|I_{Q,P_1,V_{Z|X}}(U_0 \wedge Z) + D(V_{Z|X}\|W_{Z|X}|Q_1,P_1) - E_2|^+\Big\} \\
&+ \min_{V_{Y|X}: D(V_{Y|X}\|W_{Y|X}|Q_1,P_1)\le E_1} |I_{Q,P_1,V_{Y|X}}(X \wedge Y|U_0) \\
&+ D(V_{Y|X}\|W_{Y|X}|Q_1,P_1) - E_1|^+,
\end{aligned}
$$

(25b)
$$
\begin{aligned}
&0 \le R_0 \le \\
&\min\Big\{ \min_{V_{Y|X}: D(V_{Y|X}\|W_{Y|X}|Q,P_1)\le E_1} |I_{Q,P_1,V_{Y|X}}(U_0 \wedge Y) \\
&\qquad + D(V_{Y|X}\|W_{Y|X}|Q,P_1) - E_1|^+, \\
&\min_{V_{Z|X}: D(V_{Z|X}\|W_{Z|X}|Q,P_1)\le E_2} |I_{Q,P_1,V_{Z|X}}(U_0 \wedge Z) + D(V_{Z|X}\|W_{Z|X}|Q,P_1) - E_2|^+\Big\}.
\end{aligned}
$$

Corollary 6. *In the case* $R_e = 0$, *the* $E$*-achievable region* (20) *becomes the following*

$$0 \le R_0 + R_1 \le R_0^*(Q, P_1, E_1, E_2) + R_1^*(Q, P_1, E_1), \tag{26a}$$

$$0 \le R_0 \le R_0^*(Q, P_1, E_1, E_2), \tag{26b}$$

*which coincides with region defined in* (25).

Hayashi and Matsumoto considered universally attainable error exponents $E_1$, $E_2$ for the BCC as a function of given positive rates $R_0$, $R_1$, $R_e$ [15]. We compare the inverse relation between two groups of multiple variables which express bounds in [15] with our result in Theorem 1 in extremal case, when $E \to 0$. In remark 12 of [15] it is noted that "the coding scheme used in the proof can achieve a rate triple ($R_0$, $R_1$, $R_e$) if there exists a Markov chain $U_0 \to U_1 \to X \to (Y, Z)$ such that

$$0 \le R_1 \le I_{Q,P_1,W_{Y|X}}(U_1 \wedge Y|U_0), \tag{27a}$$

$$0 \le R_0 \le \min\{I_{Q,P_1,W_{Y|X}}(U_0 \wedge Y),\ I_{Q,P_1,W_{Z|X}}(U_0 \wedge Z)\}, \tag{27b}$$

$$0 \le R_e \le I_{Q,P_1,W_{Y|X}}(U_1 \wedge Y|U_0) - I_{Q,P_1,W_{Z|X}}(U_1 \wedge Z|U_0), \tag{27c}$$

$$R_e \le R_1.\text{"} \tag{27d}$$

Remark. *The region* (27) *could be smaller than the capacity region* $\mathcal{C}$ (22), *because of distinction of* (27a) *and* (22a).

**4. Proof of Theorem 1.** The steps of the proof consist of proofs of 4 lemmas and Proposition 1.

LEMMA 1. *If the region*

$$\mathcal{R}_1^*(E) \stackrel{\triangle}{=} \bigcup_{Q,P_1} \Big\{(R_0,\, R_1,\, R_e): \quad for \;\; U_0 \to U_1 \to X \to (Y,Z)$$

$$0 \le R_1 \le R_1^*(Q,P_1,E_1),$$

$$0 \le R_0 \le R_0^*(Q,P_1,E_1,E_2),$$

$$0 \le R_e \le R_e^*(Q,P_1,E_1,E_3),$$

$$R_e \le R_1\Big\}.$$

*is $E$-achievable, then $\mathcal{R}^*(E)$ is $E$-achievable.*

*Proof.* Let us introduce

$$R_0' \stackrel{\triangle}{=} R_0 - \delta, \quad R_1' \stackrel{\triangle}{=} R_1 + \delta, \quad \text{and} \quad R_e' \stackrel{\triangle}{=} R_e, \tag{28}$$

where $0 \le \delta \le R_0$. Region $\mathcal{R}^*(E)$ can be obtained by substituting (28) into the definition of region $\mathcal{R}_1^*(E)$ and by the *Fourier-Motzkin elimination* to remove $\delta$ (see section 5.2. of [18]).

Let us now consider the new region $R_2^*(E)$ which can be obtained by replacing $U_1$ by $X$ in (17) - (19) in the following way:

$$R_0^*(Q_0,P_0,E_1,E_2) \stackrel{\triangle}{=} \min\Big\{ \min_{V_{Y|X}:D(V_{Y|X}\|W_{Y|X}|Q_0,P_0)\le E_1} \Big| I_{Q_0,P_0,V_{Y|X}}(U_0 \wedge Y)$$

$$+ D(V_{Y|X}\|W_{Y|X}|Q_0,P_0) - E_1\Big|^+,$$

$$\min_{V_{Z|X}:D(V_{Z|X}\|W_{Z|X}|Q_0,P_0)\le E_2} \Big| I_{Q_0,P_0,V_{Z|X}}(U_0 \wedge Z) + D(V_{Z|X}\|W_{Z|X}|Q_0,P_0) - E_2\Big|^+\Big\},$$

$$R_1^*(Q_0,P_0,E_1) \stackrel{\triangle}{=}$$

$$\min_{V_{Y|X}:D(V_{Y|X}\|W_{Y|X}|Q_0,P_0)\le E_1} \Big| I_{Q_0,P_0,V_{Y|X}}(X \wedge Y|U_0) + D(V_{Y|X}\|W_{Y|X}|Q_0,P_0) - E_1\Big|^+,$$

$$R_e^*(Q_0,P_0,E_1,E_3) \stackrel{\triangle}{=}$$

$$\min_{V_{Y|X}:D(V_{Y|X}\|W_{Y|X}|Q_0,P_0)\le E_1} \Big| I_{Q_0,P_0,V_{Y|X}}(X \wedge Y|U_0) + D(V_{Y|X}\|W_{Y|X}|Q_0,P_0) - E_1\Big|^+ -$$

$$\min_{V_{Z|X}:D(V_{Z|X}\|W_{Z|X}|Q_0,P_0)\leq E_3} I_{Q_0,P_0,V_{Z|X}}(U_1\wedge Z|U_0).$$

$$\mathcal{R}_2^*(E)\triangleq\bigcup_{Q_0,P_0}\Big\{(R_0,\,R_1,\,R_e):\ \textit{for}\ U_0\to X\to(Y,\,Z)$$

$$0\leq R_0\leq R_0^*(Q_0,P_0,E_1,E_2),\tag{29a}$$

$$0\leq R_1\leq R_1^*(Q_0,P_0,E_1),\tag{29b}$$

$$0\leq R_e\leq R_e^*(Q_0,P_0,E_1,E_3),\tag{29c}$$

$$R_e\leq R_1,\Big\}.\tag{29d}$$

The following inclusion is clear:

$$\mathcal{R}_2^*(E)\subseteq\mathcal{R}_1^*(E).$$

LEMMA 2. *If the region $\mathcal{R}_2^*(E)$ is $E$-achievable, then $\mathcal{R}_1^*(E)$ is $E$-achievable.*

*Proof.* We put a DMC from $U_1$ to $X$ with the transition PD $P_1$. Then similarly to the proof of Lemma 4 from [3], we can prove that the region $\mathcal{R}_1^*(E)$ is also $E$-achievable.

Now let us define the following sets of distributions:

$$\mathcal{D}_1(Q_0,\,P_0,\,E_1)=\{V'_{Y|X}\in\mathcal{V}_N(Q_0,\,P_0,\,\mathcal{Y}):\ D(V'_{Y|X}\|W_{Y|X}|Q_0,P_0)\leq E_1\},$$

$$\mathcal{D}_2(Q_0,\,P_0,\,E_2)=\{V'_{Z|X}\in\mathcal{V}_N(Q_0,\,P_0,\,\mathcal{Z}):\ D(V'_{Z|X}\|W_{Z|X}|Q_0,P_0)\leq E_2\},$$

$$\mathcal{D}_3(Q_0,\,P_0,\,E_3)=\{V'_{Z|X}\in\mathcal{V}_N(Q_0,\,P_0,\,\mathcal{Z}):\ D(V'_{Z|X}\|W_{Z|X}|Q_0,P_0)\leq E_3\}.$$

We shall prove that for all $E_1>0$, $E_2>0$, the region $\mathcal{R}_2^*(E)$ is $E$-achievable. We must show that for each $\delta>0$, $E_1$, $E_2$, $E_3$ and sufficiently large $N$ there exists a code with

$$|\mathcal{M}_N|=\exp\Big\{N\min\{\min_{V_{Y|X}\in\mathcal{D}_1(Q_0,\,P_0,\,E_1)}|I_{Q_0,P_0,V_{Y|X}}(U_0\wedge Y)$$
$$+D(V_{Y|X}\|W_{Y|X}|Q_0,P_0)-E_1-\delta|^+,$$
$$\min_{V_{Z|X}\in\mathcal{D}_2(Q_0,\,P_0,\,E_2)}|I_{Q_0,P_0,V_{Z|X}}(U_0\wedge Z)+D(V_{Z|X}\|W_{Z|X}|Q_0,P_0)-E_2-\delta|^+\}\Big\},\tag{30}$$

$$|\mathcal{L}_N|=\exp\Big\{N\min_{V_{Y|X}\in\mathcal{D}_1(Q_0,\,P_0,\,E_1)}|I_{Q_0,P_0,V_{Y|X}}(X\wedge Y|U_0)$$
$$+D(V_{Y|X}\|W_{Y|X}|Q_0,P_0)-E_1-\delta|^+\Big\},\tag{31}$$

such that maximal probabilities of error satisfy (8) and the equivocation rate is lower bounded by $R_e^*(Q_0, P_0, E_1, E_3)$. Since the secrecy leakage rate is $R_1 - R_e$, if $R_e^*(Q_0, P_0, E_1, E_3)$ is a lower bound for the equivocation rate and $R_1^*(Q_0, P_0, E_1)$ is an upper bound for $R_1$ then the secrecy leakage rate is upper bounded by $R_1^*(Q_0, P_0, E_1)$ $-R_e^*(Q_0, P_0, E_1, E_3)$. Hence in order to lower bound the equivocation rate we prove that $R_1^*(Q_0, P_0, E_1) - R_e^*(Q_0, P_0, E_1, E_3)$ is an upper bound for the secrecy leakage rate. In the following we show the existence of a code with certain properties which satisfies (6)-(9).

We modify the code constructed by Csiszár and Körner in [3] and use *minimum divergence* [12] decoding rule. We arrange elements of set $\mathcal{L}_N$ in a rectangular matrix of dimension $A \times J$ so that private message $l$ is located in the row of index $a$ and the column of index $j$. This matrix is known to receiver 1. The information about private message $l$ contained in $\mathbf{x}$ is partially available to receiver 2, we assume that it can find $j$, and $a$ presents uncertainty of receiver 2 about private message $l$. We shall lower bound the equivocation rate by $\frac{1}{N}\log A$. We use the set $\mathcal{A} \overset{\triangle}{=} \{1, ..., A\}$. To define the stochastic encoding the coder introduces a mapping $\varphi(b) = j$ from $\mathcal{B} = \{1, ..., B\}$ to $\mathcal{J} = \{1, ..., J\}$, with $B \geq J$. In order to lower bound the equivocation rate we upper bound secrecy leakage rate by $\frac{1}{N}\log B$.

**Code construction:** Let $\mathcal{U}_0$ be some finite set and $Q_0$ be a type on $\mathcal{U}_0$. Let $P_0$ be a conditional type of $\mathbf{x} \in \mathcal{X}^N$ for given $\mathbf{u}_0 \in \mathcal{T}_{Q_0}^N(U_0)$. We generate the codebook by the following steps.

First, we choose $|\mathcal{M}_N|$ vectors $\mathbf{u}_{0m}$ from $\mathcal{T}_{Q_0}^N(U_0)$. Then we draw $A \times B$ codewords $\mathbf{x}_{m,a,b}$ from $P_0$-shell $\mathcal{T}_{Q_0,P_0}^N(X|\mathbf{u}_{0m})$ for each $\mathbf{u}_{0m}$, where

$$A = \exp\{N[\min_{V_{Y|X} \in \mathcal{D}_1(Q_0,P_0,E_1)} |I_{Q_0,P_0,V_{Y|X}}(X \wedge Y|U_0)$$

$$+D(V_{Y|X}\|W_{Y|X}|Q_0,P_0) - E_1 - \delta/4|^+ -$$

$$\min_{V_{Z|X} \in \mathcal{D}_3(Q_0,P_0,E_3)} (I_{Q_0,P_0,V_{Z|X}}(U_1 \wedge Z|U_0) - \delta/4)]\}, \tag{32}$$

$$B = \exp\{N \min_{V_{Z|X} \in \mathcal{D}_3(Q_0,P_0,E_3)} (I_{Q_0,P_0,V_{Z|X}}(U_1 \wedge Z|U_0) - \delta/4)\}. \tag{33}$$

We arrange codewords in $|\mathcal{M}_N|$ classes and every class contains $A \times B$ codewords.

Let $J$ be such a number that

$$|\mathcal{L}_N| = \exp\{NR_1\} = A \times J.$$

From (31), (32) and (33) we can observe that $|\mathcal{L}_N| \leq A \times B$. To encode message $l = (a,\, j)$ we shall choose a pair $(a,\, b)$. To this end, a function $\varphi$ is defined to partition every class $m$ of codewords into $|\mathcal{L}_N|$ subsets of nearly equal size. Then we choose randomly a pair $(a,\, b_j)$ from $\{(a,\, b) : b \in \varphi^{-1}(j)\}$. Finally, we define encoder $f : (m,\, l) \to \mathbf{x}_{m,a,b_j}$.

For notational convenience we write $\mathbf{x}_{m,a,b}$ instead of $\mathbf{x}_{m,a,b_j}$. In the following expressions we omit the notation of PDs $Q_0$ and $P_0$, because they are constant; For instance, we will write:

$$\mathcal{T}^N_{Q_0,P_0,V'_{Y|X}}(Y|...) = \mathcal{T}^N_{V'_{Y|X}}(Y|...) \quad , \quad D(V'_{Y|X}\|W_{Y|X}|Q_0,P_0) = D(V'_{Y|X}\|W_{Y|X}).$$

The channels output vectors $\mathbf{y}$ and $\mathbf{z}$ will be decoded in the following way.

Every $\mathbf{y}$ first is decoded to $(m',\, a',\, b')$ as follows

$$(m',\, a',\, b') = \underset{V'_{Y|X}:\mathbf{y}\in\mathcal{T}^N_{V'_{Y|X}}(Y|\mathbf{u}_{0m'},\mathbf{x}_{m',a',b'})}{\operatorname{argmin}} D(V'_{Y|X}\|W_{Y|X}),$$

then applying the function $\varphi(b') = j'$, decoder 1 finds $m'$, $l'$.

Every $\mathbf{z}$ is decoded to such $m''$ that for some $a''$, $b''$

$$m'' = \underset{V'_{Z|X}:\mathbf{z}\in\mathcal{T}^N_{V'_{Z|X}}(Y|\mathbf{u}_{0m''},\mathbf{x}_{m'',a'',b''})}{\operatorname{argmin}} D(V'_{Z|X}\|W_{Z|X}).$$

Lemma 3. (Packing Lemma) *For the constructed code, for $N$ large enough the following is valid,*

$$\sum_{V_{Y|X}}\ \sum_{V'_{Y|X}\in\mathcal{D}_1(E_1)} [\mathbf{E}(|\mathcal{T}^N_{V_{Y|X}}(Y|\mathbf{u}_{0m},\mathbf{x}_{m,a,b}) \bigcap \bigcup_{m'\neq m}\ \bigcup_{a'\in\mathcal{A},b'\in\mathcal{B}} \mathcal{T}^N_{V'_{Y|X}}(Y|\mathbf{u}_{0m'},\mathbf{x}_{m',a',b'})|)$$

$$+\mathbf{E}(|\mathcal{T}^N_{V_{Y|X}}(Y|\mathbf{u}_{0m},\mathbf{x}_{m,a,b}) \bigcap \bigcup_{(a',b')\neq(a,b)} \mathcal{T}^N_{V'_{Y|X}}(Y|\mathbf{u}_{0m},\mathbf{x}_{m,a',b'})|)]$$

$$\times \exp\{-N(H_{V_{Y|X}}(Y|X) - E_1 - D(V'_{Y|X}\|W_{Y|X}))\}$$

$$+\sum_{V_{Z|X}}\ \sum_{V'_{Z|X}\in\mathcal{D}_2(E_2)} [\mathbf{E}(|\mathcal{T}^N_{V_{Z|X}}(Z|\mathbf{u}_{0m},\mathbf{x}_{m,a,b}) \bigcap \bigcup_{m''\neq m} \mathcal{T}^N_{V'_{Z|X}}(Z|\mathbf{u}_{0m''},\mathbf{x}_{m'',a'',b''})|)$$

$$\times \exp\{-N(H_{V_{Z|X}}(Z|X) - E_1 - D(V'_{Z|X}\|W_{Z|X}))\}\} \leq 1. \tag{34}$$

Proof is exposed in Appendix 1.

The following Proposition is a generalization of the Theorem from [7], [9], [11] and [12] about sphere packing bound of $E$-capacity of DMC.

Proposition 1. *For $E_3 > 0$,*

$$\max_{Q_0,P_0}\ \min_{V_{Z|X}:D(V_{Z|X}\|W_{Z|X|Q_0,P_0})\leq E_3} I_{Q_0,P_0,V_{Z|X}}(X\wedge Z|U_0)$$

*is a sphere packing bound for $E_3$-capacity of secrecy leakage of receiver 2.*

Proposition 1 will be proved in Appendix 2.

Based on Lemma 3 and Proposition 1, we obtain the $E$-achievability of region $\mathcal{R}_2^*(E)$ in the next.

LEMMA 4. *By the described code the rate triple $(R_0,\, R_1,\, R_e)$ satisfying (29) is $E$-achievable.*

Proof is exposed in Appendix 3.

From Lemma 4 we obtained that region $\mathcal{R}_2^*(E)$ is $E$-achievable. To complete the proof of Theorem 1 we must prove the $E$-achievability of $\mathcal{R}^*(E)$. Lemma 1 and 2 assert that if $\mathcal{R}_2^*(E)$ is $E$-achievable, then $\mathcal{R}^*(E)$ is $E$-achievable. Therefore, proof of Theorem 1 is complete.

**5. Conclusion.** We studied the BCC, and derived a random coding bound for $E$-capacity region. We also obtained an inner bound for $E$-capacity region of the generalized wiretap channel.

To compare our main result with universally error exponents as function of $R_0$ and $R_1$ proposed by Hayashi and Matsumoto [15] for the BCC we consider the extremal case, when $E \to 0$. Our inner bound of $E$-capacity coincides with capacity region found by Csiszár and Körner [3], but the region, where the estimates from [15] are valid, could be smaller than the capacity region of the BCC.

**Appendix 1. Proof of Lemma 3.** We estimate three expectations in summation (34) separately. The first expectation is estimated as follows,

$$\mathbf{E}(|\mathcal{T}^N_{V_{Y|X}}(Y|\mathbf{u}_{0m},\mathbf{x}_{m,a,b})\bigcap\bigcup_{m'\neq m}\bigcup_{a'\in\mathcal{A},b'\in\mathcal{B}}\mathcal{T}^N_{V'_{Y|X}}(Y|\mathbf{u}_{0m'},\mathbf{x}_{m',a',b'})|)$$

$$\le\sum_{\mathbf{y}\in\mathcal{T}^N_{V_{Y|X}}(Y)}\sum_{m'\neq m}\Pr\{\mathbf{y}\in\mathcal{T}^N_{V_{Y|X}}(Y|\mathbf{u}_{0m},\mathbf{x}_{m,a,b})\}$$

$$\times\Pr\{\mathbf{y}\in\bigcup_{a'\in\mathcal{A},b'\in\mathcal{B}}\mathcal{T}^N_{V'_{Y|X}}(Y|\mathbf{u}_{0m'},\mathbf{x}_{m',a',b'})\}, \tag{35}$$

because the events in the brackets are independent.

The first probability in (35) is different from zero iff $\mathbf{y}\in\mathcal{T}^N_{V_{Y|X}}(Y)$, then for $N$ large enough

$$\Pr\{\mathbf{y}\in\mathcal{T}^N_{V_{Y|X}}(Y|\mathbf{u}_{0m},\mathbf{x}_{m,a,b})\}=\frac{|\mathcal{T}^N_{V_{Y|X}}(U_0,X|\mathbf{y})|}{|\mathcal{T}^N(U_0,X)|}$$

$$\le(N+1)^{|\mathcal{X}|}\exp\{-NI_{V_{Y|X}}(Y\wedge U_0,X)\}$$

$$\le\exp\{-N[I_{V_{Y|X}}(Y\wedge U_0,X)-\delta/4]\}. \tag{36}$$

The second probability in (35) can be estimated as follows:

$$
\begin{aligned}
&\mathrm{P}r\{\mathbf{y} \in \bigcup_{a'\in\mathcal{A},b'\in\mathcal{B}} \mathcal{T}^N_{V'_{Y|X}}(Y|\mathbf{u}_{0m'},\mathbf{x}_{m',a',b'})\} \\
&\leq \mathrm{P}r\{\mathbf{y} \in \bigcup_{\mathbf{x}\in\mathcal{T}^N(X|\mathbf{u}_{0m'})} \mathcal{T}^N_{V'_{Y|X}}(Y|\mathbf{u}_{0m'},\mathbf{x})\} \\
&\leq \mathrm{P}r\{\mathbf{y} \in \mathcal{T}^N_{V'_{Y|X}}(Y|\mathbf{u}_{0m'})\} \\
&\leq \frac{|\mathcal{T}^N_{V'_{Y|X}}(U_0|\mathbf{y})|}{|\mathcal{T}^N_{Q_0}(U_0)|} \\
&\leq \exp\{-N[I_{V'_{Y|X}}(U_0\wedge Y)-\delta/4]\}. \qquad (37)
\end{aligned}
$$

For some $V'_{Y|X}\in\mathcal{V}_N(\mathcal{Y})$ from (30) we have

$$|\mathcal{M}_N|-1 \leq \exp\{N[I_{V'_{Y|X}}(U_0\wedge Y)+D(V'_{Y|X}\|W_{Y|X})-E_1-\delta]\}. \tag{38}$$

Thus by substituting (38) in (35) and from (36), (37) the conclusion is

$$
\begin{aligned}
&\mathbf{E}(|\mathcal{T}^N_{V_{Y|X}}(Y|\mathbf{u}_{0m},\mathbf{x}_{m,a,b})\bigcap\bigcup_{m'\neq m}\bigcup_{a'\in\mathcal{A},b'\in\mathcal{B}}\mathcal{T}^N_{V'_{Y|X}}(Y|\mathbf{u}_{0m'},\mathbf{x}_{m',a',b'})|) \\
&\leq \exp\{-N[I_{V_{Y|X}}(X\wedge Y)-H_{V_{Y|X}}(Y)-D(V'_{Y|X}\|W_{Y|X})+E_1-\delta/2]\}.
\end{aligned}
$$

Thus

$$
\begin{aligned}
&\mathbf{E}(|\mathcal{T}^N_{V_{Y|X}}(Y|\mathbf{u}_{0m},\mathbf{x}_{m,a,b})\bigcap\bigcup_{m'\neq m}\bigcup_{a'\in\mathcal{A},b'\in\mathcal{B}}\mathcal{T}^N_{V'_{Y|X}}(Y|\mathbf{u}_{0m'},\mathbf{x}_{m',a',b'})|) \\
&\times\exp\{-N[H_{V_{Y|X}}(Y|X)+D(V'_{Y|X}\|W_{Y|X})-E_1]\}\leq\exp\{-N\delta/2\}. \qquad (39)
\end{aligned}
$$

Then we estimate the second expectation in (34) as follows,

$$
\begin{aligned}
&\mathbf{E}(|\mathcal{T}^N_{V_{Y|X}}(Y|\mathbf{u}_{0m},\mathbf{x}_{m,a,b})\bigcap\bigcup_{(a',b')\neq(a,b)}\mathcal{T}^N_{V'_{Y|X}}(Y|\mathbf{u}_{0m},\mathbf{x}_{m,a',b'})|) \\
&\leq \sum_{(a',b')\neq(a,b)}\ \sum_{\mathbf{y}\in\mathcal{T}^N_{Y|X}(Y|\mathbf{u}_{0m})}\mathrm{P}r\{\mathbf{y}\in\mathcal{T}^N_{V_{Y|X}}(Y|\mathbf{u}_{0m},\mathbf{x}_{m,a,b})\} \\
&\times\mathrm{P}r\{\mathbf{y}\in\mathcal{T}^N_{V'_{Y|X}}(Y|\mathbf{u}_{0m},\mathbf{x}_{m,a',b'})\}. \qquad (40)
\end{aligned}
$$

Both probabilities in (40) can be estimated similarly. We estimate the second probability as follows

$$\mathrm{P}r\{\mathbf{y}\in\mathcal{T}^N_{V'_{Y|X}}(Y|\mathbf{u}_{0m},\mathbf{x}_{m,a',b'})\}=\frac{|\mathcal{T}^N_{V'_{Y|X}}(X|\mathbf{u}_{0m},\mathbf{y})|}{|\mathcal{T}^N(X)|}$$

$$\leq \exp\{-N[I_{V'_{Y|X}}(X\wedge Y|U_0)-\delta/8]\}. \tag{41}$$

By the same way, we can prove that the first probability can not exceed

$$\exp\{-N[I_{V_{Y|X}}(X\wedge Y|U_0)-\delta/8]\}. \tag{42}$$

Further for some $V'_{Y|X}\in\mathcal{V}_N(\mathcal{Y})$ from (32), (33) for $N$ large enough we have

$$A\times B\leq \exp\{N[I_{V'_{Y|X}}(X\wedge Y|U_0)+D(V'_{Y|X}\|W_{Y|X})-E_1-\delta/2]\}. \tag{43}$$

By substituting (41)-(43) in (40) we obtain that

$$\mathbf{E}(|\mathcal{T}^N_{V_{Y|X}}(Y|\mathbf{u}_{0m},\mathbf{x}_{m,a,b})\bigcap\bigcup_{(a',b')\neq(a,b)}\mathcal{T}^N_{V'_{Y|X}}(Y|\mathbf{u}_{0m},\mathbf{x}_{m,a',b'})|)$$

$$\leq \exp\{-N[I_{V_{Y|X}}(X\wedge Y|U_0)-H_{V_{Y|X}}(Y|U_0)-D(V'_{Y|X}\|W_{Y|X})+E_1+\delta/4]\}.$$

So

$$\mathbf{E}(|\mathcal{T}^N_{V_{Y|X}}(Y|\mathbf{u}_{0m},\mathbf{x}_{m,a,b})\bigcap\bigcup_{(a',b')\neq(a,b)}\mathcal{T}^N_{V'_{Y|X}}(Y|\mathbf{u}_{0m},\mathbf{x}_{m,a',b'})|)$$

$$\times\exp\{-N[H_{V_{Y|X}}(Y|X,U_0)-D(V'_{Y|X}\|W_{Y|X})-E_1]\}\leq\exp\{-N\delta/4\}. \tag{44}$$

To estimate the third expectation in (34) we observe that

$$\mathbf{E}(|\mathcal{T}^N_{V_{Z|X}}(Z|\mathbf{u}_{0m},\mathbf{x}_{m,a,b})\bigcap\bigcup_{m''\neq m}\mathcal{T}^N_{V'_{Z|X}}(Z|\mathbf{u}_{0m''},\mathbf{x}_{m'',a'',b''})|)$$

$$\leq(|\mathcal{M}_N|-1)\sum_{\mathbf{y}\in\mathcal{T}^N_{V_{Z|X}}(Z)}\mathrm{P}r\{\mathbf{z}\in\mathcal{T}^N_{V_{Z|X}}(Z|\mathbf{u}_{0m},\mathbf{x}_{m,a,b})\}$$

$$\times\mathrm{P}r\{\mathbf{z}\in\mathcal{T}^N_{V'_{Z|X}}(Z|\mathbf{u}_{0m''},\mathbf{x}_{m'',a'',b''})\}$$

$$\leq|\mathcal{T}^N_{V_{Z|X}}(Z)|(|\mathcal{M}_N|-1)\exp\{-N[I_{V_{Z|X}}(X\wedge Z)+I_{V'_{Z|X}}(U_0\wedge Z)-\delta/2]\}. \tag{45}$$

For some $V'_{Z|X}\in\mathcal{V}_N(\mathcal{Z})$ from (30) we have

$$|\mathcal{M}_N|-1\leq\exp\{N(I_{V'_{Z|X}}(U_0\wedge Z)+D(V'_{Z|X}\|W_{Z|X})-E_2-\delta)\}\}.$$

By substituting this term in (45) we obtain

$$\mathbf{E}(|\mathcal{T}^N_{V_{Z|X}}(Z|\mathbf{u}_{0m},\mathbf{x}_{m,a,b})\bigcap\bigcup_{m''\neq m}\mathcal{T}^N_{V'_{Z|X}}(Z|\mathbf{u}_{0m''},\mathbf{x}_{m'',a'',b''})|)$$

$$\leq\exp\{-N[I_{V_{Z|X}}(X\wedge Z)+H_{V_{Z|X}}(Z)+E_2+\delta/2]\},$$

thus

$$\mathbf{E}(|\mathcal{T}^N_{V_{Z|X}}(Z|\mathbf{u}_{0m},\mathbf{x}_{m,a,b})\bigcap\bigcup_{m''\neq m}\mathcal{T}^N_{V'_{Z|X}}(Z|\mathbf{u}_{0m''},\mathbf{x}_{m'',a'',b''})|)$$

$$\times\exp\{-N[H_{V_{Z|X}}(Z|X)+D(V'_{Z|X}\|W_{Z|X})-E_2]\}\leq\exp\{-N\delta/2\}. \tag{46}$$

So from (39), (44), (46) taking into account the fact that the number of all $V'_i$, $V_i$, $i=1,2$, does not exceed $(N+1)^{2|\mathcal{X}|(|\mathcal{Y}|+|\mathcal{Z}|)}$, for $N$ large enough we conclude that (34) is correct.

**Appendix 2. Proof of Proposition 1.** Let $E_3$ and $\delta$ be given such that $E_3 > \delta > 0$. Let the code $(f, g_2')$ of length $N$ be defined, $R_s$ be the rate of the code and average error probability satisfies

(47)
$$(|\mathcal{M}_N||\mathcal{L}_N|)^{-1} \sum_{m\in\mathcal{M}_N, l\in\mathcal{L}_N} \sum_{\mathbf{x}\in\mathcal{X}^N} f(\mathbf{x}|m,l) W^N_{Z|X}((g_2^{'-1}(j))^c|\mathbf{x}) \leq \exp\{-N(E_3-\delta)\}.$$

The number of messages $|\mathcal{M}_N||\mathcal{L}_N|$ can be presented as the sum of numbers of codewords of different types

$$|\mathcal{M}_N||\mathcal{L}_N| = \sum_{Q_0,P_0} |f(\mathcal{M}_N\times\mathcal{L}_N)\bigcap \bigcup_{\mathbf{u}_0\in\mathcal{T}^N_{Q_0}(U_0)} \mathcal{T}^N_{Q_0,P_0}(X|\mathbf{u}_0)|.$$

The number of all types $Q_0$, $P_0$ is less than $(N+1)^{|\mathcal{X}||\mathcal{U}_0|}$ then there exists a major type $Q_0^*$, $P_0^*$ such that

$$(N+1)^{|\mathcal{X}||\mathcal{U}_0|} |f(\mathcal{M}_N\times\mathcal{L}_N)\bigcap \bigcup_{\mathbf{u}_0\in\mathcal{T}^N_{Q_0^*}(U_0)} \mathcal{T}^N_{Q_0^*,P_0^*}(X|\mathbf{u}_0)| \geq |\mathcal{M}_N||\mathcal{L}_N|. \tag{48}$$

Now in the left-hand side of (47) we can consider only codewords of types $Q_0^*$, $P_0^*$ and the part of output vectors $\mathbf{z}$ of some conditional type $V_{Z|X}$,

$$\sum_{m,l} \sum_{\mathbf{u}_0\in\mathcal{T}^N_{Q_0^*}(U_0)} \sum_{\mathbf{x}\in\mathcal{T}^N_{Q_0^*,P_0^*}(X|\mathbf{u}_0)} f(\mathbf{x}|m,l) W^N_{Z|X}(\mathcal{T}^N_{Q_0^*,P_0^*,V_{Z|X}}(Z|\mathbf{u}_0) - g_2^{'-1}(j)|\mathbf{x})$$

$$\leq |\mathcal{M}_N||\mathcal{L}_N| \exp\{-N(E_3-\delta)\}.$$

For $\mathbf{z}\in\mathcal{T}^N_{Q_0^*,P_0^*,V_{Z|X}}(Z|\mathbf{u}_0)$ we obtain that

$$\sum_{m,l} \sum_{\mathbf{u}_0\in\mathcal{T}^N_{Q_0^*}(U_0)} \sum_{\mathbf{x}\in\mathcal{T}^N_{Q_0^*,P_0^*}(X|\mathbf{u}_0)} f(\mathbf{x}|m,l) W^N_{Z|X}(\mathbf{z}|\mathbf{x}) \times \Bigg\{ |\mathcal{T}^N_{Q_0^*,P_0^*,V_{Z|X}}(Z|\mathbf{u}_0)|$$

$$-|\mathcal{T}^N_{Q_0^*,P_0^*,V_{Z|X}}(Z|\mathbf{u}_0)\bigcap g_2^{'-1}(j)| \Bigg\} \leq |\mathcal{M}_N||\mathcal{L}_N| \exp\{-N(E_3-\delta)\},$$

from (12) for $\mathbf{x}\in\mathcal{T}^N_{Q_0^*,P_0^*}(X|\mathbf{u}_0)$ and $\mathbf{z}\in\mathcal{T}^N_{Q_0^*,P_0^*,V_{Z|X}}(Z|\mathbf{u}_0)$ we have

$$\sum_{m,l} \sum_{\mathbf{u}_0\in\mathcal{T}^N_{Q_0^*}(U_0)} \sum_{\mathbf{x}\in\mathcal{T}^N_{Q_0^*,P_0^*}(X|\mathbf{u}_0)} f(\mathbf{x}|m,l)$$

$$\exp\{-N[D(V_{Z|X}\|W_{Z|X}|Q_0^*,P_0^*) + H_{Q_0^*,P_0^*,V_{Z|X}}(Z|X)]\}$$

$$\times\Bigg\{ |\mathcal{T}^N_{Q_0^*,P_0^*,V_{Z|X}}(Z|\mathbf{u}_0)| - |\mathcal{T}^N_{Q_0^*,P_0^*,V_{Z|X}}(Z|\mathbf{u}_0)\bigcap g_2^{'-1}(j)| \Bigg\}$$

$$\leq |\mathcal{M}_N||\mathcal{L}_N| \exp\{-N(E_3-\delta)\}.$$

Then we can write

$$\sum_{m,l} \sum_{\mathbf{u}_0 \in \mathcal{T}^N_{Q_0^*}(U_0)} \sum_{\mathbf{x} \in \mathcal{T}^N_{Q_0^*,P_0^*}(X|\mathbf{u}_0)} f(\mathbf{x}|m,l)$$

$$\left\{ |\mathcal{T}^N_{Q_0^*,P_0^*,V_{Z|X}}(Z|\mathbf{u}_0)| - |\mathcal{T}^N_{Q_0^*,P_0^*,V_{Z|X}}(Z|\mathbf{u}_0) \bigcap g_2^{'-1}(j)| \right\}$$

$$\leq \frac{|\mathcal{M}_N||\mathcal{L}_N| \exp\{-N(E_3-\delta)\}}{\exp\{-N[D(V_{Z|X}\|W_{Z|X}|Q_0^*,P_0^*)+H_{Q_0^*,P_0^*,V_{Z|X}}(Z|X)]\}}.$$

So

$$\sum_{m,l} \sum_{\mathbf{u}_0 \in \mathcal{T}^N_{Q_0^*}(U_0)} \sum_{\mathbf{x} \in \mathcal{T}^N_{Q_0^*,P_0^*}(X|\mathbf{u}_0)} f(\mathbf{x}|m,l)|\mathcal{T}^N_{Q_0^*,P_0^*,V_{Z|X}}(Z|\mathbf{u}_0)|$$

$$-\frac{|\mathcal{M}_N||\mathcal{L}_N| \exp\{-N(E_3-\delta)\}}{\exp\{-N[D(V_{Z|X}\|W_{Z|X}|Q_0^*,P_0^*)+H_{Q_0^*,P_0^*,V_{Z|X}}(Z|X)]\}}$$

$$\leq \sum_{m,l} \sum_{\mathbf{u}_0 \in \mathcal{T}^N_{Q_0^*}(U_0)} \sum_{\mathbf{x} \in \mathcal{T}^N_{Q_0^*,P_0^*}(X|\mathbf{u}_0)} f(\mathbf{x}|m,l)|\mathcal{T}^N_{Q_0^*,P_0^*,V_{Z|X}}(Z|\mathbf{u}_0) \bigcap g_2^{'-1}(j)|.$$

Then we have

$$\sum_{m,l} \sum_{\mathbf{u}_0 \in \mathcal{T}^N_{Q_0^*}(U_0)} \sum_{\mathbf{x} \in \mathcal{T}^N_{Q_0^*,P_0^*}(X|\mathbf{u}_0)} f(\mathbf{x}|m,l)(N+1)^{-|\mathcal{X}||\mathcal{U}_0||\mathcal{Z}|}$$

$$\exp\{NH_{Q_0^*,P_0^*,V_{Z|X}}(Z|U_0)\}$$

$$-|\mathcal{M}_N||\mathcal{L}_N| \exp\{N[D(V_{Z|X}\|W_{Z|X}|Q_0^*,P_0^*)+H_{Q_0^*,P_0^*,V_{Z|X}}(Z|X)-E_3+\delta]\}$$

$$\leq \sum_{m,l} \sum_{\mathbf{u}_0 \in \mathcal{T}^N_{Q_0^*}(U_0)} \sum_{\mathbf{x} \in \mathcal{T}^N_{Q_0^*,P_0^*}(X|\mathbf{u}_0)} f(\mathbf{x}|m,l)|\mathcal{T}^N_{Q_0^*,P_0^*,V_{Z|X}}(Z|\mathbf{u}_0) \bigcap g_2^{'-1}(j)|,$$

since $(N+1)^{-|\mathcal{X}||\mathcal{U}_0||\mathcal{Z}|} \exp\{NH_{Q_0^*,P_0^*,V_{Z|X}}(Z|U_0)\}$ is independent from the summation indexes, we have

$$(N+1)^{-|\mathcal{X}||\mathcal{U}_0||\mathcal{Z}|} \exp\{NH_{Q_0^*,P_0^*,V_{Z|X}}(Z|U_0)\} \sum_{m,l} \sum_{\mathbf{u}_0 \in \mathcal{T}^N_{Q_0^*}(U_0)} \sum_{\mathbf{x} \in \mathcal{T}^N_{Q_0^*,P_0^*}(X|\mathbf{u}_0)} f(\mathbf{x}|m,l)$$

$$-|\mathcal{M}_N||\mathcal{L}_N| \exp\{N[D(V_{Z|X}\|W_{Z|X}|Q_0^*,P_0^*)+H_{Q_0^*,P_0^*,V_{Z|X}}(Z|X)-E_3+\delta]\}$$

$$\leq \sum_{m,l} \sum_{\mathbf{u}_0 \in \mathcal{T}^N_{Q_0^*}(U_0)} \sum_{\mathbf{x} \in \mathcal{T}^N_{Q_0^*,P_0^*}(X|\mathbf{u}_0)} f(\mathbf{x}|m,l) |\mathcal{T}^N_{Q_0^*,P_0^*,V_{Z|X}}(Z|\mathbf{u}_0) \bigcap g_2^{'-1}(j)|.$$

Since

$$\sum_{m,l} \sum_{\mathbf{u}_0 \in \mathcal{T}^N_{Q_0^*}(U_0)} \sum_{\mathbf{x} \in \mathcal{T}^N_{Q_0^*,P_0^*}(X|\mathbf{u}_0)} f(\mathbf{x}|m,l) = |f(\mathcal{M}_N \times \mathcal{L}_N) \bigcap \bigcup_{\mathbf{u}_0 \in \mathcal{T}^N_{Q_0^*}(U_0)} \mathcal{T}^N_{Q_0^*,P_0^*}(X|\mathbf{u}_0)|,$$

we have

$$|f(\mathcal{M}_N \times \mathcal{L}_N) \bigcap \bigcup_{\mathbf{u}_0 \in \mathcal{T}^N_{Q_0^*}(U_0)} \mathcal{T}^N_{Q_0^*,P_0^*}(X|\mathbf{u}_0)|(N+1)^{-|\mathcal{X}||\mathcal{U}_0||\mathcal{Z}|}$$

$$\exp\{NH_{Q_0^*,P_0^*,V_{Z|X}}(Z|U_0)\}$$

$$-|\mathcal{M}_N||\mathcal{L}_N| \exp\{N[D(V_{Z|X}\|W_{Z|X}|Q_0^*,P_0^*) + H_{Q_0^*,P_0^*,V_{Z|X}}(Z|X) - E_3 + \delta]\}$$

$$\leq \sum_{m,l} \sum_{\mathbf{u}_0 \in \mathcal{T}^N_{Q_0^*}(U_0)} \sum_{\mathbf{x} \in \mathcal{T}^N_{Q_0^*,P_0^*}(X|\mathbf{u}_0)} f(\mathbf{x}|m,l) |\mathcal{T}^N_{Q_0^*,P_0^*,V_{Z|X}}(Z|\mathbf{u}_0) \bigcap g_2^{'-1}(j)|. \tag{49}$$

From the definition of decoding function $g_2'$ it follows that the sets $g_2^{'-1}(j)$ are disjoint, therefore

$$\sum_{m,l} \sum_{\mathbf{u}_0 \in \mathcal{T}^N_{Q_0^*}(U_0)} \sum_{\mathbf{x} \in \mathcal{T}^N_{Q_0^*,P_0^*}(X|\mathbf{u}_0)} f(\mathbf{x}|m,l) |\mathcal{T}^N_{Q_0^*,P_0^*,V_{Z|X}}(Z|\mathbf{u}_0) \bigcap g_2^{'-1}(j)|$$

$$\leq \sum_{m,a} \sum_{j} \sum_{\mathbf{u}_0 \in \mathcal{T}^N_{Q_0^*}(U_0)} \sum_{\mathbf{x} \in \mathcal{T}^N_{Q_0^*,P_0^*}(X|\mathbf{u}_0)} f(\mathbf{x}|m,l) |\mathcal{T}^N_{Q_0^*,P_0^*,V_{Z|X}}(Z|\mathbf{u}_0) \bigcap g_2^{'-1}(j)|$$

$$\leq \sum_{m,a} \sum_{\mathbf{u}_0 \in \mathcal{T}^N_{Q_0^*}(U_0)} \sum_{\mathbf{x} \in \mathcal{T}^N_{Q_0^*,P_0^*}(X|\mathbf{u}_0)} f(\mathbf{x}|m,l) |\mathcal{T}^N_{Q_0^*,P_0^*,V_{Z|X}}(Z|\mathbf{u}_0) \bigcap \mathcal{Z}^N|$$

$$\leq \exp\{NH_{Q_0^*,P_0^*,V_{Z|X}}(Z|U_0)\} \sum_{m,a} \sum_{\mathbf{u}_0 \in \mathcal{T}^N_{Q_0^*}(U_0)} \sum_{\mathbf{x} \in \mathcal{T}^N_{Q_0^*,P_0^*}(X|\mathbf{u}_0)} f(\mathbf{x}|m,l)$$

$$\leq |\mathcal{M}_N| A \exp\{NH_{Q_0^*,P_0^* V_{Z|X}}(Z|U_0)\}, \tag{50}$$

where the last inequality is concluded from

$$\sum_{\mathbf{u}_0 \in \mathcal{T}^N_{Q_0^*}(U_0)} \sum_{\mathbf{x} \in \mathcal{T}^N_{Q_0^*,P_0^*}(X|\mathbf{u}_0)} f(\mathbf{x}|m,l) \leq 1$$

Taking into account (48) and substituting (50) in (49) we come to

$$|\mathcal{M}_N||\mathcal{L}_N|(N+1)^{-|\mathcal{X}||\mathcal{U}_0|(|\mathcal{Z}|+1)}\exp\{NH_{Q_0^*,P_0^*,V_{Z|X}}(Z|U_0)\}-$$

$$-|\mathcal{M}_N||\mathcal{L}_N|\exp\{N[D(V_{Z|X}\|W_{Z|X}|Q_0^*,P_0^*)+H_{Q_0^*,P_0^*,V_{Z|X}}(Z|X)-E_3+\delta]\}$$

$$\leq |\mathcal{M}_N|A\exp\{NH_{Q_0^*,P_0^*V_{Z|X}}(Z|U_0)\}.$$

From Markov chain $U_0\to X\to Z$ we conclude that

$$H_{Q_0^*,P_0^*,V_{Z|X}}(Z|U_0)\geq H_{Q_0^*,P_0^*,V_{Z|X}}(Z|X),$$

therefore

$$J\leq \frac{\exp\{NI_{Q_0^*,P_0^*,V_{Z|X}}(X\wedge Z|U_0)\}}{(N+1)^{-|\mathcal{X}||\mathcal{U}_0|(|\mathcal{Z}|+1)}-\exp\{N(D(V_{Z|X}\|W_{Z|X}|Q_0^*,P_0^*)-E_3+\delta)}. \tag{51}$$

For $N$ large enough $(N+1)^{-|\mathcal{X}||\mathcal{U}_0|(|\mathcal{Z}|+1)}-\exp\{N(D(V_{Z|X}\|W_{Z|X}|Q_0^*,P_0^*)-E_3+\delta)\}$ is positive if the following inequality holds

$$D(V_{Z|X}\|W_{Z|X}|Q_0^*,P_0^*)\leq E_3-\delta.$$

Thus from (51) and the definition of $R_s$ we conclude that

$$0\leq R_s\leq \max_{Q_0,P_0}\min_{V_{Z|X}:D(V_{Z|X}\|W_{Z|X}|Q_0,P_0)\leq E_3} I_{Q_0,P_0,V_{Z|X}}(X\wedge Z|U_0).$$

The proof is complete.

**Appendix 3. Proof of Lemma 4.** First we prove that error probabilities of the code decrease exponentially with reliabilities $E_1$, $E_2$. Decoder $g_1$ makes an error if the pair of messages $m$, $l$ is transmitted but there exists $(m',\, l')\neq(m,\, l)$ such that for some $V'_{Y|X}$

$$\mathbf{y}\in\mathcal{T}^N_{V_{Y|X}}(Y|\mathbf{u}_{0m},\,\mathbf{x}_{m,a,b})\bigcap\mathcal{T}^N_{V'_{Y|X}}(Y|\mathbf{u}_{0m'},\,\mathbf{x}_{m',a',b'}),$$

and

$$D(V'_{Y|X}\|W_{Y|X})\leq D(V_{Y|X}\|W_{Y|X}). \tag{52}$$

Decoder $g_2$ makes an error if the message $m$ is transmitted but there exists $m''\neq m$ such that for some $V'_{Z|X}$, $a$, $a''$, $b$, $b''$

$$\mathbf{z}\in\mathcal{T}^N_{V_{Z|X}}(Z|\mathbf{u}_{0m},\,\mathbf{x}_{m,a,b})\bigcap\mathcal{T}^N_{V'_{Z|X}}(Z|\mathbf{u}_{0m''},\,\mathbf{x}_{m'',a'',b''}),$$

and

$$D(V'_{Z|X}\|W_{Z|X})\leq D(V_{Z|X}\|W_{Z|X}). \tag{53}$$

We consider the following sets $\mathcal{B}_1(V_{Y|X}, V'_{Y|X})$, $\mathcal{B}_2(V_{Y|X}, V'_{Y|X})$, $\mathcal{B}_3(V_{Z|X}, V'_{Z|X})$ of decoding errors at receiver 1 and receiver 2. $\mathcal{B}_1(V_{Y|X}, V'_{Y|X})$ is defined as the set of vectors $\mathbf{y}$ which can lead to error at receiver 1:

(54)
$$\mathcal{B}_1(V_{Y|X}, V'_{Y|X}) \triangleq \mathcal{T}^N_{V_{Y|X}}(Y|\mathbf{u}_{0m}, \mathbf{x}_{m,a,b}) \bigcap \bigcup_{m'\neq m} \bigcup_{a'\in\mathcal{A}, b'\in\mathcal{B}} \mathcal{T}^N_{V'_{Y|X}}(Y|\mathbf{u}_{0m'}, \mathbf{x}_{m',a',b'}).$$

$\mathcal{B}_2(V_{Y|X}, V'_{Y|X})$ includes vectors $\mathbf{y}$ at receiver 1 which can lead to error:

$$(55)\quad \mathcal{B}_2(V_{Y|X}, V'_{Y|X}) \triangleq \mathcal{T}^N_{V_{Y|X}}(Y|\mathbf{u}_{0m}, \mathbf{x}_{m,a,b}) \bigcap \bigcup_{(a',b')\neq(a,b)} \mathcal{T}^N_{V'_{Y|X}}(Y|\mathbf{u}_{0m}, \mathbf{x}_{m,a',b'}).$$

$\mathcal{B}_3(V_{Z|X}, V'_{Z|X})$ contains all vectors $\mathbf{z}$ at receiver 2 which can lead to error:

$$(56)\quad \mathcal{B}_3(V_{Z|X}, V'_{Z|X}) \triangleq \mathcal{T}^N_{V_{Z|X}}(Z|\mathbf{u}_{0m}, \mathbf{x}_{m,a,b}) \bigcap \bigcup_{m''\neq m} \mathcal{T}^N_{V'_{Z|X}}(Z|\mathbf{u}_{0m''}, \mathbf{x}_{m'',a'',b''}).$$

Let us define the following sets of distributions:

$$\mathcal{D}'_1(E_1) = \{V_{Y|X}, V'_{Y|X} \in \mathcal{V}_N(\mathcal{Y}) : \; D(V'_{Y|X}\|W_{Y|X}) \le D(V_{Y|X}\|W_{Y|X})\},$$

$$\mathcal{D}'_2(E_2) = \{V_{Z|X}, V'_{Z|X} \in \mathcal{V}_N(\mathcal{Z}) : \; D(V'_{Z|X}\|W_{Z|X}) \le D(V_{Z|X}\|W_{Z|X})\}.$$

With this notation we upper estimate

$$e_1(f, g_1, W_{Y|X}) =^{(a)} \max_{m\in\mathcal{M}_N, l\in\mathcal{L}_N} \sum_{\mathbf{x}_{m,a,b}} f(\mathbf{x}_{m,a,b}|m,l)$$

$$\times W^N_{Y|X}(\bigcup_{V_{Y|X}\in\mathcal{V}_N(\mathcal{Y})} (g_1^{-1}(m,l))^c \bigcap \mathcal{T}^N_{V_{Y|X}}(Y|\mathbf{u}_{0m}, \mathbf{x}_{m,a,b})|\mathbf{x}_{m,a,b})$$

$$\le \max_{m\in\mathcal{M}_N, l\in\mathcal{L}_N} \sum_{\mathbf{x}_{m,a,b}} f(\mathbf{x}_{m,a,b}|m,l)$$

$$\times W^N_{Y|X}(\bigcup_{V_{Y|X}, V'_{Y|X}\in\mathcal{D}'_1(E_1)} \mathcal{B}_1(V_{Y|X}, V'_{Y|X}) \bigcup \mathcal{B}_2(V_{Y|X}, V'_{Y|X})|\mathbf{x}_{m,a,b})$$

$$\le^{(b)} \max_{m\in\mathcal{M}_N, l\in\mathcal{L}_N} \sum_{\mathbf{x}_{m,a,b}} f(\mathbf{x}_{m,a,b}|m,l) W^N_{Y|X}((\mathbf{y}|\mathbf{x}_{m,a,b})$$

$$\times |\bigcup_{V_{Y|X}, V'_{Y|X}\in\mathcal{D}'_1(E_1)} \mathcal{B}_1(V_{Y|X}, V'_{Y|X}) \bigcup \mathcal{B}_2(V_{Y|X}, V'_{Y|X})|$$

$$\le^{(c)} \max_{m\in\mathcal{M}_N, l\in\mathcal{L}_N} \sum_{V_{Y|X}, V'_{Y|X}\in\mathcal{D}'_1(E_1)} \sum_{\mathbf{x}_{m,a,b}} f(\mathbf{x}_{m,a,b}|m,l)$$

$$\times W^N_{Y|X}((\mathbf{y}|\mathbf{x}_{m,a,b}) \times [|\mathcal{B}_1(V_{Y|X},\, V'_{Y|X})| + |\mathcal{B}_2(V_{Y|X},\, V'_{Y|X})|]$$

$$\leq^{(d)} \sum_{V_{Y|X}, V'_{Y|X} \in \mathcal{D}'_1(E_1)} \exp\{-N[D(V_{Y|X}\|W_{Y|X}) + H_{V_{Y|X}}(Y|X)]\}\}$$

$$\times \max_{m\in\mathcal{M}_N, l\in\mathcal{L}_N} \sum_{\mathbf{x}_{m,a,b}} f(\mathbf{x}_{m,a,b}|m,l) \times [|\mathcal{B}_1(V_{Y|X},\, V'_{Y|X})| + |\mathcal{B}_2(V_{Y|X},\, V'_{Y|X})|\,], \tag{57}$$

where (a) holds because for every codeword $\mathbf{x}_{m,a,b}$

$$\mathcal{Y}^N = \bigcup_{V_{Y|X}\in\mathcal{V}_N(\mathcal{Y})} \mathcal{T}^N_{V_{Y|X}}(Y|\mathbf{u}_{0m}, \mathbf{x}_{m,a,b});$$

(b) follows from the definition of sets for decoding error (53) and (54); taking into account that $W_{Y|X}(\mathbf{y}|\mathbf{x})$ is constant for fixed $Q_0$, $P_0$, $V_{Y|X}$, we conclude (c); and (d) is consequence of (15).

Similarly error probability of receiver 2 can be upper bounded as follows

$$e_2(f, g_2, W_{Z|X}) \leq \max_{m\in\mathcal{M}_N, l\in\mathcal{L}_N} \sum_{V_{Z|X}, V'_{Z|X}\in\mathcal{D}'_2(E_2)} \exp\{-N[D(V_{Z|X}\|W_{Z|X})$$

$$+H_{V_{Z|X}}(Z|X)]\} \times \sum_{\mathbf{x}_{m,a,b}} f(\mathbf{x}_{m,a,b}|m,l) \times |\mathcal{B}_3(V_{Z|X},\, V'_{Z|X})|. \tag{58}$$

We prove the following inequalities for every $m \in \mathcal{M}_N$, $l \in \mathcal{L}_N$, every conditional types $V_{Y|X}$, $V'_{Y|X}$, $V_{Z|X}$, $V'_{Z|X}$ and $N$ large enough:

(59)
$$|\mathcal{B}_i(V_{Y|X},\, V'_{Y|X})| \leq \exp\{NH_{V_{Y|X}}(Y|X)\}\exp\{-N|E_1 - D(V'_{Y|X}\|W_{Y|X})|^+\},\ i = 1,\, 2,$$

$$|\mathcal{B}_3(V_{Z|X},\, V'_{Z|X})| \leq \exp\{NH_{V_{Z|X}}(Z|X)\}\exp\{-N|E_2 - D(V'_{Z|X}\|W_{Z|X})|^+\}. \tag{60}$$

Let us note that the collection of vectors $\{(\mathbf{u}_{0m},\, \mathbf{x}_{m,a,b})\}_{m\in\mathcal{M}_N, a\in\mathcal{A}, b\in\mathcal{B}}$ satisfy (59), (60) for each $V_{Y|X}$, $V'_{Y|X}$, $V_{Z|X}$, $V'_{Z|X}$, then $(\mathbf{u}_{0m'}, \mathbf{x}_{m',a',b'}) \neq (\mathbf{u}_{0m}, \mathbf{x}_{m,a,b})$ for $(m', a', b') \neq (m, a, b)$. To prove that, it is enough to choose $V'_{Y|X} = V_{Y|X}$, $V'_{Z|X} = V_{Z|X}$ and $D(V'_{Y|X}\|W_{Y|X}) \leq E_1$, $D(V'_{Z|X}\|W_{Z|X}) \leq E_2$.

If $V'_{Y|X}$ and $V'_{Z|X}$ are such that $D(V'_{Y|X}\|W_{Y|X}) \geq E_1$ and $D(V'_{Z|X}\|W_{Z|X}) \geq E_2$, then

$$\exp\{-N|E_1 - D(V'_{Y|X}\|W_{Y|X})|^+\} = 1,\ \exp\{-N|E_2 - D(V'_{Z|X}\|W_{Z|X})|^+\} = 1$$

and (59), (60) are valid for any $|\mathcal{M}_N|, A$ and $B$. It remains to prove inequalities (59), (60) for $V'_{Y|X}$ and $V'_{Z|X}$ such that $D(V'_{Y|X}\|W_{Y|X}) \leq E_1$, $D(V'_{Z|X}\|W_{Z|X}) \leq E_2$. To this end, it is sufficient to prove the following inequality for the code generated and

$N$ large enough

$$\begin{aligned}
&\sum_{V_{Y|X}}\ \sum_{V'_{Y|X}\in\mathcal{D}_1(E_1)}\ \sum_{i=1,\,2}\mathbf{E}(|\mathcal{B}_i(V_{Y|X},V'_{Y|X})|)\\
&\times\exp\{-N[H_{V_{Y|X}}(Y|X)-E_1+D(V'_{Y|X}\|W_{Y|X})]\}\\
&+\sum_{V_{Z|X}}\ \sum_{V'_{Z|X}\in\mathcal{D}_2(E_2)}\mathbf{E}(|\mathcal{B}_3(V_{Z|X},V'_{Z|X})|)\\
&\times\exp\{-N[H_{V_{Z|X}}(Z|X)-E_2+D(V'_{Z|X}\|W_{Z|X})]\}\leq 1. \qquad (61)
\end{aligned}$$

According to Lemma 3 inequality (61) is correct.

Therefore, using (57), (59) the error probability of receiver 1 can be estimated as follows

$$\begin{aligned}
&e_1(f,\,g_1,\,W_{Y|X})\\
&\leq\max_{m\in\mathcal{M}_N,l\in\mathcal{L}_N}\ \sum_{V_{Y|X},V'_{Y|X}\in\mathcal{D}_1(E_1)}\exp\{-N[D(V_{Y|X}\|W_{Y|X})+H_{V_{Y|X}}(Y|X)]\}\\
&\times 2\exp\{-N[-H_{V_{Y|X}}(Y|X)-D(V'_{Y|X}\|W_{Y|X})+E_1]\}\times\sum_{\mathbf{x}_{m,a,b}}f(\mathbf{x}_{m,a,b}|m,l)\\
&\leq\sum_{V_{Y|X},V'_{Y|X}\in\mathcal{D}_1(E_1)}\exp\{-NE_1\}.
\end{aligned}$$

So because the number of types $V'_{Y|X}$, $V_{Y|X}\in\mathcal{D}_1(E_1)$ does not exceed $(N+1)^{2|\mathcal{X}||\mathcal{Y}|}$, for $N$ large enough we obtain

$$e_1(f,\,g_1,\,W_{Y|X})\leq\exp\{-N(E_1-\epsilon)\},\ \epsilon>0. \qquad (62)$$

Hence the error probability of receiver 1 decreases exponentially while $N$ increases. Using (57), (59) the error probability for receiver 2 can be estimated similarly,

$$e_2(f,\,g_2,\,W_{Z|X})\leq\exp\{-N(E_2-\epsilon)\},\ \epsilon>0. \qquad (63)$$

It remains to prove that secrecy leakage is at most $\min\limits_{V_{Z|X}:D(V_{Z|X}\|W_{Z|X})\leq E_3}I_{V_{Z|X}}(X\wedge Z|U_0)$ per channel use at receiver 2, which we proved in Proposition 1. Therefore, proof of Lemma 4 is completed.

**Acknowledgement.** The authors are deeply grateful to Editor, Professor Sergio Verdú and to the reviewer for their helpful comments and suggestions.

## REFERENCES

[1] T. M. Cover, *Broadcast channels*, IEEE Trans. Inform. Theory, IT-18:1(1972), pp. 2-14.

[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. Inform. Theory, IT-24:3(1978), pp. 339-348.

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

[5] R. G. Gallager, *Information Theory and Reliable Communication*, New York, Wiley, 1968.

[6] S. I. Gelfand and M. S. Pinsker, *Capacity of broadcast channel with one deterministic component*, Probl. Pered. Inform., 16:1(1980), pp. 17-25.

[7] 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.

[8] E. A. Haroutunian, *Estimates of the error exponent for the semi-continuous memoryless channel*, (in Russian), Probl. Pered. Inform., 4(1968), pp. 37-48.

[9] E. A. Haroutunian, *Combinatorial method of construction of the upper bound for E-capacity*, (in Russian), Mezhvuz. Sbornic Nouchnikh Trudov, Matematika, Yerevan, vol. 1, pp. 213-220, 1982.

[10] E. A. Haroutunian and 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. Inform. Theory, Tashkent, USSR, vol. 1, pp. 19-21, 1984.

[11] E. A. Haroutunian, *On Bounds for E-Capacity of DMC*, IEEE Trans. Inform. Theory, IT-53:11(2007), pp. 4210-4220.

[12] 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.

[13] 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.

[14] M. E. Haroutunian, *Random coding bound for E-capacity region of the broadcast channel*, Mathematical Problems of Computer Science, 21(2000), pp. 50-60.

[15] M. Hayashi and R. Matsumoto, *Universally attainable error and information exponents for the broadcast channels with confidential messages*, Forty-Ninth Annual Allerton Conference Allerton House, UIUC, Illinois, USA, pp. 439 - 444, 2011.

[16] J. Körner and K. Marton, *General broadcast channels with degraded message sets*, IEEE Trans. Inform. Theory, IT-23:1(1977), pp. 60-64.

[17] J. Körner and A. Sgarro, *Universally attainable error exponents for broadcast channels with degraded message sets*, IEEE Trans. Inform. Theory, 26:6(1980), pp. 670-679.

[18] 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.

[19] R. Liu, I. Maric, P. Spasojevic, and R. Yates, *Discrete memoryless interference and broadcast channels with confidential messages: secrecy rate regions*, IEEE Trans. Inform. Theory, 54:6(2008), pp. 2493-2507.

[20] K. Marton, *A coding theorem for the discrete memoryless broadcast channel*, IEEE Trans. Inform. Theory, IT-25:3(1979), pp. 306-311.

[21] C. E. Shannon, *A mathematical theory of communication*, Bell Syst. Tech. J., 27:3(1948), pp. 379-423.

[22] E. C. Van der Meulen, *Random coding theorems for the general discrete memoryless broadcast channel*, IEEE Trans. Inform. Theory, 16:1(1980), pp. 17-25.

[23] A. D. Wyner, *The wire-tap channel*, Bell Syst. Tech. J., 54:8(1975), pp. 1355-1387.

[24] J. Xu, Y. Cao, and B. Chen, *Capacity bound for broadcast channels with confidential messages*, IEEE Trans. Inform. Theory, 55:10(2009), pp. 4529-4542.