Mathematical Problems of Computer Science 37, 39–44, 2012.

# Sphere Packing Bound for $E$-capacity of Secrecy Leakage of the Broadcast Channel With Confidential Messages

Nasrin Afshar

Institute for Informatics and Automation Problems of NAS of RA

**Abstract**

The discrete memoryless broadcast channel with confidential messages (BCC) involves two discrete memoryless channels with two sources and one encoder. A common message must be transmitted to two receivers and a private message to the intended receiver, while keeping the other receiver as ignorant of it as possible. Secrecy leakage rate is the rate of information available to the unintended receiver about the private message. Upper bound for $E$-capacity of secrecy leakage of the BCC is derived.

Key words: Broadcast channel with confidential messages, $E$-capacity, error probability exponent, method of types, secrecy leakage rate, sphere packing bound.

## Introduction

e broadcast channel with confidential messages (BCC) was first investigated by Csiszár l Körner [1]. The model of BCC is depicted in Fig. 1. It is assumed that a common ssage must be transmitted to two receivers and a private message to the intended receiver, le keeping the private message secret from the other receiver. The capacity region of the C was obtained in [1].

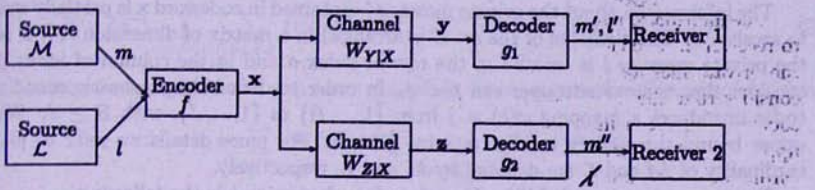


Figure 1. The model of BCC with two receivers.

his paper, we study the rate of the maximal available information which can be obtained an unintended receiver about the private message: we call it secrecy leakage rate. We find upper bound for $E$-capacity, which is the secrecy leakage rate of the unintended receiver in endence on his error probability exponent $E$. This result generalizes the sphere packing nd for $E$-capacity of DMC found by E. Haroutunian in [2] (see also [3]-[5]).

## 2. Preliminaries and Result Formulation

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

The discrete memoryless BCC has an input alphabet $\mathcal{X}$ and output alphabets $\mathcal{Y}$ and $\mathcal{Z}$, correspondingly, on the first and second receivers. The 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 of length $N$.

We introduce an additional finite set $\mathcal{U}_0$. RVs $U_0$, $X$, $Y$ and $Z$ take values in $\mathcal{U}_0$, $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$, correspondingly.

The memoryless broadcast channel is defined by the conditional transition PDs,

$$W_{Y|X} = \{W_{Y|X}(y|x),\ x \in \mathcal{X},\ y \in \mathcal{Y}\},\quad W_{Z|X} = \{W_{Z|X}(z|x),\ x \in \mathcal{X},\ z \in \mathcal{Z}\},$$

and by products for $N$ uses of channel

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

Message $m \in \mathcal{M}$ should be transmitted to both receivers, and the message $l \in \mathcal{L}$ should be sent to receiver 1 ensuring to be kept as secret as possible from the other receiver.

We consider a code $(f, g_2')$, where $f$ is an encoder and $g_2'$ is a decoder which receiver 2 applies to try to determine the private, secret message $l$. A code $(f, g_2')$ is characterized by the coding rate $R_s$.

To increase secrecy the stochastic encoding is applied [1]. The *stochastic encoder* $f$ with the block length $N$ is specified by conditional probabilities $f(\mathbf{x}|m, l)$, where $\mathbf{x} \in \mathcal{X}^N$, $m \in \mathcal{M}$, $l \in \mathcal{L}$, and $\sum_{\mathbf{x} \in \mathcal{X}^N} f(\mathbf{x}|m, l) = 1$.

The information about the private message $l$ contained in codeword $\mathbf{x}$ is partially available to receiver 2. The elements of the set $\mathcal{L}$ is arranged in a matrix of dimension $A \times J$ so that the private message $l$ is located in the row of index $a$ and in the column of index $j$. We consider that the eavesdropper can find $j$. In order to define the stochastic encoding the coder introduces a mapping $\varphi(b) = j$ from $\{1, ..., B\}$ to $\{1, ..., J\}$, with $B \geq J$. We shall upper bound the secrecy leakage rate by $\frac{1}{N} \log B$. For more details we refer to [6]. The cardinality of $\mathcal{M}$ and $\mathcal{L}$ are denoted by $M$ and $L$, respectively.

The average error probability at receiver 2 to determine $b$ is the following

$$\overline{e}_2(f, g_2', W_{Z|X}) \triangleq (M \times L)^{-1} \sum_{m \in \mathcal{M}, l \in \mathcal{L}} \sum_{\mathbf{x} \in \mathcal{X}^N} f(\mathbf{x}|m, l) W^N_{Z|X}((g_2'^{-1}(b))^c|\mathbf{x}), m, l). \tag{1}$$

The $E$-capacity $\overline{C}(E)$ of secrecy leakage is the rate $R_s$ of optimal code $(f, g_2')$ with the given exponent $E$ of average error probability.

Let $Q_0 = \{Q_0(u_0),\ u_0 \in \mathcal{U}_0\}$ be PD of RV $U_0$. We use conditional PD $P_0 = \{P(x|u_0),\ x \in \mathcal{X},\ u_0 \in \mathcal{U}_0$. Let $V_{Y|X} = \{V_{Y|X}(y|x),\ x \in \mathcal{X},\ y \in \mathcal{Y}\}$, and $V_{Z|X} = \{V_{Z|X}(z|x),\ x \in \mathcal{X},\ z \in \mathcal{Z}\}$ be some conditional PDs.

We assume that $U_0 \to X \to Y$ and $U_0 \to X \to Z$ form Markov chains.

For the given $E > 0$ consider the following functions

$$R_s^{sp}(E, Q_0, P_0) \triangleq \min_{V_{\mathcal{Z}|\mathcal{X}}: D(V_{\mathcal{Z}|\mathcal{X}} \| W_{\mathcal{Z}|\mathcal{X}} | Q_0, P_0) \le E} I_{Q_0, P_0, V_{\mathcal{Z}|\mathcal{X}}}(X \wedge Z|U_0),$$

$$R_s^{sp}(E) \triangleq \max_{Q_0, P_0} R_s^{sp}(E, Q_0, P_0).$$

The purpose of the paper is to establish an upper bound for $E$-capacity of secrecy leakage.

**Theorem:** For all $E > 0$,

$$\overline{C}(E) \le R_s^{sp}(E).$$

## Proof of the Theorem

Let $Q_0'$ be a type of vectors in $\mathcal{U}_0^N$ and $P_0'$ be a conditional type of $\mathbf{x} \in \mathcal{X}^N$ for the given $\mathbf{u}_0$. The codebook is generated by the following steps.

First, $M$ vectors $\mathbf{u}_{0m}$ are chosen from $\mathcal{T}_{Q_0'}^N(U_0)$. Then for each $\mathbf{u}_{0m}$, $A \times B$ codewords $\mathbf{x}_{m,a,b}$ are drawn from $P_0'$-shell $\mathcal{T}_{Q_0', P_0'}^N(X|\mathbf{u}_{0m})$. The codewords are arranged in $M$ classes and every class contains $A \times B$ codewords, where

$$B = \exp\{N \min_{V_{\mathcal{Z}|\mathcal{X}}: D(V_{\mathcal{Z}|\mathcal{X}} \| W_{\mathcal{Z}|\mathcal{X}} | Q_0', P_0') \le E} (I_{Q_0', P_0', V_{\mathcal{Z}|\mathcal{X}}}(X \wedge Z|U_0) - \delta)\},$$

and $A$ is such that $\frac{1}{N}\log A = \frac{1}{N}\log L - \frac{1}{N}\log J$. We use the sets $\mathcal{A} \triangleq \{1, ...A\}$, $\mathcal{B} \triangleq \{1, ...B\}$ and $\mathcal{J} \triangleq \{1, ..., J\}$.

To encode the message $l = (a, j)$ a pair $(a, b_j)$ must be chosen. To this end, a function $\varphi$ is defined to partition every class $m$ of codewords into $L$ subsets of nearly equal size. Then a pair $(a, b_j)$ is chosen randomly from $\{(a, b) : b \in \varphi^{-1}(j)\}$. The encoder of pair of messages $(m, l)$ is $f : (m, l) \to \{\mathbf{x}_{m,a,b_j}\}_{m \in \mathcal{M}, a \in \mathcal{A}, j \in \mathcal{J}}$.

Let $E$ and $\delta$ be given such that $E > \delta > 0$. Let the code $(f, g_2')$ of length $N$ be defined, $\mathcal{R}_s$ be the rate of the code and average error probability decreases exponentially

$$(M \times L)^{-1} \sum_{m \in \mathcal{M}, l \in \mathcal{L}} \sum_{\mathbf{x} \in \mathcal{X}^N} f(\mathbf{x}|m, l) W_{\mathcal{Z}|\mathcal{X}}^N((g_2'^{-1}(b))^c|\mathbf{x}) \le \exp\{-N(E - \delta)\}. \quad (2)$$

The number of messages $M \times L$ can be presented as the numbers of codewords of different types

$$M \times L = \sum_{Q_0', P_0'} |f(\mathcal{M} \times \mathcal{L}) \bigcap \bigcup_{\mathbf{u}_0 \in \mathcal{T}_{Q_0'}^N(U_0)} \mathcal{T}_{Q_0', P_0'}^N(X|\mathbf{u}_0)|.$$

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

$$|f(\mathcal{M} \times \mathcal{L}) \bigcap \bigcup_{\mathbf{u}_0 \in \mathcal{T}_{Q_0^*}^N(U_0)} \mathcal{T}_{Q_0^*, P_0^*}^N(X|\mathbf{u}_0)| \ge M \times L \times (N+1)^{-|\mathcal{X}||\mathcal{U}_0|}. \quad (3)$$

Now in the left-hand side of (2) we can consider only the codewords of types $Q_0^*$, $P_0^*$ and the part of output vectors $\mathbf{z}$ of the conditional type $V_{\mathcal{Z}|\mathcal{X}}$

$$\sum_{m,a,j: \mathbf{x}_{m,a,b_j} \in \mathcal{T}_{Q_0^*, P_0^*}^N(X|\mathbf{u}_0)} \sum_{b \in \varphi^{-1}(j)} f(\mathbf{x}_{m,a,b}|m, l) W_{\mathcal{Z}|\mathcal{X}}^N(\mathcal{T}_{Q_0^*, P_0^*, V_{\mathcal{Z}|\mathcal{X}}}^N(Z|\mathbf{u}_{0m}, \mathbf{x}_{m,a,b}) \bigcap g_2'^{-1}(b)|\mathbf{x}_{m,a,b})$$

$$\leq M \times L \times \exp\{-N(E-\delta)\}.$$

For $\mathbf{z} \in \mathcal{T}^N_{Q_0^*,P_0^*,V_{Z|X}}(Z|\mathbf{u}_{0m},\mathbf{x}_{m,a,b})$ we obtain that

$$\sum_{m,a,j:\mathbf{x}_{m,a,b_j}\in\mathcal{T}^N_{Q_0^*,P_0^*}(X|\mathbf{u}_0)} \sum_{b\in\varphi^{-1}(j)} f(\mathbf{x}_{m,a,b}|m,l)W^N_{Z|X}(\mathbf{z}|\mathbf{x}_{m,a,b}) \times \Big\{|\mathcal{T}^N_{Q_0^*,P_0^*,V_{Z|X}}(Z|\mathbf{u}_{0m},\mathbf{x}_{m,a,b})|-$$

$$-|\mathcal{T}^N_{Q_0^*,P_0^*,V_{Z|X}}(Z|\mathbf{u}_{0m},\mathbf{x}_{m,a,b})\bigcap g_2^{'-1}(b)|\Big\} \leq M \times L \times \exp\{-N(E-\delta)\},$$

or

$$\sum_{m,a,j:\mathbf{x}_{m,a,b_j}\in\mathcal{T}^N_{Q_0^*,P_0^*}(X|\mathbf{u}_0)} \sum_{b\in\varphi^{-1}(j)} f(\mathbf{x}_{m,a,b}|m,l)|\mathcal{T}^N_{Q_0^*,P_0^*,V_{Z|X}}(Z|\mathbf{u}_{0m},\mathbf{x}_{m,a,b})|-$$

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

$$\leq \sum_{m\in\mathcal{M}} \sum_{a,j:\mathbf{x}_{m,a,b_j}\in\mathcal{T}^N_{Q_0^*,P_0^*}(X|\mathbf{u}_0)} \sum_{b\in\varphi^{-1}(j)} f(\mathbf{x}_{m,a,b}|m,l)|\mathcal{T}^N_{Q_0^*,P_0^*,V_{Z|X}}(Z|\mathbf{u}_{0m},\mathbf{x}_{m,a,b})\bigcap g_2^{'-1}(b)|.$$

Then we have

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

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

$$\leq \sum_{m\in\mathcal{M}} \sum_{a,j:\mathbf{x}_{m,a,b_j}\in\mathcal{T}^N_{Q_0^*,P_0^*}(X|\mathbf{u}_0)} \sum_{b\in\varphi^{-1}(j)} f(\mathbf{x}_{m,a,b}|m,l)|\mathcal{T}^N_{Q_0^*,P_0^*,V_{Z|X}}(Z|\mathbf{u}_{0m},\mathbf{x}_{m,a,b})\bigcap g_2^{'-1}(b)|.$$

So

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

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

$$\leq \sum_{m\in\mathcal{M}} \sum_{a,j:\mathbf{x}_{m,a,b_j}\in\mathcal{T}^N_{Q_0^*,P_0^*}(X|\mathbf{u}_0)} \sum_{b\in\varphi^{-1}(j)} f(\mathbf{x}_{m,a,b}|m,l)|\mathcal{T}^N_{Q_0^*,P_0^*,V_{Z|X}}(Z|\mathbf{u}_{0m},\mathbf{x}_{m,a,b})\bigcap g_2^{'-1}(b)|. \quad (4)$$

For every $j$ we consider such $b_j$ that for each $b \in \varphi^{-1}(j)$

$$|\mathcal{T}^N_{Q_0^*,P_0^*,V_{Z|X}}(Z|\mathbf{u}_{0m},\mathbf{x}_{m,a,b})\bigcap g_2^{'-1}(b)| \leq |\mathcal{T}^N_{Q_0^*,P_0^*,V_{Z|X}}(Z|\mathbf{u}_{0m},\mathbf{x}_{m,a,b_j})\bigcap g_2^{'-1}(b_j)|,$$

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

$$\sum_{m\in\mathcal{M}} \sum_{a,j:\mathbf{x}_{m,a,b_j}\in\mathcal{T}^N_{Q_0^*,P_0^*}(X|\mathbf{u}_0)} \sum_{b\in\varphi^{-1}(j)} f(\mathbf{x}_{m,a,b}|m,l)|\mathcal{T}^N_{Q_0^*,P_0^*,V_{Z|X}}(Z|\mathbf{u}_{0m},\mathbf{x}_{m,a,b})\bigcap g_2^{'-1}(b)|$$

$$\leq \sum_{m\in\mathcal{M}} \sum_{a,j:\mathbf{x}_{m,a,b_j}\in\mathcal{T}^N_{Q_0^*,P_0^*}(X|\mathbf{u}_0)} |\mathcal{T}^N_{Q_0^*,P_0^*,V_{Z|X}}(Z|\mathbf{u}_{0m},\mathbf{x}_{m,a,b_j})\bigcap g_2^{'-1}(b_j)| \sum_{b\in\varphi^{-1}(j)} f(\mathbf{x}_{m,a,b}|m,l)$$

$$\leq \sum_{m\in\mathcal{M}} |T^N_{Q_0^*,P_0^*V_{Z|X}}(Z|u_{0m})| \leq M\exp\{NH_{Q_0^*,P_0^*V_{Z|X}}(Z|U_0)\}. \quad (5)$$

Taking into account (3) and by substituting (5) in (4) we come to

$$M\times L\times(N+1)^{-|\mathcal{X}||\mathcal{U}_0|(|\mathcal{Z}|+1)}\exp\{NH_{Q_0^*,P_0^*,V_{Z|X}}(Z|U_0,X)\}-$$
$$-M\times L\times\exp\{N[D(V_{Z|X}\|W_{Z|X}|Q_0^*,P_0^*)+H_{Q_0^*,P_0^*,V_{Z|X}}(Z|X)-E+\delta]\}$$
$$\leq M\exp\{NH_{Q_0^*,P_0^*V_{Z|X}}(Z|U_0)\}.$$

Therefore

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

Since $L=A\times J$ then $J\leq L$, so

$$J\leq\frac{\exp\{NI_{Q_0^*,P_0^*,V_{Z|X}}(X\wedge Z|U_0)\}}{(N+1)^{-|\mathcal{X}||\mathcal{U}_0|(|\mathcal{Z}|+1)}-\exp\{N(D(V_{Z|X}\|W_{Z|X}|Q_0^*,P_0^*)-E+\delta)}. \quad (6)$$

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

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

Thus from (6) and the definition of $R_s$ we conclude

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

The proof is complete.

## Conclusion

We studied the secrecy leakage rate in the BCC and derived a sphere packing bound for $E$-capacity of secrecy leakage. This result generalizes the sphere packing bound for $E$-capacity of DMC, and will be used to establish an inner bound for $E$-capacity region of the BCC.

## Acknowledgment

The author would like to thank Professor E. Haroutunian for helpful comments.

## References

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

[2] 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.

[3] 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. Inform. Theory, Tashkent, USSR*, vol. 1, pp. 19-21, 1984.

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

[5] 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.

[6] 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.

## Գաղտնի հաղորդագրություններով լայնասփյուռ կապուղու գաղտնիքի հոսակորուստի արագության գնդերի փաթեթավորման գնահատականը

Ն. Ավշար

### Ամփոփում

Գաղտնի հաղորդագրություններով լայնասփյուռ կապուղու ընդհանուր հաղորդագրությունը փոխանցվում է երկու հասցեատերերին, իսկ մասնավոր հաղորդագրությունը՝ միայն մեկին. այն պետք է հնարավորինս գաղտնի լինի մյուսի նկատմամբ: Կառուցվել է գաղտնիքի հոսակորստի արագության $E$-ունակության վերին գնահատականը:

## Граница сферической упаковки скорости утечки секрета в широковещательном канале с секретными сообщениями

Н.Афшар

### Аннотация

Общее сообщение широковещательного канала с секретными сообщениями передается двум адресатам, а частное сообщение только одному из них и должно быть насколько возможно секретным для второго. Построена верхняя граница $E$-пропускной способности скорости утечки секрета.