ՀՀ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԶԳԱՅԻՆ ԱԿԱԴԵՄԻԱ
ԻՆՖՈՐՄԱՏԻԿԱՅԻ ԵՎ ԱՎՏՈՄԱՏԱՑՄԱՆ ՊՐՈԲԼԵՄՆԵՐԻ ԻՆՍՏԻՏՈՒՏ

Նասրին Աֆշար

ԳԱՂՏՆԻ ՀԱՂՈՐԴԱԳՐՈՒԹՅՈՒՆՆԵՐՈՎ ԼԱՅՆԱՍՓՅՈՒՌ ԿԱՊՈՒՂԻՆԵՐԻ E-ՈՒՆԱԿՈՒԹՅԱՆ ՀԵՏԱԶՈՏՈՒԹՅՈՒՆ

Ե. 13. 05 «Մաթեմատիկական մոդելավորում, թվային մեթոդներ և ծրագրերի համալիրներ» մասնագիտությամբ
ֆիզիկամաթեմատիկական գիտությունների թեկնածուի
գիտական աստիճանի հայցման ատենախոսության

Ս Ե Ղ Մ Ա Գ Ի Ր

Երևան 2013

NATIONAL ACADEMY OF SCIENCES OF ARMENIA
INSTITUTE FOR INFORMATICS AND AUTOMATION PROBLEMS

NASRIN AFSHAR

INVESTIGATION OF *E*-CAPACITY OF BROADCAST CHANNELS WITH CONFIDENTIAL MESSAGES

SYNOPSIS

of dissertation for obtaining of scientific degree of candidate of physical-mathematical sciences on speciality 05. 13. 05 “Mathematical Modeling, Numerical Methods and Software Complexes”

YEREVAN 2013

Ատենախոսության թեման հաստատվել է ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտում:

Գիտական ղեկավար՝ ֆիզ. մաթ. գիտ. դոկտոր Ե. Ա. Հարությունյան

Պաշտոնական ընդդիմախոսներ՝ տեխ. գիտ. դոկտոր Գ.Հ. Խաչատրյան
ֆիզ. մաթ. գիտ. թեկնածու Ա.Ռ. Մուրադյան

Առաջատար կազմակերպություն՝ Հայաստանի պետական ճարտարագիտական համալսարան

Պաշտպանությունը կայանալու է 2013 թ. մայիսի 10-ին, ժամը՝ 15:00 - ին, ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտում գործող ԲՈՀ-ի 037 «Ինֆորմատիկա և հաշվողական համակարգեր» մասնագիտական խորհրդի նիստում, հետևյալ հասցեով՝ Երևան, 0014, Պ.Սևակի 1:

Ատենախոսությանը կարելի է ծանոթանալ ԻԱՊԻ-ի գրադարանում:

Սեղմագիրն առաքված է 2013 թ. ապրիլի 10-ին-:

Մասնագիտական խորհրդի գիտական քարտուղար՝

ֆիզ. մաթ. գիտ. դոկտոր՝ Հ. Գ. Սարուխանյան

Theme of the dissertation has been approved in Institute for Informatics and Automation Problems of NAS of RA.

Scientific advisor: Doctor of phys. math. sciences E. A. Haroutunian
Official reviewers: Doctor of technical sciences G. H. Khachaturyan
Candidate of phys. math. sciences A. R. Muradyan

Leading organization: Armenian State Engineering University.

The defense will take place during the meeting of the Specialized Council 037 “Informatics and Computer Systems” at the Institute for Informatics and Automation Problems of NAS of RA. on 10 May 2013 at 15.00.

The dissertation is available in the scientific library of IIAP.

The synopsis has been distributed at 10 April 2013.

The Scientific Secretary of the Specialized Council,

Doctor of phys. math. sciences, H. G. Sarukhanyan

CHARACTERIZATION OF THE THESIS

Actuality of the problem

Secrecy is an important requirement of many communication applications. The information-theoretic problem for single receiver secure communication system was solved by Wyner in famous paper "The wire-tap channel" [1]. The object of study of wiretap channel is to maximize the rate of reliable communication from the source to the legitimate receiver, while the wiretapper learns as little as possible about the source output. Wyner has determined the achievable rate-equivocation region when both the main and the wiretap channels are discrete memoryless. Later, Csiszar and Korner made the next important step by generalizing Wyner's result. They considered a discrete memoryless broadcast channel with a confidential message for one of the receivers and a common message for both receivers[2].

In this thesis, we study information protection systems requiring both the reliability and the confidentiality from eavesdropping.

Nowadays, new wireless devices are deployed. The broadcast nature of a wireless medium allows for the transmitted signal to be received by all users within the communication range. For example, many devices like telephones, computers, keyboards or headphones, traditionally connected via cables, are now connected in a wireless manner. With pervasive use of wireless data and voice services, the demand for reliable and secure communications with broadcast systems is becoming more urgent.

Objectives of the work

Important properties of each communication channel are characterized by the *reliability function* $E(R)$, which was introduced by Shannon [3]. The reliability function defines the optimal exponent of the exponential decrease $\exp\{-NE(R)\}$ of the decoding error probability for given R, when N increases. Another approach in channel coding problems is the *E-capacity (rate-reliability function)* denoted by $C(E)$ (also $R(E)$) introduced by E. Haroutunian [4], which presents optimal dependence of the code rate R on given error probability exponent (reliability) E. The function $C(E)$ is in natural conformity with Shannon's notion of the channel capacity C and of the zero-error capacity C_0. When E increases from zero to infinity, the function $C(E)$ decreases from C to C_0. This characteristic of the channel is also called *E-capacity*. Due to principal difficulty of determining the E-capacity function, it is usual to study its estimation. This approach can be more effective to study complicated systems rather than study of reliability function. The estimation of E-capacity region of broadcast channel without secrecy constraint is obtained by M. Haroutunian.

The main purpose of the dissertation is to generalize the previous results on the capacity region of the BCC, BC-2CM and the generalized wiretap channel. The results also develop the previous results in estimation of E-capacity of the DMC and the BC over secure communication systems. To this end, the following tasks are solved:

- construction of inner estimate for the E-capacity region of the wiretap channel,

[1] Wyner A. D., "The wire-tap channel," *Bell System Technical Journal,* vol. 54, no. 8, pp. 1355 – 1387, 1975.

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

[3] Shannon C. E., "Probability of error for optimal codes in Gaussian channels", *Bell System Technical Journal*, vol. 38, no 5, pp. 611 – 659, 1959.

[4] Haroutunian E. A., "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.

- to find inner estimate of E-capacity region of the broadcast channel with confidential messages,
- to estimate secrecy E-capacity region of the broadcast channel with two confidential messages,
- to find upper bound of the E-capacity of secrecy leakage of the BCC.

Objects of investigations

In this thesis, the E-capacity region of the wiretap channel and of some models of broadcast channels with confidential messages are studied. The secrecy leakage of the broadcast channel with confidential messages and the upper bound of the E-capacity of secrecy leakage are investigated.

Methods of investigations

In the work, we apply methods of information theory. Especially, we use effectively the method of types developed by Csiszar and Korner [5] (disscused in Chapter 1) and fundamental notions of information, entropy and the divergence of Kullback-Leibler (presented also in chapter 1).

Scientific novelty

All results presented in the thesis are new. Dependence of optimal rates on error exponents of the wiretap channels and the broadcast channel with confidential messages was not estimated before our works.

Practical and theoretical significance of the results

The results of the thesis can be used in different application of information theory. The expressions characterizing rates of optimal code for given reliabilities are derived which can be applied in different practical situations.

The following statements are presented for defending

- The stochastic encoding for random coding bound construction of E-capacity of the asymmetric broadcast channel without secrecy constraint is not effective.
- Random coding bound of E-capacity region of the wiretap channel is obtained.
- Random coding bound of E-capacity region of the broadcast channel with confidential messages is constructed.
- Sphere packing bound of E-capacity of secrecy leakage of the broadcast channel with confidential messages is found.
- Random coding bound of secrecy E-capacity region of the broadcast channel with two confidential messages is determined.

Approbation of the results

The results of the thesis have been presented in the following conferences.

- The 8th International Conference on Computer Sciences and Information Technologies, Yerevan, 2011, [2].
- Scientific Conference Devoted to 80th Anniversary of Doctor of physical-mathematical science I. Zaslasvky, Yerevan, 2012 [3].
- IEEE 20th Telecommunication Forum (TELFOR), Belgrade, Serbia, 2012 [6].
- The 7th Annual Conference RAU, Dedicated to the 90th Anniversary of Academician S. Hambartsumian, Yerevan, 2012.

[5] Csiszár I., "Method of types", *IEEE Transactions on Information Theory*, vol. 44, no. 6, pp. 2505 – 2523, 1998.

Publications

The results of the thesis are presented in 6 publications (3 articles and 3 presentations in conferences), the list of them is at the end of the text.

The structure and volume of the work

The dissertation consists of Introduction, five Chapters and Conclusion. The list of references include 97 entries. The text of the thesis is expounded on 100 pages.

Contents of the work

In Chapter 1, the necessary definitions of Information Theory, e.g. the method of types, typical sequences are introduced and the previous results related to the subject of the thesis are shortly presented. In Chapter 2, we study the stochastic encoder's affection on the random coding bound construction. In Chapter 3, the E-capacity of the generalized wiretap channel is studied. There the problem of finding inner bound of E-capacity of the wiretap channel, where error probability of the wiretapper decrease not exponentially, is solved. In Chapter 4, the broadcast channel with confidential messages is studied and the problem of finding inner bound of E-capacity of the BCC, where probability of decoding error at the eavesdropping receiver decreases exponentially, is solved. There the problem of upper bounding the E-capacity of the secrecy leakage of the BCC is also solved. In Chapter 5, the notion of secrecy E-capacity is introduced and the inner bound of secrecy E-capacity of the broadcast channel with two confidential messages is obtained.

We denote random variables by capital letters X, Y, U, ... and specific realizations of them by the corresponding lower case letters x, y, u, ... The respective random vectors of length N will be denoted by bold-faced letters $\mathbf{X}$, $\mathbf{Y}$, $\mathbf{U}$, ... and $\mathbf{x}$, $\mathbf{y}$, $\mathbf{u}$, ... We consider finite sets and denote sets by script capitals $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{U}$, ... The cardinality of the finite set $\mathcal{X}$ is denoted by $|\mathcal{X}|$. The functions exp and log are taken to the base 2.

Chapter 2: Estimation of E-capacity Region of the Asymmetric Broadcast Channel

We investigate a discrete memoryless asymmetric broadcast channel (ABC) with a finite input alphabet set $\mathcal{X}$, and finite output alphabets $\mathcal{Y}$ and $\mathcal{Z}$.

The ABC is defined by the pair $(W_{Y|X}, W_{Z|X})$ of conditional probability distributions, $W_{Y|X} : \mathcal{X} \to \mathcal{Y}$, $W_{Z|X} : \mathcal{X} \to \mathcal{Z}$, where

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

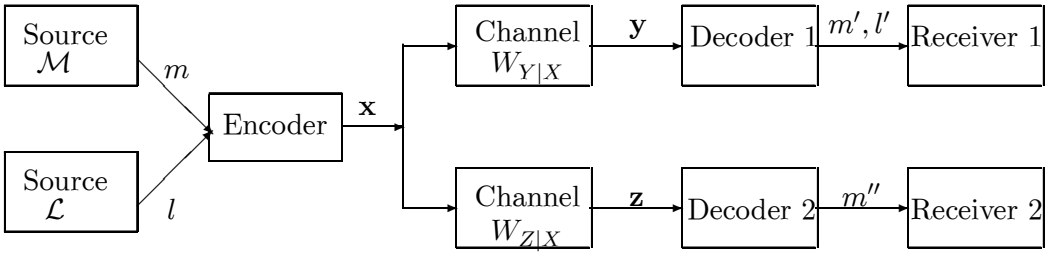

Figure 1. The model of asymmetric broadcast channel.

The $\mathcal{M}_N$ is the set of common messages which should be sent to the both receivers and $\mathcal{L}_N$ is the set of private messages which should be sent to receiver 1. Let $\mathcal{U}_1$, $\mathcal{U}_2$ be some auxiliary finite sets and U_1, U_2, X, Y and Z are random variables with values in $\mathcal{U}_1$, $\mathcal{U}_2$, $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$, correspondingly.

The randomized encoding is defined as follows.

A *stochastic encoder* f with block length N for the asymmetric broadcast channel is specified by a matrix of conditional probabilities $f(\mathbf{x}|m,\, l)$, where $\mathbf{x} \in \mathcal{X}^N$, $m \in \mathcal{M}_N$, $l \in \mathcal{L}_N$ and $\sum\limits_{\mathbf{x}\in\mathcal{X}^N} f(\mathbf{x}|m,\, l) = 1$.

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

A code (f, g_1, g_2) is characterized by rates $R_1,\, R_2$, where R_1 and R_2 are the transmission rates for $m \in \mathcal{M}_N$ and $l \in \mathcal{L}_N$, respectively,

$$R_1 = \frac{1}{N}\log|\mathcal{M}_N|, \;\; R_2 = \frac{1}{N}\log|\mathcal{L}_N|.$$

The maximal probabilities of erroneous transmission of the pair of messages $(m, l) \in \mathcal{M}_N \times \mathcal{L}_N$ by the channels $W_{Y|X}$ and $W_{Z|X}$ using a code (f, g_1, g_2) are defined, respectively,

$$e(f,\, g_1,\, W_{Y|X}) \stackrel{\triangle}{=} \max_{m\in\mathcal{M}_N,\, l\in\mathcal{L}_N} \sum_{\mathbf{x}\in\mathcal{X}^N} f(\mathbf{x}|m,\, l) W^N_{Y|X}(\mathcal{Y}^N - g_1^{-1}(m,\, l)|\mathbf{x}),$$

$$e(f,\, g_2,\, W_{Z|X}) \stackrel{\triangle}{=} \max_{m\in\mathcal{M}_N,\, l\in\mathcal{L}_N} \sum_{\mathbf{x}\in\mathcal{X}^N} f(\mathbf{x}|m,\, l) W^N_{Z|X}(\mathcal{Z}^N - g_2^{-1}(m)|\mathbf{x}),$$

and the average error probabilities for messages assuming that the pair of random messages $M_N,\; L_N$ is uniformly distributed over $\mathcal{M}_N \times \mathcal{L}_N$ are the following

$\bar{e}(f,\, g_1,\, W_{Y|X}) \stackrel{\triangle}{=}$

$$\frac{1}{|\mathcal{M}_N| \times |\mathcal{L}_N|} \sum_{m\in\mathcal{M}_N,\, l\in\mathcal{L}_N} \sum_{\mathbf{x}\in\mathcal{X}^N} f(\mathbf{x}|m,\, l) W^N_{Y|X}(\mathcal{Y}^N - g_1^{-1}(m,\, l)|\mathbf{x}),$$

$\bar{e}(f,\, g_2,\, W_{Z|X}) \stackrel{\triangle}{=}$

$$\frac{1}{|\mathcal{M}_N| \times |\mathcal{L}_N|} \sum_{m\in\mathcal{M}_N,\, l\in\mathcal{L}_N} \sum_{\mathbf{x}\in\mathcal{X}^N} f(\mathbf{x}|m,\, l) W^N_{Z|X}(\mathcal{Z}^N - g_2^{-1}(m)|\mathbf{x}).$$

We consider the following joint distributions

$$\begin{aligned} Q\circ P\circ V_{Y|X} = \{&Q\circ P\circ V_{Y|X}(u_1,u_2,x,y) = Q(u_1,u_2)P(x|u_1,u_2)V(y|x),\\ &u_1\in\mathcal{U}_1,\; u_2\in\mathcal{U}_2,\; x\in\mathcal{X},\; y\in\mathcal{Y}\},\\ Q\circ P\circ V_{Z|X} = \{&Q\circ P\circ V_{Z|X}(u_1,u_2,x,z) = Q(u_1,u_2)P(x|u_1,u_2)V(z|x),\\ &u_1\in\mathcal{U}_1,\; u_2\in\mathcal{U}_2,\; x\in\mathcal{X},\; z\in\mathcal{Z}\}. \end{aligned}$$

Let $(U_1, U_2) \to X \to (Y, Z)$ be a Markov chain.

To formulate the inner bound of E-capacity region, we consider the following inequalities

$0 \le R_1 \le \min\Big\{$

$$\min_{V_{Y|X}:D(V_{Y|X}\|W_{Y|X}|Q,P)\le E_1} \Big| I_{Q,P,V_{Y|X}}(Y\wedge U_1) + D(V_{Y|X}\|W_{Y|X}|Q,P) - E_1\Big|^+,$$

$$\min_{V_{Z|X}:D(V_{Z|X}\|W_{Z|X}|Q,P)\le E_2} \Big| I_{Q,P,V_{Z|X}}(Z\wedge U_1) + D(V_{Z|X}\|W_{Z|X}|Q,P) - E_2\Big|^+\Big\}, \qquad (1)$$

$$0 \le R_2 \le$$

$$\min_{V_{Y|X}: D(V_{Y|X}\|W_{Y|X}|Q,P)\le E_1} \left| I_{Q,V_{Y|X}}(Y \wedge U_2|U_1) + D(V_{Y|X}\|W_{Y|X}|Q,P) - E_1 \right|^+, \qquad (2)$$

and the region

$$R_r(E) = \bigcup_{QP \in QP(\mathcal{U}_1 \times \mathcal{U}_2 \times \mathcal{X})} \{(R_1, R_2) : \text{(1) and (2) take place for some}$$

$$(U_1, U_2) \to X \to (Y, Z)\}.$$

The following theorem asserts that the stochastic encoding in inner bound construction of E-capacity of the ABC is not effective. The result is the same as random coding bound for E-capacity of the ABC [6], where deterministic encoding is applied.

Theorem 1. *For all $E_1 > 0, E_2 > 0$ the region $R_r(E)$ is an inner estimate for E-capacity region of the broadcast channel:*

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

We present the proof of the theorem in chapter 2 section 2.

Chapter 3: Estimation of E-capacity Region of the Generalized Wiretap Channel

The message m is encoded into an N-vector $\mathbf{x}$ which is the input of the main channel. Let $\mathbf{y}$ and $\mathbf{z}$ be the output of the legitimate receiver and the wiretapper, respectively. The object of study wiretap channel is to maximize the rate of reliable communication from the source to the legitimate receiver, while the wiretapper learns as little as possible about the source output. Wyner has determined the achievable rate-equivocation region when both channels are discrete memoryless.

Csiszar and Korner's BCC generalized Wyner's wiretap channel (Fig.2). We call it the generalized wiretap channel.

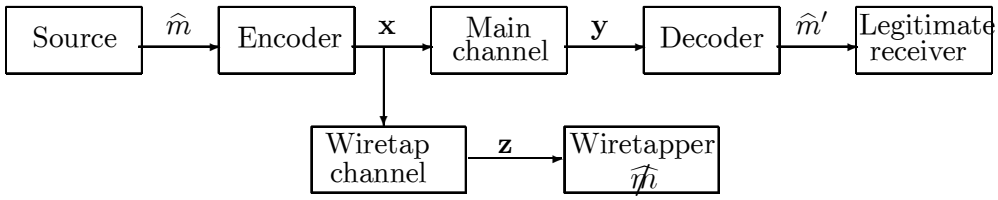

Figure 2. The model of generalized wiretap channel.

We investigate a DMC with a finite input alphabet set $\mathcal{X}$, and finite output alphabet set $\mathcal{Y}$. Let $\mathcal{Z}$ be the set of output alphabets of the wiretapper. The wiretap channel is defined by the pair (W_1, W_2) of conditional probability distributions, $W_1 : \mathcal{X} \to \mathcal{Y}$, $W_2 : \mathcal{X} \to \mathcal{Z}$, where

$$W_1^N(\mathbf{y}|\mathbf{x}) \triangleq \prod_{n=1}^{N} W_1(y_n|x_n),\ W_2^N(\mathbf{z}|\mathbf{x}) \triangleq \prod_{n=1}^{N} W_2(z_n|x_n).$$

Let $\hat{\mathcal{M}}_N$ be the message set. The message $\hat{m} \in \hat{\mathcal{M}}_N$ is communicated reliably to legitimate receiver at rate R. We use the technique of rate splitting. The message set $\hat{\mathcal{M}}_N$ is split into two parts, one part is denoted by $\mathcal{M}_N$, which can be decoded by the legitimate receiver

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

and the wiretapper at rate R_0, and the remaining part is represented by $\mathcal{L}_N$, which can be decoded by only the legitimate receiver at rate R_1 and must be kept as secrete as possible from the wiretapper. The level of ignorance is measured by equivocation rate R_e, which is the uncertainty of the wiretapper with respect to the message l.

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.

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

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

The equivocation $H(L_N|\mathbf{Z})$ is the uncertainty of receiver 2 with respect to the private message. We also consider equivocation rate $(1/N)H(L_N|\mathbf{Z})$.

Let $\mathcal{U}$ be some finite set and M_N, L_N, U, X, Y and Z are random variables with values correspondingly in $\mathcal{M}_N$, $\mathcal{L}_N$, $\mathcal{U}$, $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$.

Let Q_0 be a type and Q_1 be a conditional type of $\mathbf{x} \in \mathcal{X}^N$ given $\mathbf{u}$. Define $Q = Q_0 \circ Q_1$. Let

$$V_1 \triangleq \{V_1(y|x) : \, x \in \mathcal{X}, \;\; y \in \mathcal{Y}\}, \quad V_2 \triangleq \{V_2(z|x) : \, x \in \mathcal{X}, \;\; z \in \mathcal{Z}\}$$

be conditional types of random variable Y, Z, respectively, for given value x.

We assume that $U \to X \to (Y,\, Z)$ forms a Markov chain.

Let us define the following functions appearing in our inner estimates of E-capacity region:

$$R_0^*(Q, E_1, E_2) \triangleq \min \Big\{ \min_{V_1 : D(V_1\|W_1|Q) \le E_1} \Big| I_{Q,V_1}(U \wedge Y) + D(V_1\|W_1|Q) - E_1 \Big|^+ ,$$

$$\min_{V_2 : D(V_2\|W_2|Q) \le E_2} \Big| I_{Q,V_2}(U \wedge Z) + D(V_2\|W_2|Q) - E_2 \Big|^+ \Big\},$$

$$R_1^*(Q, E_1) \triangleq \min_{V_1 : D(V_1\|W_1|Q) \le E_1} \Big| I_{Q,V_1}(X \wedge Y|U) + D(V_1\|W_1|Q) - E_1 \Big|^+ ,$$

$$R_e^*(Q, E_1) \triangleq \min_{V_1 : D(V_1\|W_1|Q) \le E_1} \Big| I_{Q,V_1}(X \wedge Y|U) + D(V_1\|W_1|Q) - E_1 \Big|^+ -$$

$$I_{Q,W_2}(X \wedge Z|U).$$

Theorem 2. *For $E > 0$, the inner bound for E-capacity region $\mathcal{C}_W(E)$ of the generalized wiretap channel is:*

$$R_W^*(E) = \bigcup_Q \Big\{ (R,\, R_e) : \quad \textit{for} \;\; U_0 \to U_1 \to X \to (Y, Z)$$

$$R = R_0 + R_1,$$

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

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

$$0 \le R_e \le R_e^*(Q, E_1), \;\; R_e \le R \Big\}.$$

We present the proof of the theorem in Section 2 of Chapter 3.

Chapter 4: Estimation of E-capacity of the Broadcast Channel With Confidential Messages

The discrete memoryless broadcast channel with confidential messages (BCC) involves two discrete memoryless channels with two sources, one encoder and two receivers. The model

is depicted in Fig.3. 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 less than R_e. We consider error probability exponents (reliabilities) E_1, E_2, E_3, of exponentially decrease of error probabilities of the first decoder, the second decoder and of the decoder trying to find the confidential message, respectively. 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.

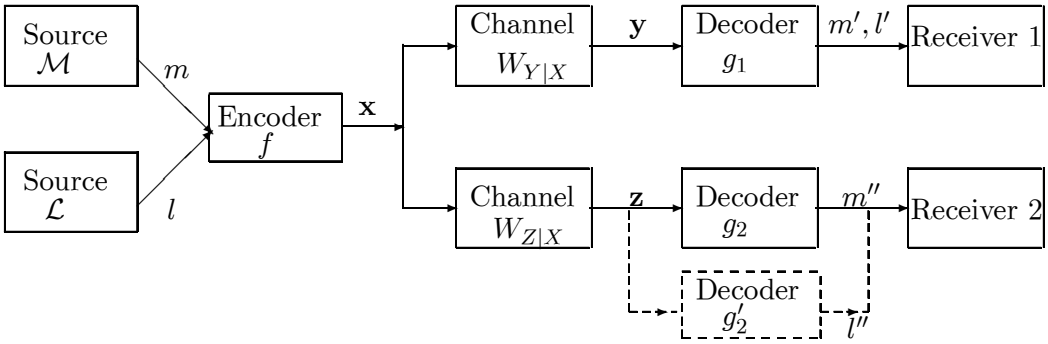

Figure 3. The model of discrete memoryless BCC.

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

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

be some conditional PDs of the channels.

We assume that $U_0 \to X \to (Y,\, Z)$ forms a Markov chain.

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

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

$$R_s^{sp}(E) \stackrel{\triangle}{=} \max_{Q_0,P_0} R_s^{sp}(E, Q_0, P_0).$$

The purpose of the following theorem is to establish a sphere packing bound for E-capacity of secrecy leakage of the BCC [4]. The proof of the theorem is presented in Section 2 of Chapter 4 .

Theorem 3: *For all $E > 0$,*

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

Consider RVs X, Y, Z and auxiliary RVs U_0, U_1 with joint PDs:
$Q \circ P_1 \circ V_{Y|X} =$

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

$Q \circ P_1 \circ V_{Z|X} =$

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

We define the following functions appearing in our inner estimates of E-capacity region:
$R_0^*(Q, P_1, E_1, E_2) \stackrel{\triangle}{=} \min\{$

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

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

$$R_1^*(Q, P_1, E_1) \stackrel{\triangle}{=} \min_{V_{Y|X}: D(V_{Y|X}\|W_{Y|X}|Q_1,P_1)\le E_1} |I_{Q,P_1,V_{Y|X}}(U_1 \wedge Y|U_0)$$
$$+D(V_{Y|X}\|W_{Y|X}|Q_1, P_1) - E_1|^+,$$

$$R_e^*(Q, P_1, E_1, E_3) \stackrel{\triangle}{=} \min_{V_{Y|X}: D(V_{Y|X}\|W_{Y|X}|Q_1,P_1)\le E_1} |I_{Q,P_1,V_{Y|X}}(U_1 \wedge Y|U_0)+$$
$$D(V_{Y|X}\|W_{Y|X}|Q_1, P_1) - E_1|^+ - \min_{V_{Z|X}: D(V_{Z|X}\|W_{Z|X}|Q_1,P_1)\le E_3} I_{Q,P_1,V_{Z|X}}(U_1 \wedge Z|U_0).$$

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

$$0 \le R_0 + R_1 \le R_0^*(Q, P_1, E_1, E_2) + R_1^*(Q, P_1, E_1), \tag{3}$$

$$0 \le R_0 \le R_0^*(Q, P_1, E_1, E_2), \tag{4}$$

$$0 \le R_e \le R_e^*(Q, P_1, E_1, E_3), \tag{5}$$

$$R_e \le R_1. \tag{6}$$

The main result of Chapter 4 is formulated in the following:

Theorem 4. ([5], [6]) *For $E_1 > 0$, $E_2 > 0$, $E_3 > 0$, the region*
$\mathcal{R}^*(E) \stackrel{\triangle}{=}$

$$\bigcup_{Q,P_1} \{(R_0,\, R_1,\, R_e) : (3) - (6) \text{ take place for } U_0 \to U_1 \to X \to (Y,\, Z)\} \tag{7}$$

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

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

Chapter 5: Estimation of secrecy E-capacity of the Broadcast Channel With Two Confidential Messages

The broadcast channel with two confidential messages (BC-2CM) involves two sources, one encoder, two discrete memoryless channels and two receivers. The model is shown in Fig. 4. Each private message $m_i \in \mathcal{M}_{i,N}$, $i = 1, 2$ is transmitted to the respective receiver at rate R_i, $i = 1, 2$, while ensuring the eavesdropping receivers to be kept in total ignorance of it. The level of ignorance is measured by the equivocation rate $R_{i,e}$, $i = 1, 2$, at the eavesdropping receiver.

The *secrecy 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, while $R_{i,e} = R_i$, $i = 1, 2$.

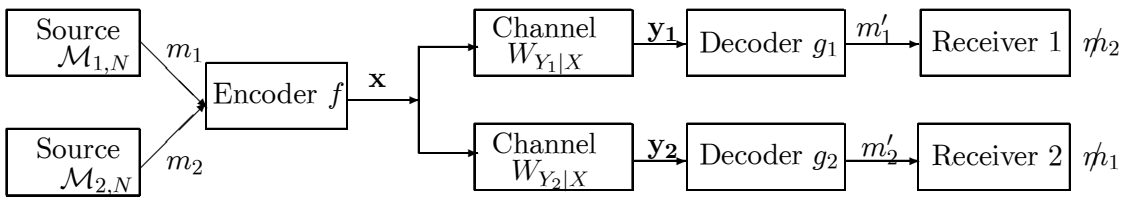

Figure 4. The model of BC-2CM.

The vector $\mathbf{x} = (x_1, ..., x_N) \in \mathcal{X}^N$ is the input, $\mathbf{y}_1 = (y_{1,1}, ..., y_{1,N}) \in \mathcal{Y}_1^N$ and $\mathbf{y}_2 = (y_{2,1}, ..., y_{2,N}) \in \mathcal{Y}_2^N$ are the output vectors after N uses of channels. We introduce some additional finite sets $\mathcal{U}_0$, $\mathcal{U}_1$, $\mathcal{U}_2$. The 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 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.

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

$$P_0 \circ P_{1,2|0} \circ P_{X|U_1,U_2} \circ V_{Y_i|X} = \{P_0 \circ P_{1,2|0} \circ P_{X|U_1,U_2} \circ V_{Y_i|X}(u_0, u_1, u_2, x, y_i) =$$
$$P_0(u_0) P_{1,2|0}(u_1, u_2|u_0) P_{X|U_1,U_2}(x|u_1, u_2) V_{Y_i|X}(y_i|x),$$
$$u_0 \in \mathcal{U}_0, u_1 \in \mathcal{U}_1, u_2 \in \mathcal{U}_2, x \in \mathcal{X}, y_i \in \mathcal{Y}_i\}, i = 1, 2. \tag{8}$$

Let $U_0 \to (U_1, U_2) \to X \to (Y_1, Y_2)$ form a Markov chain.

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,

$$P_{Y_i|U_i,U_0}(y_i|u_i, u_0) \stackrel{\triangle}{=}$$
$$\sum_{u_{3-i},x} P_{U_{3-i}|U_i,U_0}(u_{3-i}|u_i, u_0) P_{X|U_1,U_2}(x|u_1, u_2) W_{Y_i|X}(y_i|x), \tag{9}$$

$$P^1_{Y_i|U_i,U_0}(y_i|u_i, u_0) \stackrel{\triangle}{=}$$
$$\sum_{u_{3-i},x} P_{U_{3-i}|U_i,U_0}(u_{3-i}|u_i, u_0) P_{X|U_1,U_2}(x|u_1, u_2) V_{Y_i|X}(y_i|x), \tag{10}$$

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 $\mathbf{y}_i \in \mathcal{Y}_i^N$, $i = 1, 2$.

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:

$0 \le R_1 \le$

$$\min_{P^1_{Y_1|U_1,U_0} \in \mathcal{D}_1(E_1)} \left| I_{P_{0,1}, P^1_{Y_1|U_1,U_0}}(U_1 \wedge Y_1|U_0) + \mathrm{D}(P^1_{Y_1|U_1,U_0} \| P_{Y_1|U_1,U_0} | P_{0,1}) - E_1 \right|^+$$
$$- I_{P_{0,1}, P_{Y_2|U_2,U_0}}(U_1 \wedge Y_2|U_2, U_0) - I_{P_{0,1,2}}(U_1 \wedge U_2|U_0), \tag{11}$$

$0 \le R_2 \le$

$$\min_{P^1_{Y_2|U_2,U_0} \in \mathcal{D}_2(E_2)} \left| I_{P_{0,2}, P^1_{Y_2|U_2,U_0}}(U_2 \wedge Y_2|U_0) + \mathrm{D}(P^1_{Y_2|U_2,U_0} \| P_{Y_2|U_2,U_0} | P_{0,2}) - E_2 \right|^+$$
$$- I_{P_{0,2}, P_{Y_1|U_1,U_0}}(U_2 \wedge Y_1|U_1, U_0) - I_{P_{0,1,2}}(U_1 \wedge U_2|U_0). \tag{12}$$

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

$$\mathcal{R}^*(E) \stackrel{\triangle}{=} \bigcup_{P_{0,1,2}} \{(R_1, R_2) : \text{(11), (12) take place for some}$$
$$\text{Markov chain } U_0 \to (U_1, U_2) \to X \to (Y_1, Y_2)\}.$$

Theorem 5. *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:*

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

We present the proof of this theorem using the method of types.

Main results of the dissertation are the following:

- The affection of using the randomized encoder in the random coding bound construction of the E-capacity region of the asymmetric broadcast channel in comparison to applying the deterministic encoder, is studied.
- The E-capacity region of the generalized wiretap channel in two cases, when error probability of the eavesdropper to find a part of message decreases either exponentially or not exponentially is studied.
- The upper bound of E-capacity of the secrecy leakage of the BCC is found.
- Using the obtained sphere packing bound of the secrecy leakage and the method of rate-splitting, the inner estimate of E-capacity region of the BCC is derived.
- A single letter characterization of random coding bound for secrecy E-capacity region of the broadcast channel with two confidential messages is derived.

These results generalize the previous results on
a) the capacity region of the BCC, BC-2CM and the wiretap channel,
b) the E-capacity of the DMC and the BC over secure communication systems.

Publications of results of dissertation

[1] Afshar N., "Random coding bound for E-capacity region of asymmetric broadcast channel with stochastic encoding," *Mathematical Problems of Computer Science,* no. 35, 53 – 62, 2011.

[2] Haroutunian E. A., Haroutunian M. E. and Afshar N., "Random coding bound for E-capacity region of the wiretap channel," *8th International Conference of Computer Science and Information Technologies,* Yerevan, Armenia, pp. 121 – 124, 2011.

[3] Afshar N., Haroutunian E. and Haroutunian M., "Random coding bound for secrecy E-capacity region of the broadcast channel with two confidential messages", *Mathematical Problems of Computer Science,* no. 36, 79 – 90, 2012.

[4] Afshar N., "Sphere packing bound for E-capacity of secrecy leakage of the broadcast channel with confidential messages", *Mathematical Problems of Computer Science,* no. 37, 39 – 44, 2012.

[5] Afshar N., Haroutunian E. and Haroutunian M., "On Random coding bound for E-capacity region of the broadcast channel with confidential messages", *Mathematical Problems of Computer Science,* no. 38, 34 – 36, 2012.

[6] Afshar N., Haroutunian E. and Haroutunian M., "On inner bound for E-capacity region of the broadcast channel with confidential messages", *IEEE 20th Telecommunication Forum (TELFOR),* November 20-22, Serbia, 2012.

Նասրին Աֆշար

Գաղտնի հաղորդագրություններով լայնասփյուռ կապուղիների E-ունակության հետազոտում

Ամփոփում

Ատենախոսությունը նվիրված է գաղտնագողի առկայությամբ կապուղում և գաղտնի հաղորդագրություններով լայնասփյուռ կապուղիներում օպտիմալ կոդերի սխալի հավանականության ցուցիչի վարքի ուսումնասիրությանը:

Գաղտնիությունը և հուսալիությունը կարևոր պահանջ են բազմակի կապի համակարգերի նկատմամբ: Ինֆորմացիոն-տեսական խնդիրը մեկ հասցեատերով հուսալի հաղորդման համակարգի նկատմամբ լուծվել էր Վայների կողմից 1975 թ. հայտնի "Կապուղի գաղտնագողով" հոդվածում: Գաղտնագողի առկայությամբ կապուղու հետազոտման նպատակն է հնարավորին չափ մեծացնել աղբյուրից դեպի օրինական հասցեատերը հուսալի հաղորդման արագությունը, պայմանով, որ գաղտնագողը հնարավորինս քիչ տեղեկություն ստանա հաղորդման մասին: Վայները գտել է արագություն-անորոշություն հասանելի տիրույթը, երբ՝ և հիմնական կապուղին, և գաղտնագողի կապուղին ընդհատ են և առանց հիշողության: Այլ կարևոր ուսումնասիրության առակա է գաղտնի հաղորդագրություններով լայնասփյուռ կապուղին, որը առաջին անգամ դիտարկել են Չիսարը և Կյորները 1978 թ.: Նրանք ստացել են այդ կապուղու ունակության տիրույթը:

Յուրաքանչյուր կապուղու կարևոր հատկությունները բնութագրում է հուսալիության $E(R)$ ֆունկցիան, որը ներմուծել է Շենոնը 1959 թ.: Հուսալիության ֆունկցիան որոշում է տված R արագության և կոդի N ծավալի աճման դեպքում սխալի հավանականության ցուցչային $exp\{-NE(R)\}$ նվազման E ցուցիչը:

Կապուղու կոդավորման խնդրին այլ մոտեցում է Ե. Հարությունյանի կողմից 1967 թ. առաջարկված E-ունակությունը (արագություն-ունակություն ֆունկցիան), որը նշանակվում է $C(E)$ (կամ $R(E)$) և արտահայտում կոդի R արագության օպտիմալ կախվածությունը սխալի հավանականության E ցուցչից (հուսալիությունից): $C(E)$ ֆունկցիան բնական ընդհանրացում է շենոնյան գաղափարների՝ C ունակության և զերոյական սխալի հավանականությամբ C_0 ունակության: Երբ E-ն աճում է զերոից մինչև անվերջություն, $C(E)$ ֆունկցիան նվազում է C-ից մինչև C_0: Նկատի ունենալով E-ունակություն, կամ հուսալիության ֆունկցիան գտնելու սկզբունքային դժվարությունը , ընդունված է ուսումնասիրել նրանց գնահատականները: Լայնասփյուռ կապուղու E-ունակության տիրույթի ներքին սահմանը՝ գաղտնիության պայմանների բացակայության դեպքում, ստացվել է Մ. Հարությունյանի կողմից:

Ներկա աշխատանքում լուծվել են՝ գաղտնագողի առկայությամբ կապուղու և գաղտնի հաղորդագրություններով լայնասփյուռ կապուղիների որոշ մոդելների E-ունակության ուսումնասիրման ակտուալ խնդիրները: Ատենախոսությունում ստացված արդյունքները ընդհանրացում են հենյալ արդյունքների նկատմամբ.

- գաղտնի հաղորդագրություններով լայնասփյուռ կապուղու ունակության տիրույթի,
- գաղտնագողի առկայությամբ կապուղու ունակության տիրույթի,
- երկու գաղտնի հաղորդագրություններով լայնասփյուռ կապուղու ունակության տիրույթի,
- Ե. Հարությունյանի կողմից ստացված ընդհատ առանց հիշողության կապուղու E-ունակության,

- Մ. Հարությունյանի կողմից ստացված լայնասփյուռ կապուղու E-ունակության տիրույթի ներքին սահմանի:

Ատենախոսության հիմնական արդյունքները հետևյալներն են:

- Ուսումնասիրվել է անհամաչափ լայնասփյուռ կապուղու E-ունակության տիրույթի պատահական կոդավորման սահմանի կառուցման հարցում պատահականացված կոդավորման օգտագործման ազդեցությունը դետերմինացված կոդավորման օգտագործման համեմատ:

- Ուսումնասիրվել է գաղտնագողի առկայությամբ ընդհանրացված կապուղու E-ունակության տիրույթը երկու դեպքում, երբ գաղտնագողի կողմից հաղորդագրության մի մասի որոշման սխալվելու հավանականությունը նվազում է կամ ցուցչային օրենքով,, կամ ոչ ցուցչային արագությամբ:

- Գտնված է գաղտնի հաղորդագրություններով լայնասփյուռ կապուղու գաղտնիության պակասի E-ունակության տիրույթի վերին սահմանը:

- Նախորդ արդյունքի և արագությունների տրոհման եղանակի օգտագործմամբ դուրս է բերվել գաղտնի հաղորդագրություններով լայնասփյուռ կապուղու E-ունակության ներքին սահմանը:

- Ստացվել է երկու գաղտնի հաղորդագրություններով լայնասփյուռ կապուղու գաղտնիության E-ունակության տիրույթի պատահական կոդավորման սահմանի միտառանի բնութագրումը:

Ատենախոսության արդյունքները զեկուցվել են երկու միջազգային և երկու հանրապետական գիտաժողովներում, հրապարակվել են 6 գիտական հրապարակումներում:

Насрин Афшар

Исследование E-пропускной способности широковещательного канала с секретными сообщениями

Аннотация

Диссертация посвящена изучению поведения экспоненты вероятности ошибки оптимальных кодов в канале с нарушителем и в широковещательных каналах с секретными сообщениями.

Секретность и надежность являются важными требованиями ко многим системам связи. Информационно-теоретическая проблема для системы надежной передачи с одним адресатом была рещена Вайнером в знаменитой статье "Канал с нарушителем" в 1975 г. Цель изучения канала с нарушителем - максимизировать скорость надежной передачи от источника к законному адресату, при условии что нарушитель узнает об сообщении на выходе источника по-возможности меньще. Вайнер определил достижимую область скорость-неопреселенность, когда и основной канал, и канал нарущителя являются дискретными и без памяти. Другим важным объектом изучения является широковещательный канал с секретными сообщениями впервые рассмотренный Чисаром и Кернером в 1978 г. Они получили область пропускной способности такого канала.

Важные свойства каждого канала связи характеризуются функцией надежности $E(R)$ введенной Щенноном в 1959 г. Функция надежности определяет оптимальную экспоненту экспоненциального убывания $\exp\{-NE(R)\}$ вероятности ошибки при заданной скорости R и увеличении обема кода N.

Другой подход к проблеме кодирования для канала - E-пропускная способность (функция скорость-надежность) обозначаемая $C(E)$ (или $R(E)$) предложенная Е.Арутюняном в 1967 г., которая выражает оптимальную зависимость скорости кода R от экспоненты вероятности ошибки (надежности) E. Функция $C(E)$ является естественным обобщением щенноновских понятий пропускной способности C и пропускной способности при нулевой вероятности ошибки C_0. Когда E увеличивается от нуля до бесконечности, функция $C(E)$ убывает от C до C_0. В виду принципиальной трудности нахождения E-пропускной способности или функции надежности, принято изучать их оценки. Внутренная граница области E-пропускной способности широковещательного канала без условий секретности была получена М.Арутюнян.

В настящей работе рещены актуальные задачи изучения E-пропускной способности канала с нарущителем и некоторых моделей широковещательного канала с секретными сообщениями. Полученные в диссертации результаты обобщают результаты относительно:

- области пропускной способности широковещательного канала с секретными сообщениями,
- области пропускной способности канала с нарущителем,
- области пропускной способности широковещательного канала с двумя секретными сообщениями,
- E-пропускной способности дискретного канала без памяти, полученные Е.Арутюняном,
- области E-пропускной способности широковещательного канала полученой М.Арутюнян.

Основными результатами диссертации являются:

- Изучено влияние использования рандомизированного кодирования при построении границы случайного кодирования E-пропускной способности асимметричного широковещательного канала в сравнении с применением детерминированного кодирования,
- Изучена область E-пропускной способности обобщенного канала с нарущителем в двух случаях, когда вероятность ощибки нарущителя при определении части сообщения убывает или экспоненциально, или не экспоненциально,
- Найдена верхняя граница E-пропускной способности недостатка секрета широковещательного канала с секретными сообщениями,
- Использованием предыдущего результата и метода разбиения скоростей, выведена внутренняя граница области E-пропускной способности широковещательного канала с секретными сообщениями,
- Получена однобуквенная характеризация границы случайного кодирования секретной E-пропускной способности широковещательного канала с двумя секретными сообщениями.

Результаты диссертации были доложены на двух международных конференциях, двух республиканских совещаниях, и опубликованы в 6 публикациях.

Ծավալը - 1 տ.մ. Տպաքանակը - 100 օրինակ
Տպագրված է ՀՀ ԳԱԱ ԻԱՊԻ կոմպյուտերային
պոլիգրաֆիայի լաբորատորիայում