Mathematical Problems of Computer Science 41, 47–54, 2014.

The Shannon Cipher System With Correlated Source Outputs and Wiretapper Guessing Subject to Distorion

Tigran M. Margaryan

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

Abstract

The Shannon cipher system with discrete memoryless sources is considered. The wiretapper gains the cryptogram through the public noiseless channel and tries to guess the secret information which is related to the encrypted plaintext. It is assumed that at each step of sequential guesses the wiretapper has a testing mechanism to identify the secret message within the given distortion level. The security level of the encryption system is measured by the guessing rate which is the highest asymptotic exponential growth rate of the expected number of guesses. The estimations of guessing rate are obtained.

Keywords: Shannon cipher system, Correlated sources, Guessing rate.

1. Introduction

The theoretical secrecy of Shannon's model of cipher system (SCS) is traditionally measured by *equivocation* [1]. In most of works in this area it is supposed that wiretapper has exactly one chance to estimate the plaintext. Shannon also gave the idea of practical secrecy, which is the average amount of work required to break the key. Hellman took one step forward in practical (or computational) secrecy, proposed to measure the degree of security of the cipher system in terms of the expected number of key-plaintext combinations needed to explain the given ciphertext [2]. Merhav and Arikan suggested another security criterion for the SCS , *guessing exponent*, which is the highest asymptotic exponential growth rate of the moment of the number of guesses [3]. The guessing exponent for extended SCS models was explored in these works: the SCS with correlated source outputs was studied by Hayashi and Yamamoto [4] and with general sources was studied by Hanawal and Sundaresan [5]. The SCS with distortion and reliability requirements was investigated by Haroutunian and Ghazaryan [6, 7]. We have examined the *guessing rate*, which is the highest asymptotic exponential growth rate of the expected number of guesses in models: the SCS with a noisy channel to the wiretapper [8, 9], the SCS with the correlated source outputs and the noisy channel [10, 11], the SCS with the distortion and the noisy channel [12, 13].

In this paper we study the combined model of the SCS considered in the papers [6] and [4]. The cryptographic system depicted in Fig. 1 is the SCS with correlated sources. The

memoryless source generates mutually correlated messages one of which is secret and the other must be transmitted to the legitimate receiver via a public channel. The adversary may gain a transmitted message containing relevant information about a secret message, therefore, it is desirable to transmit it after ciphering even if it is not secret. The transmitter encrypts the plaintext using the key generated by the memoryless key source. The key is also communicated to the decrypter by a special secure channel. After ciphering the cryptogram is sent over a public channel to a legitimate receiver, who can recover the original plaintext using the cryptogram and the same key. Not knowing the key, the wiretapper that eavesdrops on the public channel aims to guess the secret message related to the cryptogram. It is assumed that the wiretapper knows the source distributions and encryption functions and tries to reconstruct the source secret message within some given distortion measure and distortion level.

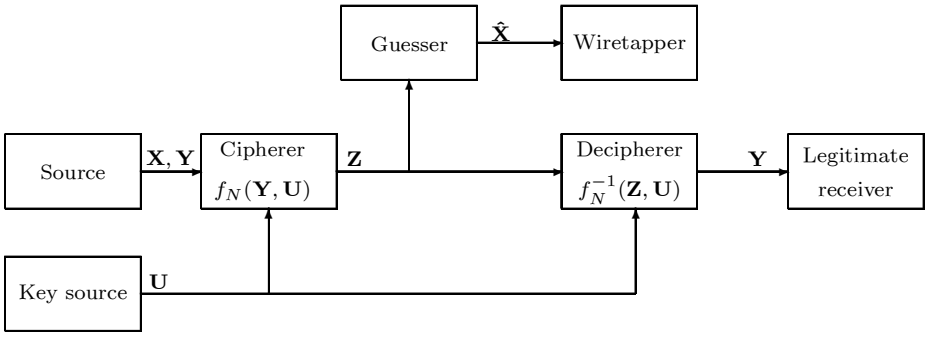

Fig. 1. The Shannon cipher system with correlated source outputs.

For an approximative reconstruction of a secret message the wiretapper makes sequential guesses, each time applying a testing mechanism by which he can learn whether the estimate is successful or not and stops when the answer is affirmative. Our goal is to estimate the *guessing rate*, which characterize the secrecy level of the system.

2. System Model and Definitions

We denote the RV by capital letters, the random vector by bold capital letters, and their realizations are denoted by lower-case letters, respectively. In the system shown in Fig. 1. the source and the key-source are stationary and memoryless.

The source is assumed to generate discrete mutually correlated random vectors $\mathbf{X}$ and $\mathbf{Y}$ which consist of discrete, independent, identically distributed (i.i.d.) random variables (RVs) $(X_1, X_2, \ldots, X_N)$ and $(Y_1, Y_2, \ldots, Y_N)$. $\mathbf{X}$ is secret and $\mathbf{Y}$ must be sent to a legitimate receiver. Y has a probability distribution (PD) $P^* = \{P^*(y), y \in \mathcal{Y}\}$ and X has a conditional PD $V^* = \{V^*(x|y), x \in \hat{\mathcal{X}}, y \in \mathcal{Y}\}$ where $\mathcal{X}$ and $\mathcal{Y}$ are the finite alphabets of source. The joint PD of the pair (X, Y) is $P^* \circ V^* = \{P^* \circ V^*(x, y) = P^*(y)V^*(x|y), y \in \mathcal{Y}, x \in \mathcal{X}\}$ and the marginal PD of X is $P^*V^* = \{P^*V^*(x) = \sum\limits_{y \in \mathcal{Y}} P^*(y)V^*(x|y), x \in \mathcal{X}\}$.

The key-source generates the random vector $\mathbf{U} = (U_1, U_2, \ldots, U_K)$ of K purely random bits independent of $(\mathbf{X}, \mathbf{Y})$. $\mathbf{U}$ is used for encryption and also is sent to legitimate receiver by a special secure channel.

We encrypt only $\mathbf{Y}$ using the key $\mathbf{U}$ by the encryption function $f_N : \mathcal{Y}^N \times \mathcal{U}^K \to \mathcal{Z}^*$ where $\mathcal{Z}$ is the cryptogram alphabet. After ciphering we obtain a random vector $\mathbf{Z}$ (may have variable length depending on N and K) which is sent via a public channel to a legitimate

receiver. This encryption function is assumed to be convertible providing the given key, i.e. there exists the decryption function $f_N^{-1} : \mathcal{Z}^* \times \mathcal{U}^K \to \mathcal{Y}^N$ which allows the legitimate receiver to recover the original $\mathbf{Y}$. The wiretapper gets the cryptogram $\mathbf{Z}$ by the public noiseless channel.

In this task it is allowed for wiretapper to recover the original secret massage with some acceptable deviation. Denote values of the RV $\hat{X}$ by the $\hat{x}$ representing the reconstruction by the wiretapper of the source secret message with values in the finite wiretapper reproduction alphabet $\hat{\mathcal{X}}$, in general, different from $\mathcal{X}$.

We consider a single-letter distortion measure between the source and the wiretapper reproduction messages: $d : \mathcal{X} \times \hat{\mathcal{X}} \to [0; \infty)$. The distortion measure between the vector $\mathbf{x} \in \mathcal{X}^N$ and a wiretapper reproduction vector $\hat{\mathbf{x}} \in \hat{\mathcal{X}}^N$ is defined as the average of the component distortions:

$$d(\mathbf{x}, \hat{\mathbf{x}}) \stackrel{\triangle}{=} N^{-1} \sum_{n=1}^{N} d(x_n, \hat{x}_n).$$

The wiretapper getting the cryptogram $\mathbf{z}$ produces some guessing strategy $g^N = \{\hat{\mathbf{x}}_1(\mathbf{z}), \hat{\mathbf{x}}_2(\mathbf{z}), \cdots\}$ until some vector $\hat{\mathbf{x}}$ is found. We say that the guessing strategy is Δ-achievable if there exists some j such that $Pr\{d(\mathbf{X}, \hat{\mathbf{x}}_j(\mathbf{z})) \leq N\Delta\} = 1$ (see [14]). Let $G_{f,g}^N(\hat{\mathbf{X}}|\mathbf{Z})$ be a number of guesses needed for the wiretapper to reproduce the $\hat{\mathbf{x}}$ by the strategy g^N.

Definition 1: *The key rate R_K of the key source is defined by $R_K = N^{-1} \log 2^K = K/N$.*

Definition 2: *The Δ-achievable guessing rate $R(P^*, V^*, R_K, \Delta)$ of this system is defined by*

$$R(P^*, V^*, R_K, \Delta) = \lim_{N \to \infty} \sup_{f_N} \inf_{g_N} \tfrac{1}{N} \log E[G_{f,g}^N(\hat{\mathbf{X}}|\mathbf{Z})],$$

where $E[G_{f,g}^N(\hat{\mathbf{X}}|\mathbf{Z})]$ is the expectation of $G_{f,g}^N(\hat{\mathbf{X}}|\mathbf{Z})$.

We apply the method of types and covering lemma ([15], [16]. The type P of vector $\mathbf{y} = (y_1, \ldots, y_N) \in \mathcal{Y}^N$ is a PD $P = \{P(y) = N(y|\mathbf{y})/N,\ y \in \mathcal{Y}\}$, where $N(y|\mathbf{y})$ is the number of repetitions of the symbol y among $y_1, \ldots, y_N$. The set of vectors $\mathbf{y}$ of type P is denoted by $\mathcal{T}_P^N(Y)$. The set of all PD on $\mathcal{Y}$ is denoted by $\mathcal{P}(\mathcal{Y})$ and the subset of $\mathcal{P}(\mathcal{Y})$ consisting of the possible types of sequences $\mathbf{y} \in \mathcal{Y}^N$ is denoted by $\mathcal{P}_N(\mathcal{Y})$.

We denote entropy of RV Y with PD P and, respectively, relative entropy between P and P^* as follows

$$H_P(Y) \stackrel{\triangle}{=} -\sum_{y \in \mathcal{Y}} P(y) \log P(y),$$

$$D(P||P^*) \stackrel{\triangle}{=} \sum_{y \in \mathcal{Y}} P(y) \log \frac{P(y)}{P^*(y)}.$$

The joint type of vector $\mathbf{y} \in \mathcal{Y}^N$ and $\mathbf{z} \in \mathcal{Z}^M$ is the PD $\{M(y, z|\mathbf{y}, \mathbf{z})/M,\ y \in \mathcal{Y},\ z \in \mathcal{Z}\}$, where $M(y, z|\mathbf{y}, \mathbf{z})$ is the number of occurrences of pair symbols (y, z) in the pair of vectors $(\mathbf{y}, \mathbf{z})$.

We say that the conditional type of $\mathbf{x}$ for the given $\mathbf{y}$ is PD $V = \{V(x|y),\ x \in \mathcal{X},\ y \in \mathcal{Y}\}$ if $N(y, x|\mathbf{y}, \mathbf{x}) = N(y|\mathbf{y})V(x|y)$ for all $y \in \mathcal{Y}$, $x \in \mathcal{X}$. The set of all sequences $\mathbf{x} \in \mathcal{X}^N$ of the conditional type V for the given $\mathbf{y} \in \mathcal{T}_P^N(Y)$ is denoted by $\mathcal{T}_{P,V}^N(X|\mathbf{y})$ and called the V-shell of $\mathbf{y}$. $\mathcal{V}_N(\mathcal{X}, P)$ is the set of all possible V-shells of $\mathbf{y}$ of type P .

For the given PDs P^* and P of Y , conditional PDs V^* and V of X for the given Y conditional entropy of RV X for the given RV Y is defined by

$$H_{P,V}(X|Y) \stackrel{\triangle}{=} -\sum_{y\in\mathcal{Y},x\in\mathcal{X}} PV(x)\log V(x|y),$$

the relative divergence between joint PDs $P\circ V$ and $P^*\circ V^*$ is defined by

$$D(P\circ V\|P^*\circ V^*) \stackrel{\triangle}{=} \sum_{y\in\mathcal{Y},x\in\mathcal{X}} P(y)V(x|y)\log\frac{P(y)V(x|y)}{P^*(y)V^*(x|y)}.$$

Let $PV = Q = \{Q(x), x\in\mathcal{X}\}$ be a PD on $\mathcal{X}$ and $W = \{W(\hat{x}\mid x),\, x\in\mathcal{X},\, \hat{x}\in\hat{\mathcal{X}}\}$ be a conditional PD on $\hat{\mathcal{X}}$ for the given x, then the mutual information between X and $\hat{X}$ is defined as

$$I_{Q,W}(X\wedge\hat{X}) = \sum_{x,\hat{x}} Q(x)W(\hat{x}\mid x)\log\frac{W(\hat{x}\mid x)}{\sum\limits_{x} Q(x)W(\hat{x}\mid x)}.$$

The rate-distortion function for a source with PD Q and distortion level Δ is equal to

$$R(Q,\Delta) = \min_{W\in\mathcal{W}(Q,\Delta)} I_{Q,W}(X\wedge\hat{X}), \tag{1}$$

where $\mathcal{W}(Q,\Delta)$ is a set of conditional PDs W satisfying the following condition

$$E_{Q,W}\, d(X,\hat{X}) = \sum_{x,\hat{x}} Q(x)\, W(\hat{x}\mid x)\, d(x,\hat{x}) \le \Delta.$$

We will use the following inequalities and covering lemma ([15], [16])

$$|\mathcal{Q}_N(\mathcal{X})| < (N+1)^{|\mathcal{X}|}, \tag{2}$$

$$|\mathcal{V}_N(\mathcal{X},P)| < (N+1)^{|\mathcal{Y}||\mathcal{X}|}, \tag{3}$$

$$|\mathcal{T}^N_{P,V}(X|\mathbf{y})| \le \exp\{NH_{P,V}(X|Y)\}, \tag{4}$$

$$P^*\circ V^*\{\mathcal{T}^N_{P,V}(X,Y)\} \le \exp\{-ND(P\circ V\|P^*\circ V^*)\}. \tag{5}$$

We write $f(N) = o(N)$ as $N\to\infty$ to mean that $\lim\limits_{N\to\infty} f(N)/N = 0$.

Lemma 1: *For every type $Q\in\mathcal{Q}_N(\mathcal{X})$ and distortion level Δ there exists a collection of vectors $\mathcal{L}(N,Q,\Delta)\in\hat{\mathcal{X}}^N$ which covers $\mathcal{T}^N_Q(X)$, such that for every vector $\mathbf{x}\in\mathcal{T}^N_Q(X)$*

$$\min_{\hat{\mathbf{x}}\in\mathcal{L}(\mathbf{N},\mathbf{Q},\mathbf{\Delta})} d(\mathbf{x},\hat{\mathbf{x}}) \le N\Delta,$$

and

$$\log|\mathcal{L}(N,Q,\Delta)| = NR(Q,\Delta) + o(N). \tag{6}$$

We also use the following notations

$$h(P,V,R_K,\Delta) = \min\{R(P,\Delta), H_{P,V}(X|Y) + R_K\},$$

$$h(P,V,R_K) = \min\{H_{PV}(X), H_{P,V}(X|Y) + R_K\}$$

and

$$h(P,R_K,\Delta) = \min\{R(P,\Delta), R_K\}.$$

3. Formulation of Result

In the following theorem the upper and lower bounds for the Δ-achievable guessing rate are presented.

Theorem 1: *For the given PD P^*, conditional PDs V^*, and any key rate R_K, the following estimates are valid:*

$$R(P^*, V^*, R_K, \Delta) \leq \max_{P,V}[h(P, V, R_K, \Delta) - D(P \circ V \| P^* \circ V^*)],$$

$$R(P^*, V^*, R_K, \Delta) \geq \max_{P}[h(P, R_K, \Delta) - D(P \| P^*)].$$

Corollary 1: *When the source generate only one message ($\mathbf{X} = \mathbf{Y}$) we arrive at the result of Haroutunian [7] if the reliability goes to infinity:*

$$R(P^*, R_K, \Delta) = \max_{P}[h(P, R_K, \Delta) - D(P||P^*)].$$

Corollary 2: *When $\Delta = 0$ we arrive at the result Hayashi and H. Yamamoto [4]:*

$$R(P^*, V^*, R_K) = \max_{P,V}[h(P, V, R_K) - D(P \circ V \| P^* \circ V^*)].$$

Proof of Theorem

Let the pair of vectors $(\mathbf{x}, \mathbf{y})$ be generated by the source having the joint type $P \circ V$ ($(\mathbf{x}, \mathbf{y}) \in \mathcal{T}_{P,V}(X, Y)$). To build a strategy for the wiretapper, we consider the following two strategies g_1^N and g_2^N.

Strategy g_1^N: The set $\mathcal{X}^N$ can be represented as the union of vectors of various types

$$\mathcal{X}^N = \bigcup_{i=1,2,\cdots,|\mathcal{Q}_N(\mathcal{X})|} \mathcal{T}_{Q_i}^N(X).$$

The wiretapper should reconstruct the vector $\mathbf{x}$ by the given distortion level Δ. The wiretapper slights the cryptogram $\mathbf{z}$ and into each type Q tries to find some $\hat{\mathbf{x}}$ such that $d(\mathbf{x}, \hat{\mathbf{x}}) \leq N\Delta$ for every $\mathbf{x} \in \mathcal{T}_{Q_i}^N(X)$.

For simplicity of formula writing we shall note only i instead of Q_i.

We consider a guessing strategy that enumerates the types Q from according to non decreasing values of the corresponding rate-distortion functions $R(Q_i, \Delta)$: $R(1, \Delta) \leq R(2, \Delta) \leq \ldots$.

According to the lemma for the fixed i the wiretapper regardless of arrangement choose such a collection of vectors $\{\hat{\mathbf{x}}_{1,i}, \hat{\mathbf{x}}_{2,i}, ...\hat{\mathbf{x}}_{l,i}\, l = 1, 2..|L(N, i, \Delta)|\}$ that covers $\mathcal{T}_i^N(X)$. The vector $\mathbf{x}$ belongs to $\mathcal{T}_Q^N(X)$ and, therefore, it is clear that in this strategy g_1^N the number of guesses is bounded with (2) and (6) in the following way

$$\begin{aligned} G_{f,g_1}^N(\hat{\mathbf{x}}|\mathbf{z}) &\leq \sum_{i:R(i,\Delta)\leq R(Q,\Delta)} |L(N, i, \delta)| \\ &\leq (N+1)^{|\mathcal{X}|} \exp\{N(R(Q, \Delta)) + o(N)\} \qquad (7) \\ &= \exp\{NR(Q, \Delta) + o(N)\}. \end{aligned}$$

Strategy g_2^N*:* In this sub-strategy the wiretapper wants to find $\hat{\mathbf{x}}$ exactly ($\hat{\mathbf{x}} = \mathbf{x}$). $\mathcal{X}^N$ can be represented as a family of vectors of various conditional types for each given vector $\mathbf{y} \in \mathcal{T}_P^N(Y)$.

$$\mathcal{X}^N = \bigcup_{i=1,2,\cdots|\mathcal{V}_N(\mathcal{X},P)|} \mathcal{T}_{P,V_i}^N(X|\mathbf{y}).$$

The wiretapper using all keys on cryptogram $\mathbf{z}$ obtains all possible $\{\mathbf{y}_i, i = 1, 2...2^K\}$, after that he tries to guess $\mathbf{x}$ assuming conditional entropy for the given vector $\mathbf{y}_i$ in ascending order ($H_{P,V_1}(X|Y) \leq H_{P,V_2}(X|Y) \leq \cdots$) tries to guess $\mathbf{x}$. The number of guesses is bounded with the help of (3) and (4) as follows

$$\begin{aligned} G_{f,g_2}^N(\hat{\mathbf{x}}|\mathbf{z}) &\leq \sum_{V_j:H_{P,V_j}(X|Y)\leq H_{P,V}(X|Y)} |\mathcal{T}_{P,V_j}^N(X|\mathbf{y})|\exp\{K\} \\ &\leq (N+1)^{|\mathcal{X}||\mathcal{Y}|}\exp\{NH_{P,V}(X|Y)\}\exp\{NR_K\} \\ &= \exp\{N(H_{P,V}(X|Y)+R_K)+o(N)\}. \end{aligned} \tag{8}$$

Strategy g_3^N*:* Combining the strategies g_1^N and g_2^N, we define a new g_3^N as follows

$$g_3^N = (\hat{\mathbf{x}}_1^1, \hat{\mathbf{x}}_1^2, \hat{\mathbf{x}}_2^1, \hat{\mathbf{x}}_2^2 \cdots).$$

Then, the number of guesses in the strategy g_3^N is not more than twofold the smaller number of guesses in g_1^N and g_2^N. We can obtain from (7) and (8)

$$\begin{aligned} G_{f,g_3}^N(\hat{\mathbf{x}}|\mathbf{z}) \leq 2\min[&\exp\{NR(P,\Delta)+o(N)\}, \\ &\exp\{N(H_{P,V}(X|Y)+R_K)+o(N)\}] \\ \leq \exp\{&Nh(P,V,R_K,\Delta)+o(N)\}. \end{aligned} \tag{9}$$

Applying the inequalities (2),(3),(8),(9), the expectation $E[G_{f,g_3}^N(\hat{\mathbf{X}}|\mathbf{Z})]$ can be bounded in the following way

$$\begin{aligned} E[G_{f,g_3}^N(\hat{\mathbf{X}}|\mathbf{Z})] \leq &\sum_{P,V} \exp\{-ND(P\circ V\|P^*\circ V^*)\}G_{f,g_3}^N(\hat{\mathbf{x}}|\mathbf{z}) \\ \leq &(N+1)^{|\mathcal{Y}||\mathcal{X}|+|\mathcal{X}|}\exp\{-ND(P\circ V\|P^*\circ V^*)\}G_{f,g_3}^N(\hat{\mathbf{x}}|\mathbf{z}) \\ \leq &\exp\{N(h(P,V,R_K,\Delta)-D(P\circ V\|P^*\circ V^*))+o(N)\}. \end{aligned} \tag{10}$$

Since our strategy is valid for any function f_N, from the inequality (10) we obtain the upper bound for the guessing rate

$$\begin{aligned} R(P^*,V^*,R_K,\Delta) &= \lim_{N\to\infty}\sup_{f_N}\inf_{g_N}\frac{1}{N}\log E[G_{f,g}^N(\hat{\mathbf{X}}|\mathbf{Z})] \\ &\leq \lim_{N\to\infty}\sup\frac{1}{N}\log E[G_{f,g_3}^N(\hat{\mathbf{X}}|\mathbf{Z})] \\ &\leq \max_{P,V}(h(P,V,R_K,\Delta)-D(P\circ V\|P^*\circ V^*)). \end{aligned}$$

It is obvious that the lower bound for $R(P^*,R_K,\Delta)$ ([7]) is also a lower bound for $R(P^*,V^*,R_K,\Delta)$

$$R(P^*,V^*,R_K,\Delta) \geq \max_P[h(P,R_K,\Delta)-D(P||P^*)].$$

Theorem is proved.

References

[1] C. E. Shannon, "Communication theory of secrecy systems", *Bell System Thechnical Journal*, vol.28, no. 3, pp. 565-715, 1949.

[2] M. E. Hellman, "An extention of the Shannon theory approach to cryptography", *IEEE Transactions on Information Theory*, vol. 23, no. 3, pp. 289–294, 1977.

[3] N. Merhav and E. Arikan, "The Shannon cipher system with a guessing wiretapper", *IEEE Transactions on Information Theory*, vol. 45, no. 6, pp. 1860-1866, 1999.

[4] Y. Hayashi and H. Yamamoto, "Coding theorems for the Shannon cipher system with a guessing wiretapper and correlated source outputs", *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2808-2817, June 2008.

[5] M. K. Hanawal and R. Sundaresan ,"The Shannon cipher system with a guessing wiretapper: General sources", *IEEE Transactions on Information Theory*, vol. 57, no. 4, pp. 2503–2515, 2011.

[6] E. A. Haroutunian and A. R. Ghazaryan, "On the Shannon cipher system with a wiretapper guessing subject to distortion and reliability requirements", *IEEE-ISIT 2002*, Lausanna , June 30-July 5, p. 324, 2002.

[7] E. A. Haroutunian, "Realibility approach in wiretapper guessing theory", *in "Aspects of Network and Information Security", NATO Science for Peace and Security, series D: Information and Communication Security*, IOS Press, vol. 17, pp. 248–260, 2008.

[8] E. A. Haroutunian and T. M. Margaryan, "The Shannon cipher system with a guessing wiretapper eavesdropping through a noisy channel", *Transactions of IIAP NAS RA, Mathematical Problems of Computer Science*, vol. 35, pp. 70-76, 2011.

[9] E. A. Haroutunian and T. M. Margaryan, "The Shannon cipher system with a guessing wiretapper eavesdropping through a noisy channel", *20th Telecommunication Forum TELFOR*, Serbia, November 20-22, pp. 532-536, 2012.

[10] E. A. Haroutunian and T. M. Margaryan, "Wiretapper guessing by noisy channel for the Shannon cipher system with correlated source outputs", *Proceedings of International Conference Computer Science and Information Technologies*, pp. 125–128, 2011.

[11] T. Margaryan, "On the Shannon cipher system with correlated source outputs and guessing wiretapper eavesdropping through a noisy Channel ", *Transactions of IIAP NAS RA, Mathematical Problems of Computer Science*, vol. 37, pp. 17-24, 2012.

[12] E. A. Haroutunian and T. M. Margaryan, "On the Shannon Cipher System with Noisy Channel to the Wiretapper Guessing Subject to Distortion Criterion", *Annual Session Dedicated to 90 Anniversary of Rafael Alexandrian*, Yerevan, pp. 53– 54, 2013.

[13] T. M. Margaryan and E. A. Haroutunian , "On the Shannon cipher system with distortion and guessing wiretapper eavesdropping through a noisy channel", *Proceedings of International Conference Computer Science and Information Technologies*, pp. 116–120, 2013

[14] E. Arikan and N. Merhav, "Guessing subject to distortion", *IEEE Transactions on Information Theory*, vol. 44, no. 3, pp. 1041-1056, 1998.

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

[16] T. M. Cover and J. A. Thomas, *Elements of Information Theory*,Second Edition, New York: Wiley, 2006.

Submitted 10.01.2014, accepted 06.03.2014.

Տրված շեղումով հարաբերակցված հաղորդագրություններով Շենոնյան ծածկագրման համակարգը գուշակող գաղտնավերլուծողի առկայությամբ

Տ. Մարգարյան

Ամփոփում

Դիտարկվել է հարաբերակցված հաղորդագրություններով Շենոնյան ծածկագրման համակարգը: աղտնագողը ստանում է գաղտնագիրը և ձգտում է գուշակել գաղտնի տեղեկությունը, որը կապված է գաղտնագրի հետ: Ենթադրվում է, որ գուշակման յուրաքանչյուր քայլում գաղտնավերլուծողը ունի ստուգման մեխանիզմ, ըստ որի կարող է իմանալ, թե արդյոք, գուշակված հաղորդագրությունը բավարարում է տրված շեղմանը: Ծածկագրման համակարգի գաղտնիության աստիճանը չափվում է գուշակման արագությամբ, որը գուշակումների քանակի սպասելի ամենամեծ ասիմպտոտիկ ցուցիչն է: նահատվել է գաղտնալսողի գուշակման արագությունը:

Шенноновская секретная система с коррелированными сообщениями источника с заданным искажением и угадывающим нарушителем

Т. Маргарян

Аннотация

В статье рассматривается шенноновская секретная система с дискретными источниками без памяти. Нарушитель получает криптограмму и стремится угадать секретную информацию, связанную с зашифрованным сообщением. Предполагатеся, что на каждом шагу нарушитель владеет тестирующим механизмом, исходя из которого он может узнать удовлетворяет ли криптограмма данному искажению. Уровень секретности криптографической системы измеряется скоростью угадывания, которая определяется наибольшим асимтотическим показателем математического ожидания числа угадываний нарушителя. Оценена скорость угадывания нарушителя.