Mathematical Problems of Computer Science 22, 2001, 12–26.

Guessing Subject to Distortion and Reliability Criteria in the Shannon Cipher System

Evgueni A. Haroutunian, Anahit R. Ghazaryan*

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

Abstract

A problem of a discrete memoryless source messages guessing within given distortion level Δ for the Shannon cipher system is solved. The security of this system is measured by the expected number of required guesses of the wiretapper needed for the reconstruction of the source messages on the base of cryptograms. In addition to the problem studied by Merhav and Arikan we demand that for a given guessing list, distortion level $\Delta \geq 0$ and reliability $E > 0$ the probability that distortions between blocklength N source messages and each of all first $L(N)$ guessing vectors will be larger than Δ, does not exceed 2^{-NE}.

For given key rate R' the minimum (over all guessing lists) of the maximal (over all encryption functions) $L(N)$ and of the expected number of required guesses, with respect to distortion and reliability criteria, are found.

1 Introduction

We investigate the wiretapper guessing problem with respect to fidelity and reliability conditions for the Shannon cipher system (see Fig.). Encrypted messages of a discrete memoryless stationary source must be communicated as securely as possible to a legitimate receiver, which has access to a common key-vector which is independent of source messages.

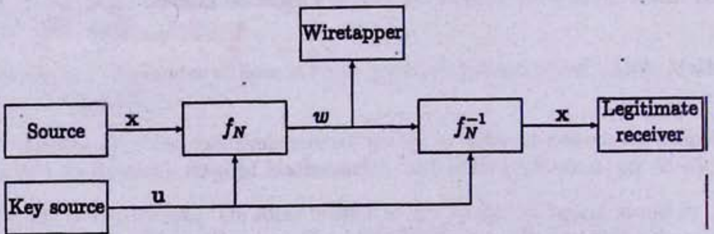

Fig. The Shannon cipher system with a guessing wiretapper.

The key-vector is transmitted by the special secure channel protected against wiretappers. The transmitter encodes the source message and key-vector and sends a cryptogram over a

*The work of the author was supported by INTAS YSF Grant 00-4163.

public channel to a legitimate receiver which based on the cryptogram and key-vector recovers the original message by the inverse, decryption function. The wiretapper that eavesdrop a public channel aims to decrypt the original source message in the framework of given distortion and reliability on the base of cryptogram, source statistic and encryption function. The wiretapper has a testing mechanism by which he can know whether the estimate is successful (is within given distortion level). The problem is to determine the minimum of the maximal (over all possible encryption functions) expected numbers of sequential guesses until the satisfactory message will be found.

The guessing problem was first considered by Massey [20] and later was investigated in [3]–[7], [9], [21]. The guessing problem subject to fidelity criterion was considered by Arikan and Merhav in [5]–[7], for reliability criterion – in [14], for the Shannon cipher system with exact reconstruction – in [21]. The Shannon cipher system with wiretapper reconstructing source messages subject to fidelity criterion were studied by Yamamoto in [23]. We study a combination of these problems with additional reliability criterion: a generalization proposed by E. Haroutunian and B. Mekoush [18] of the usual Shannon rate-distortion concept as a rate-reliability-distortion dependence. The idea is that the minimum of the maximal (over all possible encryption functions) expected number of required guesses is considered in relation to demands of guesser not only to distortion level but also to the error probability exponent (reliability). This approach was investigated for various multiterminal systems (see for example [13]–[19], [22]).

Now we pass to more detailed definitions. The source $\{X\}$ is defined as a sequence $\{X_i\}_{i=1}^{\infty}$ of discrete, independent, identically distributed (d. i. i. d.) random variables (RV) taking values in the finite set $\mathcal{X}$ of messages of the source. Let

$$P^* = \{P^*(x), x \in \mathcal{X}\}$$

be the given probability distribution (PD) of source messages. Since we study the memoryless source,

$$P^{*N}(\mathbf{x}) = \prod_{n=1}^{N} P^{*N}(x_n).$$

The key $\{U\}$ is a sequence $\{U_i\}_{i=1}^{\infty}$ of d. i. i. d. RV taking values in the set $\mathcal{U} = \{0, 1\}$. Let $\mathbf{X} = (X_1, X_2, \dots, X_N)$ be a random sequence of N messages, $\mathbf{U} = (U_1, U_2, \dots, U_K)$ be a sequence of K purely random bits independent of the source messages vector $\mathbf{X}$. Denote by $\hat{X}$ the reconstruction by the wiretapper of the source message, with values in finite set $\hat{\mathcal{X}}$, which in general is different from $\mathcal{X}$ and is wiretapper reproduction alphabet. $\mathcal{X}^N$ and $\hat{\mathcal{X}}^N$ denote the N-th order Cartesian powers of the sets $\mathcal{X}$ and $\hat{\mathcal{X}}$, respectively, $\mathcal{U}^K$ - the K-th order Cartesian power of the set $\mathcal{U}$. We consider a single-letter distortion measure between source and wiretapper reproduction messages:

$$d : \mathcal{X} \times \hat{\mathcal{X}} \to [0; \infty).$$

The distortion measure between a source vector $\mathbf{x} = (x_1, x_2, ..., x_N) \in \mathcal{X}^N$ and a wiretapper reproduction vector $\hat{\mathbf{x}} = (\hat{x}_1, \hat{x}_2, ..., \hat{x}_N) \in \hat{\mathcal{X}}^N$ is defined as average of the components'. distortions:

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

Distribution $P_1^* = \{1/2, 1/2\}$ is the PD of the key bits. The key-vector $\mathbf{u} = (u_1, u_2, \dots, u_K)$ is a sequence of these bits and $P_1^{*K}(\mathrm{u}) = \dfrac{1}{2^K}$.

Let

$$f_N : \mathcal{X}^N \times \mathcal{U}^K \rightarrow \mathcal{W}(N,K)$$

be an encryption function and $\mathcal{W}(N,K)$ be the set of all corresponding cryptograms. It is assumed that this function is invertible given the key, that is there exists the decryption function

$$f_N^{-1} : \mathcal{W}(N,K) \times \mathcal{U}^K \rightarrow \mathcal{X}^N.$$

For a cryptogram $w = f_N(\mathbf{x}, \mathbf{u})$, the ordered list of sequential guesses

$$\mathcal{G}_N(w) = \{\hat{\mathbf{x}}_1(w), \hat{\mathbf{x}}_2(w), \ldots\} \ (\hat{\mathbf{x}}_l(w) \in \hat{\mathcal{X}}^N, l = 1, 2, \ldots, |\hat{\mathcal{X}}|^N)$$

is called the guessing strategy of the wiretapper. For given guessing strategy $\mathcal{G}_N(w)$, $w \in \mathcal{W}(N,K)$ we name a guessing function and note $G_N(\mathbf{x} \mid w)$ the function that maps each vector $\mathbf{x} \in \mathcal{X}^N$ into a positive integer:

$$G_N : \mathcal{X}^N \times \mathcal{W}(N,K) \rightarrow \{1, 2, 3, \ldots, L(N)\},$$

which is the index l of the first such guessing vector $\hat{\mathbf{x}}_l(w) \in \mathcal{G}_N(w)$ that $d(\mathbf{x}, \hat{\mathbf{x}}_l(w)) \leq \Delta$. In other words, l is the number of sequential guesses of the wiretapper for a source vector $\mathbf{x} \in \mathcal{X}^N$ until the successful estimate $\hat{\mathbf{x}}_l(w) \in \mathcal{G}_N(w)$ will be found. Let $L(N)$ is prescribed limitation of the number of guesses.

For each distortion level $\Delta \geq 0$, positive number $L(N) < |\hat{\mathcal{X}}|^N$ and a guessing strategy $\mathcal{G}_N(w)$ consider the following set of successfully deciphered vectors of messages

$$\mathcal{A}(L(N), \mathcal{G}_N(w), \Delta) = \{\mathbf{x} : \exists \mathbf{u}, \exists l, \, l \leq L(N) : \ f(\mathbf{x}, \mathbf{u}) = w, \ \ d(\mathbf{x}, \hat{\mathbf{x}}_l(w)) \leq \Delta\},$$

and the probability of error

$$e(L(N), \mathcal{G}_N(w), \Delta) = 1 - P^{*N}\left(\mathcal{A}(L(N), \mathcal{G}_N(w), \Delta)\right).$$

Below log-s and exp-s are taken to the base 2.

Let R' be the key rate:

$$R' = N^{-1} \log 2^K = K.$$

A pair of guessing rates (R'', R) is called (R', E, Δ)-achievable for $E > 0$, $\Delta \geq 0$ and R', if for every $\varepsilon > 0$, encryption function f and sufficiently large N there exists a guessing strategy $\mathcal{G}_N(w)$ such that

$$N^{-1} \log L(N) \leq R'' + \varepsilon,$$

$$N^{-1} \log \mathrm{E}_{P^*, P_1^*}\{G_N(\mathbf{X} \mid W)\} \leq R + \varepsilon,$$

and

$$e(L(N), \mathcal{G}_N(w), \Delta) \leq \exp\{-NE\}.$$

Let us denote by $\mathcal{R}_G(P^*, R', E, \Delta)$ and call the key-distortion-reliability guessing rates region the set of all (R', E, Δ)-achievable pairs of guessing rates. When $E \rightarrow \infty$, $\mathcal{X} \equiv \hat{\mathcal{X}}$ and $R'' = \log |\mathcal{X}|$, $R_G(P^*, R', E, \Delta)$ becomes the key guessing rate function $R_G(P^*, R')$, studied by Merhav and Arikan in [21].

In the next section we specify the region of key-distortion-reliability guessing rates. The proof is presented in the section 3.

2 Formulation of Result

Let $P = \{P(x), x \in \mathcal{X}\}$ be a PD on $\mathcal{X}$ and $Q = \{Q(\hat{x} \mid x), x \in \mathcal{X}, \hat{x} \in \hat{\mathcal{X}}\}$ be a conditional PD on $\hat{\mathcal{X}}$ for given x.

Consider for given $E > 0$ the following set of PD P:

$$\alpha(E) = \{P : D(P \parallel P^*) \leq E\}$$

with divergence

$$D(P \parallel P^*) = \sum_x P(x) \log \frac{P(x)}{P^*(x)}.$$

Denote by $\Phi(P, \Delta) = Q_P$ a function, which puts into the correspondence to PD P some such conditional PD Q_P that for given Δ the following condition is fulfilled:

$$\mathrm{E}_{P,Q_P} d(X, \hat{X}) = \sum_x P(x) Q_P(\hat{x} \mid x) d(x, \hat{x}) \leq \Delta.$$

Denote by $\mathcal{M}(P, \Delta)$ the set of all such functions $\Phi(P, \Delta)$ for given Δ and P. Below for brevity we shall just write $\Phi(P)$.

We use the following notations for entropy and information:

$$H_P(X) = -\sum_x P(x) \log P(x),$$

$$I_{P,Q_P}(X \wedge \hat{X}) = \sum_{x,\hat{x}} P(x) Q_P(\hat{x} \mid x) \log \frac{Q_P(\hat{x} \mid x)}{\sum_x P(x) Q_P(\hat{x} \mid x)}.$$

We denote by $R(P, \Delta)$ the rate-distortion function for given PD P (see [11]):

$$R(P, \Delta) = \min_{\Phi(P) \in \mathcal{M}(P,\Delta)} I_{P,\Phi(P)}(X \wedge \hat{X}),$$

and by $R(P^*, E, \Delta)$ the rate-reliability-distortion function for PD of source messages P^* (see [18]):

$$R(P^*, E, \Delta) = \max_{P \in \alpha(E)} \min_{\Phi(P) \in \mathcal{M}(P,\Delta)} I_{P,\Phi(P)}(X \wedge \hat{X}).$$

Let us introduce the following region:

$$\widetilde{\mathcal{R}}_G(P^*, R', E, \Delta) = \{(R'', R) :$$

$$R'' \geq \min(R', R(P^*, E, \Delta)), \qquad (1)$$

$$R \geq \max_{P \in \alpha(E)} [\min(R', R(P, \Delta)) - D(P \parallel P^*)]\}. \qquad (2)$$

Theorem: For given PD P^* on $\mathcal{X}$, key rate $R' \geq 0$ and every $E > 0$, $\Delta \geq 0$,

$$\mathcal{R}_G(P^*, R', E, \Delta) = \widetilde{\mathcal{R}}_G(P^*, R', E, \Delta).$$

Corollary: When $E \to \infty$, wiretapper requires exact reconstruction of the source messages and $R'' = \log|\mathcal{X}|$, we arrive to the result of Merhav and Arikan from [21]:

$$\lim_{E \to \infty,\ \Delta = 0,\ R'' = \log|\mathcal{X}|} R_G(P^*, R', E, \Delta) = \max_P [\min(R', H_P(X)) - D(P \parallel P^*)].$$

3 Proof of the theorem

In the theorem proof we apply the method of types (see [10]–[12]). We begin with the formulation of base notions and relations.

The type P of a vector $\mathbf{x} \in \mathcal{X}^N$ is a PD $P = \{P(x) = N(x|\mathbf{x})/N,\ x \in \mathcal{X}\}$, where $N(x|\mathbf{x})$ is the number of repetitions of symbol x among $x_1, \dots, x_N$. The set of all PD P on $\mathcal{X}$, which for given N are types of vectors in $\mathcal{X}^N$ is denoted by $\mathcal{P}(\mathcal{X}, N)$. The set of vectors $\mathbf{x}$ of type P is denoted by $\mathcal{T}_P(X)$ and also called type.

The conditional type of $\hat{\mathbf{x}}$ for given $\mathbf{x}$ is PD $Q_P = \{Q_P(\hat{x}|x),\ x \in \mathcal{X},\ \hat{x} \in \hat{\mathcal{X}}\}$ if $N(x, \hat{x}|\mathbf{x}, \hat{\mathbf{x}}) = N(x|\mathbf{x})Q_P(\hat{x}|x)$ for all $x \in \mathcal{X}$, $\hat{x} \in \hat{\mathcal{X}}$. The set of all vectors $\hat{\mathbf{x}} \in \hat{\mathcal{X}}^N$ of conditional type Q_P for given $\mathbf{x} \in \mathcal{T}_P(X)$ is denoted by $\mathcal{T}_{P,Q_P}(\hat{X}|\mathbf{x})$. The set of all possible $\mathcal{T}_{P,Q_P}(\hat{X}|\mathbf{x})$ for $\mathbf{x}$ of type P is denoted by $\mathcal{Q}_{\mathcal{P}}(\hat{\mathcal{X}}, P, N)$.

We will use the following useful properties of types ([10]–[12]):

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

$$|\mathcal{Q}_{\mathcal{P}}(\hat{\mathcal{X}}, P, N)| \le (N+1)^{|\mathcal{X}||\hat{\mathcal{X}}|}, \tag{4}$$

for any type $P \in \mathcal{P}(\mathcal{X}, N)$

$$(N+1)^{-|\mathcal{X}|} \exp\{NH_P(X)\} \le |\mathcal{T}_P(X)| \le \exp\{NH_P(X)\}, \tag{5}$$

for any conditional type Q_P and $\mathbf{x} \in \mathcal{T}_P(X)$

$$(N+1)^{-|\mathcal{X}||\hat{\mathcal{X}}|} \exp\{NH_{P,Q_P}(\hat{X}|X)\} \le |\mathcal{T}_{P,Q_P}(\hat{X}|\mathbf{x})| \le \exp\{NH_{P,Q_P}(\hat{X}|X)\}, \tag{6}$$

if $\mathbf{x} \in \mathcal{T}_P(X)$, then for any PD Q on $\mathcal{X}$

$$Q^N(\mathbf{x}) = \exp\{-N(H_P(X) + D(P \parallel Q))\}, \tag{7}$$

$$(N+1)^{-|\mathcal{X}|} \exp\{-ND(P \parallel Q)\} \le Q^N(\mathcal{T}_P(X)) \le \exp\{-ND(P \parallel Q)\}. \tag{8}$$

The proof of the inequality

$$\widetilde{\mathcal{R}}_G(P^*, R', E, \Delta) \subseteq \mathcal{R}_G(P^*, R', E, \Delta) \tag{9}$$

is based on the following random coding lemma about covering of types of vectors, which is a modification of the covering lemmas from [1], [2], [11], [19]:

Lemma: Let for $\varepsilon > 0$,

$$L(P, Q) = \exp\{N(I_{P,Q}(X \wedge \hat{X}) + \varepsilon)\}.$$

Then for every type P and conditional distribution Q for N large enough there exist the collections of vectors

$$\{\hat{\mathbf{x}}_l \in \mathcal{T}_{P,Q}(\hat{X}),\ l = \overline{1, L(P,Q)}\},$$

such that the family of conditional types

$$\{\mathcal{T}_{P,Q}(X \mid \hat{\mathbf{x}}_l),\ l = \overline{1, L(P,Q)}\}$$

cover $\mathcal{T}_P(X)$.

The proof of lemma is similar to the proof of lemmas in [1], [2], [11], [13], [19].

Let us represent $\mathcal{X}^N$ as a family of disjoint types

$$\mathcal{X}^N = \bigcup_{P \in \mathcal{P}(\mathcal{X},N)} \mathcal{T}_P(X).$$

In the sequel without mention we consider only PD P which are types P for N, that is $P \in \mathcal{P}(\mathcal{X}, N)$.

Let some $\delta > 0$ be given. Then for N large enough the probability of appearance of the source sequences of types beyond $\alpha(E+\delta)$ can be estimated as follows:

$$P^{*N}(\bigcup_{P \notin \alpha(E+\delta)} \mathcal{T}_P(X)) = \sum_{P \notin \alpha(E+\delta)} P^{*N}(\mathcal{T}_P(X)) \leq$$

$$\leq (N+1)^{|\mathcal{X}|} \exp\{-N \min_{P \notin \alpha(E+\delta)} D(P \parallel P^*)\} \leq$$

$$\leq \exp\{-NE - N\delta + |\mathcal{X}| \log(N+1)\} \leq \exp\{-N(E+\delta/2)\} \leq \exp\{-NE\}.$$

Here the first inequality follows from (upper estimate in (5)) and the second inequality holds due to the definition of the set $\alpha(E)$. Consequently, in order to obtain the desired level of probability $e(L(N), \mathcal{G}_N(w), \Delta)$, it is sufficient to construct the guessing strategy only for the vectors with types P from $\alpha(E+\delta)$.

First we construct a guessing strategy that ignores the cryptogram. It is possible to order the types P from $\alpha(E+\delta)$ as $\{P_1, P_2, \ldots\}$ according to increasing value of corresponding rate-distortion functions $R(P_i, \Delta) = R(i, \Delta)$ (for simplicity of formulae writing instead of P_i we shall write only i):

$$R(i, \Delta) \leq R(i+1, \Delta), \ 1 \leq i \leq |\alpha(E+\delta)|.$$

For fixed i let the set $\{\hat{\mathbf{x}}_{i,l} \in \mathcal{T}_{i,Q_i^{\min}}(\hat{X}), l = \overline{1, L(i, Q_i^{\min})}\}$, with

$$L(i, Q_i^{\min}) = \exp\{N(\min_{\Phi(i) \in \mathcal{M}(i,\Delta)} I_{i,\Phi(i)}(X \wedge \hat{X}) + \varepsilon)\} = \exp\{N(R(i,\Delta) + \varepsilon)\}$$

be a collection of vectors such that according to the lemma for N large enough the set

$$\{\mathcal{T}_{i,Q_i^{\min}}(X \mid \hat{\mathbf{x}}_{i,l}), l = \overline{1, L(i, Q_i^{\min})}\},$$

covers $\mathcal{T}_i(X)$.

Consider the following guessing strategy:

$$\mathcal{G}_N^*(w) = \{\{\hat{\mathbf{x}}_{1,l}, l = \overline{1, L(Q_{P_1}^{\min})}\}, \{\hat{\mathbf{x}}_{2,l}, l = \overline{1, L(Q_{P_2}^{\min})}\}, \ldots\}.$$

The number of required guesses $G_N^*(\mathbf{x} \mid w)$ for $\mathbf{x} \in \mathcal{T}_i(X)$, $P_i \in \alpha(E+\delta)$ and any w is upperbounded by

$$G_N^*(\mathbf{x} \mid w) \leq \sum_{j,\, j \leq i} L(j, Q_j^{\min}) \leq L(i, Q_i^{\min}) \exp\{N\varepsilon\} = \exp\{N(R(i,\Delta) + 2\varepsilon)\}.$$

Consider now a guessing strategy that using cryptogram w carries out an key-search attack:

$$\mathcal{G}_N^{**}(w) = \{f_N^{-1}(w, \mathbf{u}_1), f_N^{-1}(w, \mathbf{u}_2), \ldots\},$$

where $\mathbf{u}_1, \mathbf{u}_2, \ldots$ is a sequence of all possible key-vectors of lengh K. This sequence contains 2^K vectors, therefore for any cryptogram w the number of required guesses $G_N^{**}(\mathbf{x} \mid w)$ for $\mathbf{x} \in \mathcal{T}_P(X)$, $P \in \alpha(E+\delta)$, is upperbounded by

$$G_N^{**}(\mathbf{x} \mid w) \le \exp\{K\}.$$

Finally, let us consider the following combined guessing list:

$$\mathcal{G}_N^{***}(w) = \{\{\hat{\mathbf{x}}_{1,l}, l = \overline{1, L(1, Q_1^{\min})}\}, f_N^{-1}(w, \mathbf{u}_1), \{\hat{\mathbf{x}}_{2,l}, l = \overline{1, L(2, Q_2^{\min})}\}, f^{-1}(w, \mathbf{u}_2), \ldots\}.$$

For the given cryptogram w the number of sequential wiretapper guesses for the source vector $\mathbf{x} \in \mathcal{T}_i(X)$, $P_i \in \alpha(E+\delta)$ is upperbounded by

$$G_N^{***}(\mathbf{x} \mid w) \le 2 \cdot \min\{\exp\{K\}, \exp\{N(R(i,\Delta) + 2\varepsilon)\} = \exp\{N(\min(R', R(i,\Delta)) + 3\varepsilon)\}.$$

Hence

$$L(N) = \exp\{N(\min(R', R(P^*, E+\delta, \Delta)) + 3\varepsilon)\}.$$

Taking into account independence of key-vectors and source message vectors and using upper estimates (5) for probabilities of the sets $\mathcal{T}_i(X)$, $1 \le i \le |\alpha(E+\delta)|$, we obtain that

$$\begin{aligned}
\mathrm{E}_{P^*, P_1^*}\{G_N^{***}(\mathbf{X} \mid W)\} &= \sum_{i: P_i \in \alpha(E+\delta)} \sum_{\mathbf{x} \in \mathcal{T}_i(X)} \sum_{\mathbf{u} \in \mathcal{U}^K} P^{*N}(\mathbf{x}) P_1^{*K}(\mathbf{u}) G_N^{***}(\mathbf{x} \mid f_N(\mathbf{x}, \mathbf{u})) \le \\
&\le \sum_{i: P_i \in \alpha(E+\delta)} \sum_{\mathbf{x} \in \mathcal{T}_i(X)} P^{*N}(\mathbf{x}) \exp\{N(\min(R', R(i,\Delta)) + 3\varepsilon)\} \sum_{\mathbf{u} \in \mathcal{U}^K} P_1^{*K}(\mathbf{u}) = \\
&= \sum_{i: P_i \in \alpha(E+\delta)} \exp\{N(\min(R', R(i,\Delta)) + 3\varepsilon)\} \sum_{\mathbf{x} \in \mathcal{T}_i(X)} P^{*N}(\mathbf{x}) = \\
&= \sum_{i: P_i \in \alpha(E+\delta)} \exp\{N(\min(R', R(i,\Delta)) + 3\varepsilon)\} P^{*N}(\mathcal{T}_i(X)) \le \\
&\le \sum_{P \in \alpha(E+\delta)} \exp\{N(-D(P \parallel P^*) + \min(R', R(P,\Delta)) + 3\varepsilon)\} \le \\
&\le \max_{P \in \alpha(E+\delta)} \exp\{N(-D(P \parallel P^*) + \min(R', R(P,\Delta)) + 4\varepsilon)\} = \\
&= \exp\{N(\max_{P \in \alpha(E+\delta)} (-D(P \parallel P^*) + \min(R', R(P,\Delta)) + 4\varepsilon))\}.
\end{aligned}$$

Therefore a pair of guessing rates (R'', R') such that

$$R'' \ge \frac{1}{N} \log L(N) - \varepsilon \ge \min(R', R(P^*, E+\delta, \Delta)) + 2\varepsilon,$$

$$R \ge \max_{P \in \alpha(E+\delta)} (-D(P \parallel P^*) + \min(R', R(P,\Delta)) + 4\varepsilon) - \varepsilon$$

is (R', E, Δ)-achievable.

Taking into account the arbitrariness of ε and δ, the continuity of all functions with respect to E, we obtain (9).

Now we shall prove the inclusion

$$\mathcal{R}_G(P^*, R', E, \Delta) \subseteq \widetilde{\mathcal{R}}_G^*(P^*, R', E, \Delta). \qquad (10)$$

To obtain lower bounds on $L(N)$ and $\mathrm{E}_{P^*,P_1^*}\{G_N^*(\mathbf{X} \mid W)\}$ we may assume that the guesser is informed of the type $\mathcal{T}_P(X)$ of the source message $\mathbf{x}$. Any lower bounds on $L(N)$ and $\mathrm{E}_{P^*,P_1^*}\{G_N^*(\mathbf{X} \mid W)\}$ for this informed guesser are also lower bounds for the original, uninformed guesser because the class of guessing strategies with side information is a superset of the class of guessing strategies without it. We shall consider a specific encryption function from [21]. Let $\mathcal{G}_N(w)$ be an arbitrary guessing strategy for this encryption function and $e(L(N), \mathcal{G}_N(w), \Delta) \leq \exp\{-NE\}$ for some $L(N)$.

The encryption function is constructed as follows. A given source vector $\mathbf{x}$ is represented as a sequence (w_{b_1}, w_{b_2}) of $(b_1 + b_2)$ bits: the first $b_1 = \lceil \log |\mathcal{P}(\mathcal{X}, N)| \rceil$ bits of the sequence describe the index of the type P of the set $\mathcal{T}_P(X)$ that contains $\mathbf{x}$, the last $b_2 = \lceil \log |\mathcal{T}_P(X)| \rceil$ bits identify the index of $\mathbf{x}$ within $\mathcal{T}_P(X)$. The encryption function is constructed by different ways for the cases $\exp\{K\} < |\mathcal{T}_P(X)|$ and $\exp\{K\} \geq |\mathcal{T}_P(X)|$.

1) Consider the case $\exp\{K\} < \log |\mathcal{T}_P(X)|$.

The set $\mathcal{T}_P(X)$ is partitioned into $M = \lfloor |\mathcal{T}_P(X)| / \exp\{K\} \rfloor$ disjoint subsets $\mathcal{T}_P^{(1)}(X)$, $\mathcal{T}_P^{(2)}(X), \ldots, \mathcal{T}_P^{(M)}(X)$, each of size $\exp\{K\}$ and if $|\mathcal{T}_P(X)| / \exp\{K\}$ is not integer an additional subset $\mathcal{T}_P^{(M+1)}(X)$. Then the index of the subset $\mathcal{T}_P^{(m)}(X)$ $(1 \leq m \leq M+1)$ which contains $\mathbf{x}$ is identified by a sequence w_{c_1} of $c_1 = \log(M+1) = \lceil \log |\mathcal{T}_P(X)| \rceil - K$ bits, and the index of $\mathbf{x}$ within $\mathcal{T}_P^{(m)}(X)$ - by a sequence of $c_2 = K$ bits. Let the encryption function f is following: $f(\mathbf{x}, \mathbf{u}) = (w_{b_1}, w_{c_1}, w_{c_2})$, where the sequence w_{c_2} of last c_2 bits is obtained after using simple bit-by-bit XOR operation on the c_2 bits describing the index of $\mathbf{x}$ within $\mathcal{T}_P^{(m)}(X)$ and on the bits of $\mathbf{u}$.

Let $\mathcal{W}(\mathbf{x})$ be the set of all cryptograms w of the fixed vector $\mathbf{x}$. Then the conditional probability of w given $\mathbf{x} \in \mathcal{T}_P(X)$ is equal

$$Pr(w \mid \mathbf{x}) = Pr(\mathbf{u} \mid \mathbf{x}) = P_1^{*K}(\mathbf{u}) = \begin{cases} \exp\{-K\}, & w \in \mathcal{W}(\mathbf{x}), \\ 0, & \text{elsewhere.} \end{cases}$$

Using Bayes rule and (7) the conditional probability of $\mathbf{x} \in \mathcal{T}_P(X)$ given $w = f(\mathbf{x}, \mathbf{u})$ (that is $\mathbf{x} \in \mathcal{W}^{-1}(w)$) is

$$Pr(\mathbf{x} \mid \mathbf{x} \in \mathcal{T}_P(X), w) = \frac{Pr(\mathbf{x} \mid \mathbf{x} \in \mathcal{T}_P(X)) P(w \mid \mathbf{x})}{\sum\limits_{\mathbf{x}' \in \mathcal{T}_P(X)} Pr(\mathbf{x}' \mid \mathbf{x}' \in \mathcal{T}_P(X)) P(w \mid \mathbf{x}')} =$$

$$= \frac{\exp\{-NH_P(X) - ND(P \parallel P^*) - K\}}{\sum\limits_{\mathbf{x}' \in \mathcal{T}_P(X) \bigcap \mathcal{W}^{-1}(w)} \exp\{-NH_P(X) - ND(P \parallel P^*) - K\}} = |\mathcal{W}^{-1}(w) \bigcap \mathcal{T}_P(X)|^{-1}. \tag{11}$$

Let $\mathcal{A}_1(L(N), \mathcal{G}_N(w), \Delta)$ be the set of those $\mathbf{x} \in \mathcal{A}(L(N), \mathcal{G}_N(w), \Delta)$ which can be guessed successfully only by one vector from the guessing strategy $\mathcal{G}_N(w)$:

$$\mathcal{A}_1(L(N), \mathcal{G}_N(w), \Delta) =$$

$$= \{\mathbf{x} \in \mathcal{A}(L(N), \mathcal{G}_N(w), \Delta) : \forall \mathbf{y} \in \mathcal{A}(L(N), \mathcal{G}_N(w), \Delta),\ G_N(\mathbf{x} \mid w) \neq G_N(\mathbf{y} \mid w)\}.$$

For brevity instead of $\mathcal{A}(L(N), \mathcal{G}_N(w), \Delta)$ we shall just write $\mathcal{A}$, instead of $\mathcal{A}_1(L(N), \mathcal{G}_N(w), \Delta)$ - just $\mathcal{A}_1$.

We can write:

$$\left|\mathcal{A}_1 \bigcap \mathcal{T}_P(X)\right| = |\mathcal{T}_P(X)| - \left|\overline{\mathcal{A}_1} \bigcap \mathcal{T}_P(X)\right|.$$

a) If $\mathbf{x} \in \mathcal{T}_P^{(m)}(X)$ $(1 \le m \le M)$, then from (11)

$$Pr(\mathbf{x} \mid \mathbf{x} \in \mathcal{T}_P^{(m)}(X), w) = \left|\mathcal{T}_P^{(m)}(X)\right|^{-1} = \exp\{-K\}.$$

Therefore from (8) we obtain

$$\left|\overline{\mathcal{A}_1} \bigcap \mathcal{T}_P(X)\right| = \frac{Pr(\overline{\mathcal{A}_1} \cap \mathcal{T}_P(X))}{Pr(\mathbf{x} \mid \mathbf{x} \in \mathcal{T}_P^{(m)}(X), w)} \le \frac{P^{*N}(\mathcal{T}_P(X))}{\exp\{-K\}} \le \exp\{K - ND(P \parallel P^*)\}. \tag{12}$$

Hence for $P \ne P^*$ and N large enough

$$\begin{aligned} |\mathcal{A}_1 \cap \mathcal{T}_P(X)| &\ge \exp\{K\} - \exp\{K - ND(P \parallel P^*)\} = \\ &= \exp\{K\}(1 - \exp\{-ND(P \parallel P^*)\}) \ge \exp\{K - 1\}. \end{aligned} \tag{13}$$

To find low estimate of maximum of $G_N(\mathbf{x} \mid w)$ for $\mathbf{x} \in \mathcal{A}_1 \bigcap \mathcal{T}_P(X)$ we can write as for arithmetical progression

$$\sum_{\mathbf{x} \in \mathcal{A}_1 \bigcap \mathcal{T}_P(X)} G_N(\mathbf{x} \mid w) \ge \sum_{i=1}^{|\mathcal{A}_1 \bigcap \mathcal{T}_P(X)|} i = \frac{1 + |\mathcal{A}_1 \bigcap \mathcal{T}_P(X)|}{2} \cdot \left|\mathcal{A}_1 \bigcap \mathcal{T}_P(X)\right| \tag{14}$$

and

$$\sum_{\mathbf{x} \in \mathcal{A}_1 \bigcap \mathcal{T}_P(X)} G_N(\mathbf{x} \mid w) < \left|\mathcal{A}_1 \bigcap \mathcal{T}_P(X)\right| \cdot \max_{\mathbf{x} \in \mathcal{A}_1 \bigcap \mathcal{T}_P(X)} G_N(\mathbf{x} \mid w). \tag{15}$$

Therefore from (13), (14) and (15) we obtain that for $P \ne P^*$

$$\max_{\mathbf{x} \in \mathcal{A}_1 \bigcap \mathcal{T}_P(X)} G_N(\mathbf{x} \mid w) > \frac{1 + |\mathcal{A}_1 \cap \mathcal{T}_P(X)|}{2} \ge \frac{1 + \exp\{K - 1\}}{2} \ge \exp\{K - 2\}. \tag{16}$$

b) For $\mathbf{x} \in \mathcal{T}_P^{(M+1)}(X)$ from (11) we receive that the conditional probability

$$Pr(\mathbf{x} \mid \mathbf{x} \in \mathcal{T}_P^{(M+1)}(X), w) = \left|\mathcal{T}_P^{(M+1)}(X)\right|^{-1} \ge \frac{1}{\exp\{K\} - 1}.$$

Then from (8) the following estimates take place:

$$\begin{aligned} \left|\overline{\mathcal{A}_1} \cap \mathcal{T}_P(X)\right| &= \frac{Pr(\overline{\mathcal{A}_1} \cap \mathcal{T}_P(X))}{Pr(\mathbf{x} \mid \mathbf{x} \in \mathcal{T}_P^{(M+1)}(X), w)} \le P^{*N}(\mathcal{T}_P(X)) \cdot (\exp\{K\} - 1) \le \\ &\le \exp\{-ND(P \parallel P^*)\} \cdot (\exp\{K\} - 1). \end{aligned}$$

Therefore for $P \ne P^*$ and N large enough

$$\begin{aligned} |\mathcal{A}_1 \cap \mathcal{T}_P(X)| &\ge \exp\{K\} - \exp\{-ND(P \parallel P^*)\} \cdot (\exp\{K\} - 1) \ge \\ &\ge \exp\{K\}(1 - \exp\{-ND(P \parallel P^*)\} + \exp\{-K - ND(P \parallel P^*)\}) \ge \exp\{K - 1\}. \end{aligned} \tag{17}$$

From (14), (15) and (17) we receive that (16) holds. Remark that from definition of $\mathcal{A}_1$ it follows that

$$\max_{\mathbf{x} \in \mathcal{A} \bigcap \mathcal{T}_P(X)} G_N(\mathbf{x} \mid w) = \max_{\mathbf{x} \in \mathcal{A}_1 \bigcap \mathcal{T}_P(X)} G_N(\mathbf{x} \mid w). \tag{18}$$

Hence it must be

$$L(N) \geq \max_{P \in \alpha(E)} \max_{\mathbf{x} \in \mathcal{A} \bigcap \mathcal{T}_P(X)} G_N(\mathbf{x} \mid w) \geq \exp\{K-2\}, \tag{19}$$

from where we can receive one of the estimates for R'' in (1).

Now for bounding of R we estimate

$$\begin{aligned} \mathrm{E}_{P^*,P_1^*}\{G_N(\mathbf{X} \mid w)\} &= \sum_{\mathbf{x} \in \mathcal{X}^N} \sum_{\mathbf{u} \in \mathcal{U}^K} P^{*N}(\mathbf{x}) P_1^{*K}(\mathbf{u}) G_N(\mathbf{x} \mid w) \geq \\ &\geq \sum_{P \in \alpha(E)} \sum_{\mathbf{x} \in \mathcal{T}_P(X)} \sum_{\mathbf{u} \in \mathcal{U}^K} P^{*N}(\mathbf{x}) P_1^{*K}(\mathbf{u}) G_N(\mathbf{x} \mid w) \geq \\ &\geq \max_{P \in \alpha(E)} \sum_{\mathbf{x} \in \mathcal{T}_P(X)} \sum_{\mathbf{u} \in \mathcal{U}^K} P^{*N}(\mathbf{x}) P_1^{*K}(\mathbf{u}) G_N(\mathbf{x} \mid w). \end{aligned} \tag{20}$$

Using (5) we continue the estimates (12)

$$\begin{aligned} \left|\overline{\mathcal{A}_1} \cap \mathcal{T}_P(X)\right| \leq \exp\{K - ND(P \parallel P^*)\} \leq |\mathcal{T}_P(X)| \exp\{ND(P \parallel P^*)\} \leq \\ \leq \exp\{N(H_P(X) - D(P \parallel P^*))\}. \end{aligned} \tag{21}$$

Therefore from (5) for N large enough

$$\begin{aligned} |\mathcal{A}_1 \cap \mathcal{T}_P(X)| &= |\mathcal{T}_P(X)| - \left|\overline{\mathcal{A}_1} \cap \mathcal{T}_P(X)\right| \geq \\ &\geq \exp\{NH_P(X)\} \left((N+1)^{-|\mathcal{X}|} - \exp\{-ND(P \parallel P^*)\}\right) = \\ &= (N+1)^{-|\mathcal{X}|} \exp\{NH_P(X)\} \left(1 - (N+1)^{|\mathcal{X}|} \exp\{-ND(P \parallel P^*)\}\right) \geq \\ &\geq \frac{1}{2}(N+1)^{-|\mathcal{X}|} \exp\{NH_P(X)\} \geq \exp\{N(H_P(X) - \varepsilon)\}. \end{aligned} \tag{22}$$

Taking into account (7), (17), (20) and (22) and definition of the set $\mathcal{A}_1$ we obtain

$$\mathrm{E}_{P^*,P_1^*}\{G_N(\mathbf{X} \mid w)\} \geq \max_{P \in \alpha(E)} \exp\{-N(D(P \parallel P^*) + H_P(X))\} \sum_{i=1}^{|\mathcal{A}_1 \bigcap \mathcal{T}_P(X)|} i \sum_{\mathbf{u} \in \mathcal{U}^K} P_1^{*K}(\mathbf{u}).$$

Using the properties of arithmetic progression and (13) we can continue estimation

$$
\begin{aligned}
&\mathrm{E}_{P^*,P_1^*}\{G_N(\mathbf{X} \mid w)\} \geq \\
&\geq \max_{P\in\alpha(E)} \exp\{-N(D(P\,\|\,P^*)+H_P(X))\}\frac{1+|\mathcal{A}_1\bigcap\mathcal{T}_P(X)|}{2}\cdot|\mathcal{A}_1\bigcap\mathcal{T}_P(X)|\geq \\
&\geq \max_{P\in\alpha(E)} \exp\{-N(D(P\,\|\,P^*)+H_P(X))\}\frac{|\mathcal{A}_1\bigcap\mathcal{T}_P(X)|^2}{2}\geq \\
&\geq \max_{P\in\alpha(E)} \exp\{-N(D(P\,\|\,P^*)+H_P(X))\}\exp\{K-2\}\exp\{N(H_P(X)-\varepsilon)\} = \\
&= \max_{P\in\alpha(E)} \exp\{-ND(P\,\|\,P^*)\}\exp\{K-2\}\exp\{-N\varepsilon\}\geq \\
&\geq \max_{P\in\alpha(E)} \exp\{N(-D(P\,\|\,P^*)+R'-2\varepsilon)\}.
\end{aligned}
\tag{23}
$$

Thus we receive one of the estimates for R in (2).

2) Now consider the case $\exp\{K\}\geq|\mathcal{T}_P(X)|$. In this case it is natural to use the following encryption function: $f(\mathbf{x},\mathbf{u})=(w_{b_1},w_{b_2})$, where the first $b_1=\lceil\log|\mathcal{P}(\mathcal{X},N)|\rceil$ bits (the bits of w_{b_1}) describe the index of the set $\mathcal{T}_P(X)$ containing $\mathbf{x}$, the last $b_2=\lceil\log|\mathcal{T}_P(X)|\rceil$ bits (the bits of w_{b_2}) are obtained after encryption by simple bit-by-bit XOR operation on the b_2 bits identifying the index of $\mathbf{x}$ within $\mathcal{T}_P(X)$ and on the bits of $\mathbf{u}$.

Then the conditional probability of w given $\mathbf{x}\in\mathcal{T}_P(X)$ is equal

$$
Pr(w \mid \mathbf{x}) = \begin{cases} \exp\{-\lceil\log|\mathcal{T}_P(X)|\rceil\}, & w\in\mathcal{W}(\mathbf{x}),\\ 0, & \text{elsewhere.}\end{cases}
$$

By analogy with (11) and using (5) we have

$$
Pr(\mathbf{x} \mid \mathbf{x}\in\mathcal{T}_P(X), w) = \left|\mathcal{W}^{-1}(w)\bigcap\mathcal{T}_P(X)\right|^{-1} = |\mathcal{T}_P(X)|^{-1}\geq\exp\{-NH_P(X)\}.
$$

Then for $P\in\alpha(E)$

$$
\left|\overline{\mathcal{A}}\bigcap\mathcal{T}_P(X)\right| = \frac{Pr(\overline{\mathcal{A}}\bigcap\mathcal{T}_P(X))}{Pr(\mathbf{x}\mid\mathbf{x}\in\mathcal{T}_P(X), w)} \leq \exp\{N(H_P(X)-E)\},
$$

therefore for sufficiently large N and $0<\varepsilon<E$ we can have the following lower estimate

$$
\begin{aligned}
&|\mathcal{A}\bigcap\mathcal{T}_P(X)|\geq(N+1)^{-|\mathcal{X}|}\exp\{NH_P(X)\}-\exp\{N(H_P(X)-E)\} = \\
&= \exp\{N(H_P(X)-\varepsilon)\}(\exp\{N\varepsilon\}\cdot(N+1)^{-|\mathcal{X}|}-\exp\{N(\varepsilon-E)\})\geq \\
&\geq \exp\{N(H_P(X)-\varepsilon)\}(2-\exp\{N(\varepsilon-E)\})\geq\exp\{N(H_P(X)-\varepsilon)\}.
\end{aligned}
\tag{24}
$$

Now we shall obtain upper estimate for $|\mathcal{A}\bigcap\mathcal{T}_P(X)|$. To each $\mathbf{x}\in\mathcal{A}\bigcap\mathcal{T}_P(X)$ an unique guessing vector $\hat{\mathbf{x}}_i(w)\in\mathcal{G}_N(w)$ corresponds, such that $G_N(\mathbf{x}\mid w)=i$. This vector determines a conditional type $Q=Q_P(\hat{x}(w)\mid x)$, for which $\hat{\mathbf{x}}_i(w)\in\mathcal{T}_{P,Q}(\hat{X}(w)\mid\mathbf{x})$. Remark that for the case $K \geq \log |\mathcal{T}_P(X)|$ (according to the definition of the constructed encryption function f) the wiretapper is informed only about the type $\mathcal{T}_P(X)$ of the source message $\mathbf{x}$. Therefore

$$Q = Q_P(\hat{x}(w) \mid x) = Q_P(\hat{x} \mid x) = Q_P \text{ and } \mathcal{T}_{P,Q}(\hat{X}(w) \mid \mathbf{x}) = \mathcal{T}_{P,Q_P}(\hat{X} \mid \mathbf{x}).$$

Since $\mathbf{x} \in \mathcal{A}$, then $\mathbf{E}_{P,Q_P} d(X, \hat{X}(w)) = d(\mathbf{x}, \hat{\mathbf{x}}_i(w)) \leq \Delta$. So, $Q_P \in \mathcal{M}(P, \Delta)$. The set of all vectors $\mathbf{x} \in \mathcal{A} \bigcap \mathcal{T}_P(X)$ is divided into classes corresponding these conditional types Q_P and is the union of all such Q_P - shells. Let us select $Q_P = \Phi(P)$ - shell having maximal cardinality for given P and denote it by $(\mathcal{A} \bigcap \mathcal{T}_P(X))\,(\Phi(P))$. Using (4) we have for N large enough

$$\begin{aligned} |\mathcal{A} \bigcap \mathcal{T}_P(X)| &\leq (N+1)^{|\mathcal{X}||\hat{\mathcal{X}}|}\, |(\mathcal{A} \bigcap \mathcal{T}_P(X))\,(\Phi(P))| \leq \\ &\leq \exp\{N\varepsilon\}\, |(\mathcal{A} \bigcap \mathcal{T}_P(X))\,(\Phi(P))|. \end{aligned} \tag{25}$$

Let $\mathcal{C}(P, \Phi(P), \mathcal{A})$ be the set of all guessing vectors $\hat{\mathbf{x}}_i(w) \in \mathcal{G}_N(w)$, which satisfy $G_N(\mathbf{x} \mid w) = i$ for some $\mathbf{x} \in \mathcal{A} \bigcap \mathcal{T}_P(X)$, $\mathbf{x} \in \mathcal{T}_{P,\Phi(P)}(X \mid \hat{\mathbf{x}}_i(w))$. In accordance with the definition of the guessing strategy $\mathcal{G}_N(w)$

$$|\mathcal{C}(P, \Phi(P), \mathcal{A})| \leq \max_{\mathbf{x} \in \mathcal{A} \bigcap \mathcal{T}_P(X)} G_N(\mathbf{x} \mid w).$$

Then

$$\left|\left((\mathcal{A} \bigcap \mathcal{T}_P(X)\right)(\Phi(P))\right| \leq \sum_{\hat{\mathbf{x}} \in \mathcal{C}(P, \Phi(P), \mathcal{A})} \left|\mathcal{T}_{P,\Phi(P)}(X \mid \hat{\mathbf{x}}(w))\right| \leq$$

$$\leq \exp\{N H_{P,\Phi(P)}(X \mid \hat{X})\} \cdot \max_{\mathbf{x} \in \mathcal{A} \bigcap \mathcal{T}_P(X)} G_N(\mathbf{x} \mid w).$$

From the last inequality, (24) and (25) we obtain that for $P \in \alpha(E)$

$$\max_{\mathbf{x} \in \mathcal{A} \bigcap \mathcal{T}_P(X)} G_N(\mathbf{x} \mid w) \geq \exp\{N(I_{P,\Phi(P)}(X \wedge \hat{X}) - 2\varepsilon)\}. \tag{26}$$

Hence the estimate of the number of guesses $L(N)$ must be

$$L(N) \geq \exp\{N(R(P^*, E, \Delta) - 2\varepsilon)\}. \tag{27}$$

Using (8) we receive (21):

$$\left|\overline{\mathcal{A}_1} \bigcap \mathcal{T}_P(X)\right| = \frac{Pr(\overline{\mathcal{A}_1} \bigcap \mathcal{T}_P(X))}{Pr(\mathbf{x} \mid \mathbf{x} \in \mathcal{T}_P(X), w)} \leq \frac{P^{*N}(\mathcal{T}_P(X))}{\exp\{-NH_P(X)\}} \leq$$

$$\leq \exp\{N(H_P(X) - D(P \parallel P^*))\},$$

hence (22) too. Remark that

$$\left|\mathcal{A}_1 \bigcap \mathcal{T}_P(X)\right| \leq |\mathcal{T}_P(X)| \leq \exp\{NH_P(X)\}. \tag{28}$$

Using (7), (18), (20), (22), (26), (28) and definition of the set $\mathcal{A}_1$ we obtain

$$\mathrm{E}_{P^*,P_1^*}\{G_N(\mathbf{X}\mid w)\} \geq \max_{P\in\alpha(E)} \sum_{\mathbf{x}\in\mathcal{A}_1\bigcap\mathcal{T}_P(X)} P^{*N}(\mathbf{x}) \sum_{\mathbf{u}\in\mathcal{U}^K} P_1^{*K}(\mathbf{u})G_N(\mathbf{x}\mid w) \geq$$

$$\geq \max_{P\in\alpha(E)} \exp\{-N(D(P\parallel P^*)+H_P(X))\}\left(\max_{\mathbf{x}\in\mathcal{A}_1\bigcap\mathcal{T}_P(X)} G_N(\mathbf{x}\mid w) + \sum_{i=1}^{|\mathcal{A}_1\bigcap\mathcal{T}_P(X)|-1} i\right) \geq$$

$$\geq \max_{P\in\alpha(E)} (\exp\{-N(D(P\parallel P^*)+H_P(X))\}\cdot$$

$$\cdot(\exp\{N(I_{P,\Phi(P)}(X\wedge\hat{X})-2\varepsilon)\}+(|\mathcal{A}_1\cap\mathcal{T}_P(X)|^2-|\mathcal{A}_1\cap\mathcal{T}_P(X)|)/2)) \geq$$

$$\geq \max_{P\in\alpha(E)} (\exp\{-N(D(P\parallel P^*)+H_P(X))\}\cdot$$

$$\cdot(\exp\{N(I_{P,\Phi(P)}(X\wedge\hat{X})-2\varepsilon)\}+\exp\{2N(H_P(X)-\varepsilon)-1\}-\exp\{NH_P(X)-1\})) \geq$$

$$\geq \max_{P\in\alpha(E)} \left(\exp\{N(-D(P\parallel P^*)+I_{P,\Phi(P)}(X\wedge\hat{X})-2\varepsilon)\}\cdot\right.$$

$$\cdot(\exp\{-NH_P(X)\}+\exp\{N(H_{P,\Phi(P)}(X\mid\hat{X})-\varepsilon)\}-\exp\{-N(I_{P,\Phi(P)}(X\wedge\hat{X})-\varepsilon)\}) \geq$$

$$\geq \max_{P\in\alpha(E)} \exp\{N(-D(P\parallel P^*)+I_{P,\Phi(P)}(X\wedge\hat{X})-2\varepsilon)\}. \tag{29}$$

Therefore uniting the both cases, from (19) and (27) we receive

$$L(N) \geq \exp\{\min(K-2, N(R(P^*,E,\Delta)-2\varepsilon))\},$$

from (23) and (29) we obtain

$$\mathrm{E}_{P^*,P_1^*}\{G_N(\mathbf{X}\mid w)\} \geq \max_{P\in\alpha(E)} \exp\{N(-D(P\parallel P^*)+\min(R'-2\varepsilon, I_{P,\Phi(P)}(X\wedge\hat{X})-2\varepsilon))\}.$$

Hence for N large enough

$$R'' \geq \frac{1}{N}\log L(N)-\varepsilon \geq \min(R'-\varepsilon, R(P^*,E,\Delta)-3\varepsilon),$$

$$R \geq \frac{1}{N}\log \mathrm{E}_{P^*,P_1^*}\{G_N(\mathbf{X}\mid w)\}-\varepsilon \geq$$

$$\geq \max_{P\in\alpha(E)}(-D(P\parallel P^*)+\min(R'-2\varepsilon, R(P,\Delta)-2\varepsilon))-\varepsilon.$$

Taking into account arbitrariness of ε, continuity by E of all functions in above expressions, we obtain (1) and (2), therefore the proof of the inclusion (10) is completed.

References

[1] R. Ahlswede, "Coloring hypergraphs. A new approach to multi-user source coding", I, *J. Combin. Inform. and Syst. Sci.*, vol. 4, no. 1, pp. 75-115, 1979.

[2] R. Ahlswede, "Coloring hypergraphs. A new approach to multi-user source coding", II, *J. Combin. Inform. and Syst. Sci.*, vol. 5, no. 2, pp. 220-268, 1980.

[3] E. Arikan, "On the average number of guesses required to determine the value of a random variable", *Proceedings of the 12-th Prague Conference on Information Theory, Statistical Decision Functions and Random Processes* (Prague, the Czech Republic, 1994), pp. 20-23.

[4] E. Arikan, "An inequality on guessing and its application to sequential decoding", *IEEE Trans. Inform. Theory*, vol. 42, no. 1, pp. 99-105, 1996.

[5] E. Arikan and N. Merhav, "Joint source-channel coding and guessing", *Proceedings of the 1997 IEEE International Symposium on Information Theory* (Ulm, Germany, 1997), p. 162.

[6] E. Arikan and N. Merhav, "Guessing subject to distortion", *IEEE Trans. Inform. Theory*, vol. 44, no. 3, pp. 1041-1056, 1998.

[7] E. Arikan and N. Merhav, "Joint source-channel coding and guessing with application to sequential decoding", *IEEE Trans. Inform. Theory*, vol. 44, no. 5, pp. 1756-1769, 1998.

[8] T. Berger, *Rate Distortion Theory: A Mathematical Basis for Data Compression*, Englewoods Cliffs, NJ: Prentice-Hall, 1971.

[9] S. Boztas, "Comments on "An inequality on guessing and its application to sequential decoding"", *IEEE Trans. Inform. Theory*, vol. 43, no. 6, pp. 2062-2063, 1997.

[10] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, New York: Wiley, 1991.

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

[12] I. Csiszár, "The method of types", *IEEE Trans. Inform. Theory*, vol. 44, no. 6, pp. 2505-2523, 1998.

[13] A. R. Ghazaryan, "Multiterminal sources optimal coding rates depending on levels of reliability, distortion and secrecy", Candidate of Science thesis (in Russian), Institute for Informatics and Automation Problems of the NAS of RA and of the YSU, 1999.

[14] E. A. Haroutunian, A. R. Ghazaryan, "Guessing subject to distortion and reliability criteria", *Transactions of the Institute for Informatics and Automation Problems of the NAS of RA and of the Yerevan State University, Mathematical problems of computer science*, vol. 21, pp. 83-90, 2000.

[15] E. A. Haroutunian, A. N. Harutyunyan, A. R. Ghazaryan, E. C. van der Meulen, "On the rates-reliability-distortions region of a one-stage branching system with wiretappers", *Proceedings of 2000 Cornell Summer Workshop on Information Theory* (Cornell University, Ithaca NY, 2000), p. 12.

[16] E. A. Haroutunian, A. N. Harutyunyan, A. R. Ghazaryan, E. C. van der Meulen, "On branching communication system rates-reliability-distortions region with partial secrecy under distortion criterion", *Transactions of the Institute for Informatics and Automation Problems of the NAS of RA and of the Yerevan State University, Mathematical problems of computer science*, vol. 21, pp. 61-76, 2000.

[17] E. A. Haroutunian, A. N. Harutyunyan, A. R. Ghazaryan, "On rate-reliability-distortion function for a robust descriptions system", *IEEE Trans. Inform. Theory*, vol. 46, no. 7, pp. 2690-2697, 2000.

[18] E. A. Haroutunian and B. Mekoush, "Estimates of optimal rates of codes with given error probability exponent for certain sources" (in Russian), *Abstracts of Papers, Sixth International Symposium on Information Theory* (Tashkent, USSR, 1984), vol. 1, pp. 22-23.

[19] E. A. Haroutunian and R. Sh. Maroutian, "(E, Δ)-achievable rates for multiple descriptions of random varying source", *Problems of Control and Inform. Theory*, vol. 20, no. 2, pp. 165-178, 1991.

[20] J. L. Massey, "Guessing and entropy", *Proceedings of the 1994 IEEE International Simposium on Information Theory* (Trondheim, Norway, 1994), p. 204.

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

[22] E. C. van der Meulen, E. A. Haroutunian, A. N. Harutyunyan, A. R. Ghazaryan, "On the rates-reliability-distortions and partial secrecy region of a one-stage branching communication system", *Proceedings of the 2000 IEEE International Simposium on Information Theory* (Sorrento, Italy, 2000), p. 211.

[23] H. Yamamoto, "Rate-distortion theory for the Shannon cipher system", *IEEE Trans. Inform. Theory*, vol. 43, no. 3, pp. 827-835, 1997.

Կռահումն ըստ շեղման և հուսալիության չափանիշների Շենոնի ծածկագրման համակարգի համար

Ե. Ա. Հարությունյան, Ա. Ռ. Ղազարյան

Ամփոփում

Լուծվում է դիսկրետ առանց հիշողության աղբյուրի հաղորդագրությունների տրված շեղման և հուսալիության մակարդակի սահմաններում կռահման խնդիրը Շենոնի ծածկագրման համակարգի համար: Գաղտնիությունը չափվում է աղբյուրի ծածկագրի հիման վրա կատարվող հակառակորդի հաղորդագրությունների վերականգնման գուշակումների միջին թվով: Ի հավելումն Մերհավի և Արիկանի կողմից դիտարկված խնդրի, աշխատանքում դիտարկվում են շեղման և հուսալիության լրացուցիչ պայմանները:

Բանալու արագության համար որոշված է շեղման և հուսալիության պահանջվող մակարդակները ապահովող կռահման փորձերի փոքրագույն (ըստ բոլոր գուշակման ցուցակների) և մեծագույն (ըստ բոլոր ծածկագրման ֆունկցիաների) թվի համապատասխան կռահումների սպասելի արժեքը: