On the Shannon Cipher System with Distortion and Guessing Wiretapper Eavesdropping through a Noisy Channel

Tigran Margaryan
Institute for Informatics and Automation
Problems of NAS of RA, Yerevan, Armenia
e-mail: tigran.ipia.sci.am

Evgueni Haroutunian
Institute for Informatics and Automation
Problems of NAS of RA, Yerevan, Armenia

ABSTRACT

We investigated the Shannon cipher system with discrete memoryless source and noisy channel to the wiretapper. The wiretapper gains the noisy version of the cryptogram and tries to guess encrypted plaintext given some exactness. In each step of sequential guesses the wiretapper has a testing mechanism. The security level of the encryption system is measured by the expected number of wiretapper's guesses. The upper and lower bounds are obtained for the guessing rate.

Keywords

Shannon cipher system, guessing, wiretap channel.

1. INTRODUCTION

The guessing as a computational secrecy for Shannon cipher system (SCS) was introduced by Merhav and Arikan [1], [2].The SCS with distortion and reliability requirements was solved by Haroutunian and Ghazaryan [3], [4]. The SCS with correlated source outputs was studied by Hayashi and Yamamoto [5] and with general sources was studied by Hanawal and Sundaresan [6]. We considered the SCS with a noisy channel to the wiretapper [7]. For using some techiques we also refer to these two papers: Arikan and Merhav's work [8] is dedicated to the guessing subject to distortion and Yamamoto and Okudra's work [9] regards the channel coding theorem for the number of guesses in decoding. In this paper we investigate the combined model of the SCS considered in the papers [3] and [7]. The cryptographic system depicted in Fig. 1. is the SCS with a noisy channel to the wiretapper.

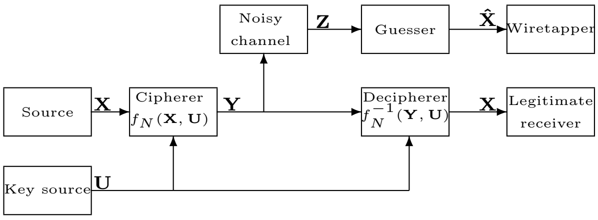

Fig. 1. The Shannon cipher system with a noisy channel.

The memoryless stationary source generates a message which after ciphering is transmitted to legitimate receiver via a public channel. To encrypt the plaintext encipherer applies the key-vector generated by memoryless stationary key-source. The key-vector is also communicated to decipherer by an extra secure channel secured against adversaries. The legitimate receiver can recover the original plaintext using the cryptogram and the key. The wiretapper eavesdropping on the noisy channel gains a noisy version of cryptogram and tries to guess the plaintext on degree of exactness without knowing the key. It is assumed that the wiretapper knows the source and channel distributions and encryption functions. The wiretapper tries to reconstruct source messages within the given some distortion measure and distortion level. For approximative reconstruction of secret information the wiretapper makes sequential guesses, each time applying a testing mechanism by which he can know whether the estimate is successful or not and stops it when the answer is affirmative. The security level of this system is measured by the expected number of the wiretapper's guesses needed before succeeding.Our goal is to estimate the expectation of the number of guesses that the wiretapper may have to submit before succeeding.

2. SYSTEM MODEL AND DEFINITIONS

We denote the RV by capital letters, the random vector by bold capital letters, and their realizations are denoted in lower-case letters, respectively. In the system shown in Fig. 1. the source, key-source and channel are stationary and memoryless. The source is assumed to generate random vector $\mathbf{X}$ which consists of discrete, independent, identically distributed (i.i.d.) random variables (RVs) $(X_1, X_2, \dots, X_N)$. The secret $\mathbf{X}$ should be sent to a legitimate receiver. The RV X taking values in finite set $\mathcal{X}$ has a probability distribution (PD) $P^* = \{P^*(x), x \in \mathcal{X}\}$. The key-source generates the random vector $\mathbf{U} = (U_1, U_2, \dots, U_K)$ of K purely random bits independent of $\mathbf{X}$. The key $\mathbf{U}$ which is used for enciphering also must be sent to the decipherer by an extra secure channel. The random vector $\mathbf{X}$ is encrypted using the key $\mathbf{U}$ by the encryption function $f_N : \mathcal{X}^N \times \mathcal{U}^K \to \mathcal{Y}^M$ where $\mathcal{Y}$ is the cryptogram alphabet and M/N is supposed to be equal to a constant λ. After ciphering, the obtained random vector $\mathbf{Y}$ of length M is dispatched via a public channel to a legitimate receiver. This encryption function is assumed to be invertible providing the key is given, i.e. there exists a decryption function $f_N^{-1} : \mathcal{Y}^M \times \mathcal{U}^K \to \mathcal{X}^N$ which allows the legitimate receiver to recover the original $\mathbf{X}$. A random vector $\mathbf{Y}$=$(Y_1, Y_2, \dots, Y_M)$ depends on the source and encryption function and PD of random vector $\mathbf{Y}$ was determined by a vector with size $|\mathcal{Y}|^M$. In the noiseless version of SCS a wiretapper does not need for PD of cryptograms, but in this case the wiretapper must compute PD of random vector $\mathbf{Y}$ for the sake of making a better guess. In theory knowing P^* the wiretapper and f_N can count PD of random vector for each N , but in practice such computation as well as storage of information for large N is a very complicated task.

The wiretapper assumes that the cryptogram $\mathbf{Y}$ consists in i.i.d. RVs and the RV Y has PD $S = \{S(y), y \in$

$\mathcal{Y}\}$ which the wiretapper computes by the statistics of cryptograms. The wiretapper gets a cryptogram through a noisy discrete memoryless channel (DMC) with the input alphabet $\mathcal{Y}$, the output alphabet $\mathcal{Z}$ and with a stochastic matrix of transition probabilities $W^* = \{W^*(z|y), y \in \mathcal{Y}, z \in \mathcal{Z}\}$. The joint PD of RVs Y and Z is $S \circ W^* = \{S \circ W^*(z,y) = S(y)W^*(z|y), y \in \mathcal{Y}, z \in \mathcal{Z}\}$ and PD of RV Z is $SW^* = \{SW^*(z) = \sum\limits_{y\in\mathcal{Y}} S(y)W^*(z|y), z \in \mathcal{Z}\}$. The conditional probability of $y \in \mathcal{Y}$ for the given $z \in \mathcal{Z}$ is the following $\widehat{W}{=}S{\circ}W^*/SW^* = \{\widehat{W}(y|z) = S{\circ}W^*(z,y)/SW^*(z), y \in \mathcal{Y}, z \in \mathcal{Z}\}$.

In this task it is allowed for wiretapper to guess the original 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 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 source and wiretapper reproduction messages: $d : \mathcal{X} \times \hat{\mathcal{X}} \to [0;\infty)$. The distortion measure between a source vector $\mathbf{x} \in \mathcal{X}^N$ 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 an average of the component distortions:

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

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 message $\hat{}\mathbf{x}$ is found. We say that the guessing strategy is Δ-achievable if there exists some j such that $P\,r\{d(\mathbf{X}, \hat{}\mathbf{x}_j\,(\mathbf{z})) \leq N\Delta\} = 1$. Let $G_{f\,g}(\mathbf{X}\hat{}\;|\overset{N}{\mathbf{Z}})$ be a num- ber 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 $R(R_K, \Delta, P^*, W^*)$ of this system is defined by $R(R_K, \Delta, P^*, W^*) = \lim\limits_{N\to\infty} \sup\limits_{f_N} \inf\limits_{g_N} \frac{1}{N} \log E[G^N_{f,g}(\hat{\mathbf{X}}|\mathbf{Z})]$,

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

We apply the method of types and covering lemma ([10], [11], [12]). The type P of vector $\mathbf{x} = (x_1, \ldots, x_N) \in \mathcal{X}^N$ 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 the symbol x among $x_1, \ldots, x_N$. The set of vectors $\mathbf{x}$ of type P is denoted by $\mathcal{T}^N_P(X)$. The set of all PD on $\mathcal{X}$ is denoted by $\mathcal{P}(\mathcal{X})$ and the subset of $\mathcal{P}(\mathcal{X})$ consisting of the possible types of sequences $\mathbf{x} \in \mathcal{X}^N$ is denoted by $\mathcal{P}_N(\mathcal{X})$.

We denote entropy of RV X with PD P and, respectively, divergence of PD P^* from P as follows:

$$H_P(X) \overset{\triangle}{=} -\sum_{x\in\mathcal{X}} P(x) \log P(x),$$

$$D(P||P^*) \overset{\triangle}{=} \sum_{x\in\mathcal{X}} P(x) \log \frac{P(x)}{P^*(x)}.$$

The type of vector $\mathbf{z}$ is denoted by Q, and the set of vectors $\mathbf{z}$ of type Q is denoted by $\mathcal{T}^M_Q(Z)$.

The joint type of vector $\mathbf{y} \in \mathcal{Y}^M$ 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 $\mathbf{y}$ for the given $\mathbf{z}$ is PD $W = \{W(y|z),\ z \in \mathcal{Z},\ y \in \mathcal{Y}\}$ if $M(z,y|\mathbf{z},\mathbf{y}) = M(z|\mathbf{z})W(y|z)$ for all $z \in \mathcal{Z}$, $y \in \mathcal{Y}$. The set of all sequences $\mathbf{y} \in \mathcal{Y}^M$ of the conditional type W for the given $\mathbf{z} \in \mathcal{T}^M_Q(Z)$ is denoted by $\mathcal{T}^M_{Q,W}(Y|\mathbf{z})$ and called the W-shell of $\mathbf{z}$. $\mathcal{W}_M(\mathcal{Y}, Q)$ is the set of all possible W-shells of $\mathbf{z}$ of type Q .

For the given PDs Q and $\widehat{Q}$ of Z and conditional PDs W and $\widehat{W}$ of Y for the given Z conditional entropy of RV Y for the given RV Z is defined by

$$H_{Q,W}(Y|Z) \overset{\triangle}{=} -\sum_{z\in\mathcal{Z},y\in\mathcal{Y}} QW(y) \log W(y|z),$$

the conditional divergence of joint PD $Q \circ W$ from joint PD $Q \circ \widehat{W}$ is defined by

$$D(Q \circ W \| Q \circ \widehat{W}) = D(W \| \widehat{W}|Q)$$

$$\overset{\triangle}{=} \sum_{z\in\mathcal{Z},y\in\mathcal{Y}} Q(z)W(y|z) \log \frac{W(y|z)}{\widehat{W}(y|z)}$$

and the divergence of the joint PD $Q \circ W$ from the joint PD $\widehat{Q} \circ \widehat{W}$ is defined by

$$D(Q \circ W \| \widehat{Q} \circ \widehat{W}) = D(Q \| \widehat{Q}) + D(W \| \widehat{W}|Q)$$

$$\overset{\triangle}{=} \sum_{z\in\mathcal{Z},y\in\mathcal{Y}} Q(z)W(y|z) \log \frac{Q(z)W(y|z)}{\widehat{Q}(z)\widehat{W}(y|z)}.$$

We will use the following inequalities, concerting the types ([10], [11]).

$$|\mathcal{P}_N(\mathcal{X})| < (N+1)^{|\mathcal{X}|}, \qquad (1)$$

$$|\mathcal{W}_M(\mathcal{Y}, Q)| < (M+1)^{|\mathcal{Z}||\mathcal{Y}|}, \qquad (2)$$

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

$$|\mathcal{T}^N_P(X)| \leq \exp\{NH_P(X)\}, \qquad (3)$$

for any PD P^*

$$P^{*N}\{\mathcal{T}^N_P(X)\} \leq \exp\{-ND(P\|P^*)\}, \qquad (4)$$

for any type Q , conditional type W and $\mathbf{z} \in \mathcal{T}^M_Q(Z)$

$$|\mathcal{T}^M_{Q,W}(Y|\mathbf{z})| \leq \exp\{MH_{Q,W}(Y|Z)\}, \qquad (5)$$

and for any joint type $Q \circ W$ and joint PD $\widehat{Q} \circ \widehat{W}$ on $(\mathcal{Y} \times \mathcal{Z})^M$

$$\widehat{Q} \circ \widehat{W}^M\{\mathcal{T}^M_{Q,W}(Y|Z)\} \leq \exp\{-MD(Q \circ W \| \widehat{Q} \circ \widehat{W})\}. \qquad (6)$$

Let $P = \{P(x), x \in \mathcal{X}\}$ be a PD on $\mathcal{X}$ and let $V = \{V(\hat{x} \mid x),\ x \in \mathcal{X},\ \hat{x} \in \hat{\mathcal{X}}\}$ be a conditional PD on $\hat{\mathcal{X}}$ for given x, also we denote by $PV = \{PV(\hat{x}) = \sum\limits_x P(x)V(\hat{x} \mid x),\ \hat{x} \in \hat{\mathcal{X}}\}$ the marginal PD on $\hat{\mathcal{X}}$.

For RVs X and $\hat{X}$, the mutual information between X and $\hat{X}$ is defined as

$$I_{P,V}(X \wedge \hat{X}) = \sum_{x,\hat{x}} P(x)V(\hat{x} \mid x) \log \frac{V(\hat{x} \mid x)}{\sum\limits_x P(x)V(\hat{x} \mid x)}.$$

Denote by $V(P, \Delta)$ (below for brevity we shall just write V) a function, which puts into the correspondence to the PD P the conditional PD V such that for given Δ the following condition is implemented:

$$E_{P,V}\, d(X, \hat{X}) = \sum_x P(x)\, V(\hat{x} \mid x) d(x, \hat{x}) \leq \Delta.$$

Let $\mathcal{V}(P, \Delta)$ be the set of all functions V for given Δ and P.

$R(P,\Delta)$ is the notation of the rate-distortion function for the PD P and Δ and is equal to (see [10]):

$$R(P,\Delta) = \min_{V \in \mathcal{V}(P,\Delta)} I_{P,V}(X \wedge \hat{X}). \tag{7}$$

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

The proof of the theorem is based on the above mentioned inequalities and the following random coding lemma about covering of types of vectors , which is a modification of the covering lemmas from [10]:

Lemma: For every type P and conditional type V, there exists a collection of vectors

$$\{\hat{\mathbf{x}}_l \in \mathcal{T}^N_{PV}(\hat{X}),\ l = 1, ..., L(P,V,N)\},$$

such that the family

$$\{\mathcal{T}^N_{P,V}(X \mid \hat{\mathbf{x}}_l),\ l = 1, ..., L(P,V,N)\}$$

covers $\mathcal{T}^N_P(X)$, i. e.

$$\mathcal{T}^N_P(X) = \bigcup_{l=1}^{L(P,V,N)} \mathcal{T}^N_{P,V}(X \mid \hat{\mathbf{x}}_l).$$

where

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

We also use the following notations

$$h(P,\Delta,Q,W,R_K) = \min\{R(P,\Delta), \lambda H_{Q,W}(Y|Z) + R_K\}$$

and

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

3. FORMULATION OF THE RESULT

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

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

$$R(R_K,\Delta,P^*,W^*) \leq \max_S \max_{P,Q,W} [h(P,\Delta,Q,W,R_K) \\ -D(P||P^*) - \lambda D(Q \circ W \| S \circ W^*)],$$

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

Corollary: When the wiretapper's channel is noiseless we arrive at the result of Haroutunian [4] if the reliability function goes to infinity:

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

Corollary: When $\Delta = 0$ we arrive at our result from [7]:

$$R(R_K,P^*,W^*) \leq \max_S \max_{P,Q,W} [\min\{H_P(X), \lambda H_{Q,W}(Y|Z) \\ + R_K\} - D(P||P^*) - \lambda D(Q \circ W \| S \circ W^*)],$$

$$R(R_K,P^*,W^*) \geq \max_P [\min\{H_P(X), R_K\} - D(P||P^*)].$$

Corollary: When the wiretapper's channel is noiseless and $\Delta = 0$ we get the result of Merhav and Arikan from [1]:

$$R(R_K,P^*) = \max_P [\min\{H_P(X), R_K\} - D(P||P^*)].$$

4. PROOF OF THEOREM

Let the vector $\mathbf{x}$ generated by the source have the type P $(\mathbf{x} \in \mathcal{T}_P{}^N(X))$, wiretapper receive vector $\mathbf{z}$ of type Q ($\mathbf{z}$ $\in \mathcal{T}_Q{}^M(Z)$) and our cryptogram belong to W-shell of vector $\mathbf{z}$ ($\mathbf{y} \in \mathcal{T}^M{}_{Q,W}(Y|\mathbf{z})$). 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

$$\mathcal{X}^N = \bigcup_{i=1,2,\cdots,|\mathcal{P}_N(\mathcal{X})|} \mathcal{T}^N_{P_i}(X).$$

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 P tries to find some $\hat{\mathbf{x}}$ in each type so that $d(\mathbf{x}, \hat{\mathbf{x}} \leq N\Delta)$.

We consider a guessing strategy that enumerates the types P from according to nondecreasing values of corresponding rate-distortion functions $R(P_i,\Delta)$ (for simplicity of formula writing we shall note only i in $R(i,\Delta)$, $\mathcal{T}_i{}^N(X)$ instead of P_i and so on): $R(1,\Delta) \leq R(2,\Delta) \leq \ldots$. Taking into account our notation we can write

$$L(i,V_i^{\min},N) = \exp\{N(\min_{V_i \in \mathcal{V}(i,\Delta)} I_{i,V_i}(X \wedge \hat{X}) + o(N))\} \\ = \exp\{N(R(i,\Delta) + o(N))\} \tag{8}$$

For fixed i let the set $\{\hat{\mathbf{x}}_{i,l} \in \mathcal{T}^N_{P_i V_i^{\min}}(\hat{X}),\ l = 1, ...$ $, L(i,V_i^{\min},N)\}$ be such a collection of vectors (regardless of arrangement) that according to the lemma

$$\{\mathcal{T}^N_{i,V_i^{\min}}(X \mid \hat{\mathbf{x}}_{i,l}),\ l = 1, ..., L(i,V_i^{\min},N)\},$$

covers $\mathcal{T}_i{}^N(X)$. Ignoring the cryptogram $\mathbf{z}$ the wiretapper constructs the following sub-strategy in the above mentioned consequence : $g_1{}^N = \{\{\hat{\mathbf{x}}_{1,m},\ m = 1, ..., L(1,V_1^{\min},N)\}, \{\hat{\mathbf{x}}_{2,l},\ l = 1, ..., L(2,V_2^{\min},N)\}, \ldots\}$. The vector $\mathbf{x}$ belongs to $\mathcal{T}^N_P(X)$ and, therefore, it is clear that in this strategy g_1^N the number of guesses is bounded with (1) and (8) in the following way

$$G^N_{f,g_1}(\hat{\mathbf{x}}|\mathbf{z}) \leq \sum_{i:R(i,\Delta)\leq R(P,\Delta)} L(i,V_i^{\min},N) \\ \leq \quad (N+1)^{|\mathcal{X}|} \exp\{N(R(P,\Delta) + o(N))\} \\ \leq \quad \exp\{N(R(P,\Delta) + o(N))\} \tag{9}$$

Strategy $g_2{}^N$ *:* The set $\mathcal{Y}^M$ can be represented as the union of vectors of various conditional types for the given vector $\mathbf{z} \in \mathcal{T}_Q{}^M(Z)$ (these conditional types we arrange in ascending order of conditional entropy: $H_{Q,W_1}(Y|Z) \leq H_{Q,W_2}(Y|Z) \leq \cdots$)

$$\mathcal{Y}^M = \bigcup_{j=1,2,\cdots,|\mathcal{V}_M(\mathcal{Y},Q)|} \mathcal{T}^M_{Q,V_j}(Y|\mathbf{z}).$$

In this strategy, the wiretapper aims to find the message $\mathbf{x}$ (luck improves if finds some $\hat{\mathbf{x}}$) sequentially applying different keys on cryptograms $\mathbf{y}$ in ascending order of conditional entropy for the given vector $\mathbf{z}$. To find some vector $\hat{\mathbf{x}}$ wiretapper finds the key $\mathbf{u}$ and the cryptogram $\mathbf{y}$ which belongs to the W-shell of vector $\mathbf{z}$ ($\mathbf{y} \in \mathcal{T}^M_{Q,W}(Y|\mathbf{z})$), so in this strategy

$$g_2^N = \{f^{-1}(\mathbf{y}_1,\mathbf{u}_1), f^{-1}(\mathbf{y}_1,\mathbf{u}_2) \cdots f^{-1}(\mathbf{y}_1,\mathbf{u}_{\exp\{K\}}), \\ f^{-1}(\mathbf{y}_2,\mathbf{u}_1), f^{-1}(\mathbf{y}_2,\mathbf{u}_2) \cdots\},$$

the number of guesses by (2), (5) is bounded

$$G^N_{f,g_2}(\mathbf{x}|\mathbf{z}) \leq \sum_{W_j:H_{Q,W_j}(Y|Z)\leq H_{Q,W}(Y|Z)} |\mathcal{T}^M_{Q,W_j}(Y|\mathbf{z})| \exp\{K\}$$

$$\begin{aligned}&\leq (M+1)^{|\mathcal{Z}||\mathcal{Y}|}\exp\{MH_{Q,W}(Y|Z)+NR_K\}\\&\leq \exp\{MH_{Q,W}(Y|Z)+o(M)+NR_K\}\\&\leq \exp\{N(\lambda H_{Q,W}(Y|Z)+R_K)+o(N)\}. \qquad (10)\end{aligned}$$

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

$$g_3^N = (\mathbf{x}_{1,1}, f^{-1}(\mathbf{y}_1,\mathbf{u}_1), \mathbf{x}_{1,2}, f^{-1}(\mathbf{y}_1,\mathbf{u}_2)\cdots).$$

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. Therefore, we have as can be seen (9) and (10)

$$\begin{aligned}G^N_{f,g_3}(\hat{\mathbf{x}}|\mathbf{z}) &\leq 2\min[\exp\{NR(P,\Delta)+o(N)\},\\&\qquad \exp\{N(\lambda H_{Q,W}(Y|Z)+R_K)+o(N)\}]\\&\leq \exp\{Nh(P,\Delta,Q,W,R_K)+o(N)\}. \qquad (11)\end{aligned}$$

The expectation $E[G^N_{f\,g_3}(\hat{\mathbf{X}}|\mathbf{Z})]$ can be calculated in the following way:

$$\begin{aligned}E[G^N_{f,g_3}(\hat{\mathbf{X}}|\mathbf{Z})] &= \sum_{\mathbf{z}\in\mathcal{Z}^M} SW^{*M}(\mathbf{z})E[G^N_{f,g_3}(\hat{\mathbf{X}}|\mathbf{z})]\\&= \sum_{(\mathbf{y},\mathbf{z})\in(\mathcal{Y}\times\mathcal{Z})^M} S\circ W^{*M}(\mathbf{y},\mathbf{z})E[G^N_{f,g_3}(\hat{\mathbf{X}}|\mathbf{z})]\\&= \sum_{(\mathbf{y},\mathbf{z})\in(\mathcal{Y}\times\mathcal{Z})^M} S\circ W^{*M}(\mathbf{y},\mathbf{z})\\&\times \sum_{\hat{\mathbf{x}}\in\mathcal{X}^N} Pr\{\hat{\mathbf{x}}|\mathbf{z}\}G^N_{f,g_3}(\hat{\mathbf{x}}|\mathbf{z}).\end{aligned}$$

Applying inequalities (1), (2), (4), (6), (11) and taking into consideration that the expectation of $G_f{}^N{}_{,g_3}(\mathbf{X}\hat{}\ |\mathbf{Z})$ is maximum when random vectors $\mathbf{Z}$ and $\mathbf{X}$ are independent we obtain

$$\begin{aligned}E[G^N_{f,g_3}(\hat{\mathbf{X}}|\mathbf{Z})] &\leq \sum_{Q\circ W\in\mathcal{Q}\circ\mathcal{W}_M(\mathcal{Y},\mathcal{Z})} S\circ W^{*M}(\mathcal{T}^M_{Q\circ W}(Y,Z))\\&\times \sum_{P\in\mathcal{P}_N(\mathcal{X})} P^{*N}(\mathcal{T}^N_P(X))G^N_{f,g_3}(\hat{\mathbf{x}}|\mathbf{z})\\&\leq \max_{P,Q,W}[(N+1)^{|\mathcal{X}|}(M+1)^{|\mathcal{Z}||\mathcal{Y}|+|\mathcal{Z}|}\\&\times\exp\{-MD(Q\circ W\|S\circ W^*)\}\\&\times\exp\{-ND(P\|P^*)\}G^N_{f,g_3}(\hat{\mathbf{x}}|\mathbf{z})]\\&\leq \max_{P,Q,W}[\exp\{-\lambda ND(Q\circ W\|S\circ W^*)\\&\quad -ND(P\|P^*)+o(N)\}G^N_{f,g_3}(\hat{\mathbf{x}}|\mathbf{z})]\\&\leq \exp\{N\max_{P,Q,W}[h(P,\Delta,Q,W,R_K)-D(P\|P^*)\\&-\lambda D(Q\circ W\|S\circ W^*)]+o(N)\}. \qquad (12)\end{aligned}$$

Since our strategy is valid for any function f_N, from inequality (12) we obtain the upper bound for the guessing rate

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

With respect to the lower bound, we have not got a better result for it and we will use the result of Haroutunian from [4], if the reliability function goes into infinity . It is obvious that any lower bound on $R(R_K,W^*,P^*)$ for SCS with a noiseless channel to the wiretapper is also a lower bound for the same system with a noisy channel. Thus,

$$\begin{aligned}R(R_K,\Delta,W^*,P^*) &\geq R(R_K,\Delta,P^*)\\&\geq \max_P[h(P,\Delta,R_K)-D(P||P^*)].\end{aligned}$$

The theorem is proved.

5. CONCLUSION

We utilize Merhav-Arikan's security criterion applying only the expected first moment of the number of guesses. We gave some restrictions cryptograms : namely, wiretapper assumes that cryptogram consists in i.i.d. RVs and the second the cryptogram is assumed to be of fixed length M for given N.

REFERENCES

[1] 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.

[2] E. Arikan, "Guessing and cryptology", in "Aspects of Network and Information Security", NATO Science for Peace and Security, series D: Information and Communication Security, IOS Press, vol. 17, pp. 211–217, 2008

[3] E. A. Haroutunian and A. R. Ghazaryan, "On the Shannon cipher system with a wiretapper guessing subject to distortion and reliability requirements", *IEEE-ISIT2002,p.324, Lausanna , June 30-July 5, 2002.*

[4] 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.

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

[6] M. K. Hanawal and R. Sundaresan ,"The Shannon cipher system with a guessing wiretapper: General sources", *IEEE Trans. Inform. Theory*, vol. 57, no. 4, pp. 2503-2515, 2011.

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

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

[9] H. Yamamoto and K. Okudra, "Channel coding theorem for the number of guesses in decoding", *IEEE-ISIT2011,pp.419-423, Saint Petersburg, July 31-August 5, 2011.*

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

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

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