Mathematical Problems of Computer Science 63, 14–24, 2025.
doi:10.51408/1963-0128

UDC 519.72

Reliability Criteria in Source Coding Problem with Secret Component

Mariam E. Haroutunian[1], Jemma S. Santrosyan[2] and Parandzem M. Hakobyan[1]

[1]Institute for Informatics and Automation Problems of NAS RA, Yerevan, Armenia
[2]Vanadzor State University, Vanadzor, Armenia
e-mail: armar@sci.am, j.santrosian@gmail.com, par_h@iiap.sci.am

Abstract

This work addresses a source coding problem for one-way sources with correlated outputs. In this scenario, one source output must be transmitted to the receiver within a specified distortion level, similar to conventional source coding. Simultaneously, the other source output must be kept as confidential as possible from the receiver or a potential wiretapper. For this model, the rate-reliability-distortion-equivocation function and the equivocation-reliability-distortion function are defined and analyzed.

Keywords: Rate-reliability-distortion-equivocation function, Source coding.
Article info: Received 27 March 2025; sent for review 1 April 2025; accepted 2 May 2025.

1. Introduction

The source coding problem in information theory focuses on the efficient encoding of information generated by a source so it can be transmitted or stored with minimal redundancy. The main goal is to represent the information as compactly as possible while still enabling perfect or near-perfect reconstruction of the original message.

In lossy coding, some information is sacrificed to achieve greater compression. The reconstructed data is an approximation of the original, acceptable when perfect fidelity isn't necessary. JPEG for images and MP3 for audio are examples of lossy coding methods. In general, source coding is fundamental to efficient data transmission and storage in various fields, including:

- Digital communications (e.g., reducing bandwidth in cellular networks),
- Data compression (e.g., ZIP files, media codecs),
- Machine learning and statistics (e.g., feature selection and data encoding),
- Distributed storage systems (e.g., minimizing storage costs by reducing redundancy).

Shannon **rate-distortion function** (RD) [1] shows the dependence of the asymptotically minimal coding rate on a required average fidelity (distortion) threshold for source noiseless transmission.

The source coding problem for a one-way communication system with correlated source outputs was considered by Yamamoto in [2], where one of the outputs must be transmitted to the receiver within a given distortion level as in ordinary source coding, while the other source output has to be kept as secret as possible from the wiretapper (Fig. 1). The **rate-distortion-equivocation function** (RDE) was defined and evaluated, which is the minimum rate necessary to attain both the equivocation tolerance for the wiretapper and the distortion tolerance for the receiver.

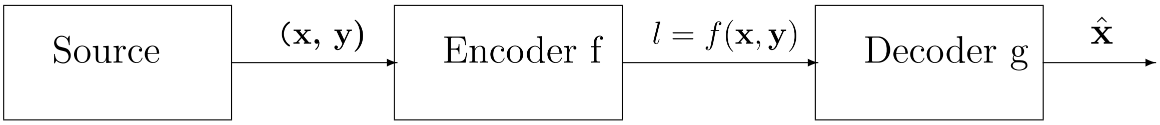

Fig.1. One-way communication system with correlated source outputs.

Previously, Yamamoto [3] studied the source coding problem for cascade and branching communication systems. Later in [4], he considered the RD problem for a communication system with a secondary decoder to be hindered, where security is evaluated by the distortion measure instead of the equivocation function used in [2]. RD problem related to security setting is considered also in [5].

Another characteristic in source coding subject to a distortion criterion can be considered, namely **rate-reliability-distortion function** (RRD) as the minimal rate at which the message of a source can be encoded and then reconstructed by the receiver with an error probability that decreases exponentially with the codeword length. The coding rate as a function of the given distortion level and error exponent E has been studied for various source models. We refer to [6], which in turn refers to the list of main results. In addition to that list, it is worth mentioning [7], where the RRD region with partial secrecy under the distortion criterion is considered, which is the generalization of the encoding problem studied in [3].

Here we introduce and investigate the **rate-reliability-distortion-equivocation function** (RRDE) for the model from [2]. This function combines all aspects, including error control and security. This framework is useful in scenarios involving secure and reliable data transmission, where the goal is to balance the trade-offs among rate, reliability, distortion, and secrecy. Balancing these four elements in a single framework is challenging because improving one aspect often comes at the expense of another.

This setting of source coding with a secret component has many applications, including:

- *sensor networks* in distributed systems like IoT, to ensure that data is compressed, securely transmitted, and reliably received,
- *video and audio streaming* to ensure high-quality, low-latency streaming with some degree of security against unauthorized access,
- *cryptographic communication systems* need guidelines for encoding methods that balance data rate, fidelity, error protection, and secrecy.

Particularly, in [8], the *utility-privacy tradeoff* problem is modeled as source coding and solved using the tool of RRD theory.

In this paper, we introduce and study the set of E-achievable (R, Δ_d, Δ_e) triples. As a consequence, we obtain the equivocation-reliability-distortion function and the rate-reliability-distortion function.

The paper is organized as follows. In the next section, the main notations and definitions are given. The main results are formulated in Section 3. The proof of the main theorem is given in the Appendix. The paper is summarized in Section 5.

2. Notations and Definitions

The Discrete Memoryless Source (DMS) is defined as a sequence $\{(X_i, Y_i)\}_{i=1}^{\infty}$ of discrete independent identically distributed (i. i. d.) random variables X and Y, taking values in finite sets $\mathcal{X}$ and $\mathcal{Y}$, which are the alphabets of messages of the source, respectively. Let

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

be the generating probability distribution of the source outputs (X, Y). The source is memoryless, which means that for N-length vector pairs $\mathbf{x} = (x_1, x_2, ..., x_N) \in \mathcal{X}^N$ and $\mathbf{y} = (y_1, y_2, ..., y_N) \in \mathcal{Y}^N$

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

The finite set $\hat{\mathcal{X}}$, different in general from $\mathcal{X}$, is the reproduction alphabet at the receiver.

A code (f_N, g_N) is defined by a pair of mappings: a coding

$$f_N : \mathcal{X}^N \times \mathcal{Y}^N \to \{1, 2, ..., L(N)\},$$

and decoding

$$g_N : \{1, 2, ..., L(N)\} \to \hat{\mathcal{X}},$$

where $L(N)$ is the code volume. Code rate is

$$R(f_N, g_N) = \frac{1}{N} \log L(N).$$

Throughout this paper, all log-s and exp-s are of base 2.

We consider the distortion measure

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

between source and reconstruction messages. The distortion measure for N -length sequences is the average of the components' distortions

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

The task of this system is to ensure restoration of one of the components of source messages, i.e. X, at the receiver within a given distortion level Δ_d and with a small error probability. At the same time, the other source output Y has to be kept as secret as possible from the receiver or wiretapper. This protection level is measured by the **equivocation rate**, defined as

$$R_e = \frac{1}{N} H(\mathbf{Y}|L(N)),$$

where $H(\mathbf{Y}|L(N))$ is the conditional entropy [9]. In other words, the equivocation rate indicates the receiver's uncertainty about $\mathbf{y}$ given l.

We define the **error probability** of the code (f_N, g_N) as

$$e(f_N, g_N, P^*, \Delta_d) = 1 - P^{*N}(\mathcal{A}),$$

where $\mathcal{A}$ is the set of satisfactorily transmitted vectors:

$$\mathcal{A} = \{(\mathbf{x}, \mathbf{y}) : g_N(f_N(\mathbf{x}, \mathbf{y})) = \hat{\mathbf{x}}, d(\mathbf{x}, \hat{\mathbf{x}}) \le \Delta_d\}.$$

Definition 1. The triple (R, Δ_d, Δ_e) is called E-achievable for given $P^*, E > 0, \Delta_d \ge 0, \Delta_e \ge 0$, if for every $\epsilon > 0, \delta > 0$, there exists a code (f_N, g_N) such that

$$\frac{1}{N} \log L(N) \le R + \epsilon,$$

the error probability is exponentially small

$$e(f_N, g_N, P^*, \Delta_d) \le \exp\{-N(E - \delta)\}$$

and the equivocation rate

$$R_e \ge \Delta_e - \epsilon.$$

We denote by $\mathcal{R}^*(E)$ the set of all E**-achievable triples**. We will consider the **distortion-equivocation** E**-achievable region**:

$$\mathcal{R}^*_{\Delta_d, \Delta_e}(E) = \{(\Delta_d, \Delta_e) : (R, \Delta_d, \Delta_e) \in \mathcal{R}^*(E) \text{ for some } R \ge 0\}.$$

Then the **RRDE function** is defined as

$$R^*(E, \Delta_d, \Delta_e) = \min_{(R, \Delta_d, \Delta_e) \in \mathcal{R}^*(E)} R.$$

At last, the **equivocation-reliability-distortion function** (ERD) is:

$$\Gamma^*(E, \Delta_d) = \max_{(\Delta_d, \Delta_e) \in \mathcal{R}^*_{\Delta_d, \Delta_e}(E)} \Delta_e.$$

3. Formulation of the Results

Let

$$Q = \{Q(\hat{x}|x, y), x \in \mathcal{X}, y \in \mathcal{Y}, \hat{x} \in \hat{\mathcal{X}}\}$$

be a conditional PD on $\hat{\mathcal{X}}$ for given x, y.

Consider the following set of distributions P:

$$\alpha(E, P^*) = \{P : D(P||P^*) \le E\},$$

where $D(P||P^*)$ is the KL-divergence [9].

Let $\mathcal{Q}(P, \Delta_d, \Delta_e)$ be the set of all conditional PDs $Q_P(\hat{x}|x, y) = Q_P$, corresponding to the PD P, for which the following conditions hold:

$$\mathbf{E}d(X, \hat{X}) = \sum_{x,y,\hat{x}} P(x, y) Q_P(\hat{x}|x, y) d(x, \hat{x}) \le \Delta_d, \tag{1}$$

$$H_{P,Q_P}(Y|\hat{X}) \ge \Delta_e.$$

Then

$$\mathcal{Q}(P, \Delta_d) = \bigcup_{H_{P,Q_P}(Y|X) \leq \Delta_e \leq H_{P,Q_P}(Y)} \mathcal{Q}(P, \Delta_d, \Delta_e).$$

The main result of this paper is presented in the following theorem.

Theorem 1. *For given P^*, every $E > 0$,*

$$\mathcal{R}^*(E) = \left\{ \begin{array}{l} (R, \Delta_d, \Delta_e) : \Delta_d \geq 0, \Delta_e \geq 0, \\ \\ 0 \leq R_e \leq \min\limits_{P \in \alpha(E,P^*)} \max\limits_{Q_P \in \mathcal{Q}(P,\Delta_d)} H_{P,Q_P}(Y|\hat{X}), \\ \\ R \geq \max\limits_{P \in \alpha(E,P^*)} \min\limits_{Q_P \in \mathcal{Q}(P,\Delta_d,\Delta_e)} I_{P,Q_P}(X, Y; \hat{X}) \end{array} \right\}.$$

Corollary 2. *The ERD function equals*

$$\Gamma^*(E, \Delta_d) = \min_{P \in \alpha(E,P^*)} \max_{Q_P \in \mathcal{Q}(P,\Delta_d)} H_{P,Q_P}(Y|\hat{X}).$$

Corollary 3.

$$\mathcal{R}^*_{\Delta_d,\Delta_e}(E) = \left\{ \begin{array}{l} R(E, \Delta_d, \Delta_e) : \Delta_d \geq 0, \\ \\ 0 \leq \Delta_e \leq \Gamma^*(E, \Delta_d) \end{array} \right\}.$$

Corollary 4. *The RRDE function equals*

$$R^*(E, \Delta_d, \Delta_e) = \max_{P \in \alpha(E,P^*)} \min_{Q_P \in \mathcal{Q}(P,\Delta_d,\Delta_e)} I_{P,Q_P}(X, Y; \hat{X}).$$

Corollary 5. *The limits of the RRDE and ERD functions when E tends to 0, coincide with the RDR and ED functions stated in [2]:*

$$\lim_{E \to 0} R^*(E, \Delta_d, \Delta_e) = R^*(\Delta_d, \Delta_e) = \min_{Q^*_P \in \mathcal{Q}(P^*,\Delta_d,\Delta_e)} I_{P^*,Q^*_P}(X, Y; \hat{X}).$$

$$\lim_{E \to 0} \Gamma^*(E, \Delta_d) = \Gamma^*(\Delta_d) = \max_{Q_{P^*} \in \mathcal{Q}(P^*,\Delta_d)} H_{P^*,Q_{P^*}}(Y|\hat{X}).$$

The proofs are given in the Appendix and are based on the method of types [10].

4. Conclusion

In this paper, we introduced and examined the set of E-achievable (R, Δ_d, Δ_e) triples. Additionally, we defined and analyzed the ERD function and the RRDE. The limits of these functions, when E tends to 0, coincide with the results from [2].

Appendix

For the proof of Theorem 1, we will use the following modification of the Covering Lemma [11], [6].

Lemma 1. *Let for $\epsilon > 0$*

$$J(P,Q) = \exp\{N(I_{P,Q}(X,Y;\hat{X}) + \epsilon)\}.$$

Then, for every type P and conditional type Q, there exists a collection of vectors

$$\{\hat{\mathbf{x}}_j \in \mathcal{T}^N_{P,Q}(\hat{X}), j = 1, ..., J(P,Q)\},$$

such that the set

$$\{\mathcal{T}^N_{P,Q}(X,Y|\hat{\mathbf{x}}_j), j = 1, ..., J(P,Q)\},$$

covers $\mathcal{T}^N_P(X,Y)$ for N large enough, that is

$$\mathcal{T}^N_P(X,Y) \subset \bigcup_{j=1}^{J(P,Q)} \mathcal{T}^N_{P,Q}(X,Y|\hat{\mathbf{x}}_j).$$

We omit the proof of Lemma 1, since it is similar to the proof of Lemma 5.5. from [6].

Proof of the Theorem 1: First we shall show that

$$\mathcal{R}^*(E) \supseteq \left\{ \begin{array}{l} (R, \Delta_d, \Delta_e) : \Delta_d \geq 0, \Delta_e \geq 0, \\ \\ 0 \leq R_e \leq \min\limits_{P \in \alpha(E,P^*)} \max\limits_{Q_P \in \mathcal{Q}(P,\Delta_d)} H_{P,Q_P}(Y|\hat{X}), \\ \\ R \geq \max\limits_{P \in \alpha(E,P^*)} \min\limits_{Q_P \in \mathcal{Q}(P,\Delta_d,\Delta_e)} I_{P,Q_P}(X,Y;\hat{X}) \end{array} \right\}.$$

Let us represent the set of all source messages of length N as follows:

$$\mathcal{X}^N \times \mathcal{Y}^N = \bigcup_{P \in \mathcal{P}_N(X \times Y)} \mathcal{T}^N_P(X,Y),$$

where $\mathcal{P}_N(X \times Y)$ is the set of possible types of pairs $(\mathbf{x}, \mathbf{y}) \in \mathcal{X}^{\mathbf{N}} \times \mathcal{Y}^{\mathbf{N}}$.

Using the properties of types and the definition of the set $\alpha(E, P^*)$ for each $\delta > 0$, we can find the estimation of the probability of appearance of the source of types beyond $\alpha(E + \delta, P^*)$ as follows:

$$\begin{aligned} P^{*N}\left(\bigcup_{P \notin \alpha(E+\delta,P^*)} \mathcal{T}^N_P(X,Y)\right) &= \sum_{P \notin \alpha(E+\delta,P^*)} P^{*N}\left(\mathcal{T}^N_P(X,Y)\right) \\ &\leq (N+1)^{|\mathcal{X}||\mathcal{Y}|} \exp\left\{-N \min_{P \notin \alpha(E+\delta,P^*)} D(P||P*)\right\} \quad (2) \\ &\leq \exp\{-NE - N\delta + |\mathcal{X}||\mathcal{Y}| \log(N+1)\} \\ &\leq \exp\{-N(E + \delta/2)\}. \end{aligned}$$

For each $\Delta_d \geq 0$, let us pick some types $P \in \alpha(E+\delta, P^*)$ and some $Q_P \in \mathcal{Q}(P, \Delta_d, \Delta_e)$. Let

$$C(P, Q_P, j) = \mathcal{T}^N_{P,Q_P}(X, Y|\hat{\mathbf{x}}_j) - \bigcup_{j'<j} \mathcal{T}^N_{P,Q_P}(X, Y|\hat{\mathbf{x}}_{j'}), \quad j = \overline{1, J(P, Q_P)}.$$

We define a code (f_N, g_N) for vector pairs of type P with the encoding:

$$f_N(\mathbf{x}, \mathbf{y}) = \begin{cases} j, \ \text{when } (\mathbf{x}, \mathbf{y}) \in C(P, Q_P, j), \ P \in \alpha(E+\delta, P^*), \\ \\ j_0, \ \text{when } (\mathbf{x}, \mathbf{y}) \in \mathcal{T}^N_P(X, Y), \ P \notin \alpha(E+\delta, P^*), \end{cases}$$

and the decoding

$$g_N(j) = \hat{\mathbf{x}}_j, \qquad g_N(j_0) = \hat{\mathbf{x}}_0,$$

where the number j_0 and the reconstruction vector $\hat{\mathbf{x}}_0$ are fixed. Obviously, with such code, an error occurs only when the number j_0 is sent.

According to the definition of the code and the inequality (1), for $P \in \alpha(E+\delta, P^*)$ and $Q_P \in \mathcal{Q}(P, \Delta_d, \Delta_e)$ we have:

$$\begin{aligned} d(\mathbf{x}, \hat{\mathbf{x}}_\mathbf{j}) &= \frac{1}{N} \sum_{x,\hat{x}} n(x, \hat{x}|\mathbf{x}, \hat{\mathbf{x}}_\mathbf{j}) d(x, \hat{x}) \\ &= \sum_{x,y,\hat{x}} P(x, y) Q_P(\hat{x}|x, y) d(x, \hat{x}) \\ &= \mathbf{E}_{P,Q_P} d(X, \hat{X}) \leq \Delta_d, \quad j = \overline{1, J(P, Q_P)}. \end{aligned}$$

According to Lemma 1, the number of vectors $\hat{\mathbf{x}}$ for a fixed type P and corresponding conditional type $Q_P \in \mathcal{Q}(P, \Delta_d, \Delta_e)$ is:

$$L_{P,Q_P}(N) = \exp\left\{N(I_{P,Q_P}(X, Y; \hat{X}) + \epsilon)\right\}.$$

Then, taking into account that the number of types has a polynomial estimate [10]

$$L(N) \leq \sum_{P \in \alpha(E+\delta, P^*)} \min_{Q_P \in \mathcal{Q}(P, \Delta_d, \Delta_e)} L_{P,Q_P}(N)$$

$$\leq (N+1)^{|\mathcal{X}||\mathcal{Y}|} \max_{P \in \alpha(E+\delta, P^*)} \min_{Q_P \in \mathcal{Q}(P, \Delta_d, \Delta_e)} \exp\left\{N(I_{P,Q_P}(X, Y; \hat{X}) + \epsilon)\right\}.$$

Hence, the corresponding limit for the transmission rate is:

$$\frac{1}{N} \log L_{P,Q_P}(N) - \epsilon - \frac{1}{N}|\mathcal{X}||\mathcal{Y}| \log(N+1) \leq$$

$$\leq \max_{P \in \alpha(E+\delta, P^*)} \min_{Q_P \in \mathcal{Q}(P, \Delta_d, \Delta_e)} I_{P,Q_P}(X, Y; \hat{X}). \tag{3}$$

Taking into account the arbitrariness of ϵ and δ and the continuity of the information expression (3), we get:

$$R^*(E, \Delta_d, \Delta_e) \leq \max_{P \in \alpha(E, P^*)} \min_{Q_P \in \mathcal{Q}(P, \Delta_d, \Delta_e)} I_{P,Q_P}(X, Y; \hat{X}). \tag{4}$$

For this code, the equivocation rate can be evaluated as follows:

$$\frac{1}{N}H(\mathbf{Y}|L(N)) \geq \frac{1}{N}\sum_{j=1}^{L(N)} H_{P^*,Q_{P^*}}(Y|\mathbf{x},\mathbf{y}\in C(P,Q_P,j)))P^*\{\mathbf{x},\mathbf{y}\in C(P,Q_P,j)\} \tag{5}$$

$$= \frac{1}{N}\sum_{j=1}^{L(N)}\left[-\sum_{\mathbf{y}:\mathbf{x},\mathbf{y}\in C(P,Q_P,j)} P^*\{\mathbf{y}|\mathbf{x},\mathbf{y}\in C(P,Q_P,j)\}\log P^*\{\mathbf{y}|\mathbf{x},\mathbf{y}\in C(P,Q_P,j)\}\right]$$
$$\times P^*\{\mathbf{x},\mathbf{y}\in C(P,Q_P,j)\}.$$

For any $\mathbf{y}$ such that $\mathbf{x},\mathbf{y}\in C(P,Q_P,j)$ for some $\mathbf{x}$

$$P^*\{\mathbf{y}|\mathbf{x},\mathbf{y}\in C(P,Q_P,j)\} = \frac{P^*\{\mathbf{x},\mathbf{y}\in C(P,Q_P,j)|\mathbf{y}\}P^*\{\mathbf{y}\}}{P^*\{\mathbf{x},\mathbf{y}\in C(P,Q_P,j)\}}$$

$$= \frac{\sum\limits_{\mathbf{x},\mathbf{y}\in C(P,Q_P,j)} P^*\{\mathbf{x},\mathbf{y}|\mathbf{y}\}P^*\{\mathbf{y}\}}{\sum\limits_{\mathbf{x},\mathbf{y}\in C(P,Q_P,j)} P^*\{\mathbf{x},\mathbf{y}\}} \leq \frac{\sum\limits_{\mathbf{x}\in\mathcal{T}^N_{P,Q_P}(X|\mathbf{y},\hat{\mathbf{x}}_j)} P^*\{\mathbf{x}|\mathbf{y}\}P^*\{\mathbf{y}\}}{\sum\limits_{\mathbf{x},\mathbf{y}\in C(P,Q_P,j)} P^*\{\mathbf{x},\mathbf{y}\}}. \tag{6}$$

As the probability of the pair $(\mathbf{x},\mathbf{y})$ is constant within the same type, from (6) we obtain that

$$P^*\{\mathbf{y}|\mathbf{x},\mathbf{y}\in C(P,Q_P,j)\} \leq \frac{|\mathcal{T}^N_{P,Q_P}(X|\mathbf{y},\hat{\mathbf{x}}_j)|}{|C(P,Q_P,j)|}$$

$$\leq \frac{\exp[N(H_{P,Q_P}(X|Y\hat{X})]}{(N+1)^{|\mathcal{X}||\mathcal{Y}|}\exp[N(H_{P,Q_P}(XY|\hat{X})]} \leq \exp[-N(H_{P,Q_P}(Y|\hat{X})-\epsilon)]. \tag{7}$$

Then, from (5), (7) and (2) we obtain that

$$\frac{1}{N}H(\mathbf{Y}|L(N)) \geq$$

$$\frac{1}{N}\sum_{j=1}^{L(N)}\left[N\sum_{\mathbf{y}:\mathbf{x},\mathbf{y}\in C(P,Q_P,j)} P^*\{\mathbf{y}|\mathbf{x},\mathbf{y}\in C(P,Q_P,j)\}(H_{P,Q_P}(Y|\hat{X})-\epsilon)\right]$$
$$\times P^*\{\mathbf{x},\mathbf{y}\in C(P,Q_P,j)\}$$
$$= P^*\{\mathbf{x},\mathbf{y}\in\bigcup_{j=1}^{L(N)} C(P,Q_P,j)\}(H_{P,Q_P}(Y|\hat{X})-\epsilon)$$
$$\geq (1-\exp\{-N(E+\delta/2)\})(H_{P,Q_P}(Y|\hat{X})-\epsilon).$$

For N large enough, we obtain that

$$R_e \geq H_{P,Q_P}(Y|\hat{X})-\epsilon \geq \Delta_e-\epsilon. \tag{8}$$

According to (2), (4) and (8), we state that the triple (R,Δ_d,Δ_e) is E-achievable.

Now we pass to the inverse part, let us prove that:

$$\mathcal{R}^*(E)\subseteq\left\{\begin{array}{l}(R,\Delta_d,\Delta_e):\Delta_d\geq 0,\Delta_e\geq 0,\\[2ex] 0\leq R_e\leq \min\limits_{P\in\alpha(E,P^*)}\max\limits_{Q_P\in\mathcal{Q}(P,\Delta_d)} H_{P,Q_P}(Y|\hat{X}),\\[2ex] R\geq \max\limits_{P\in\alpha(E,P^*)}\min\limits_{Q_P\in\mathcal{Q}(P,\Delta_d,\Delta_e)} I_{P,Q_P}(X,Y;\hat{X})\end{array}\right\}.$$

Let $\epsilon > 0$ be fixed. Consider a code (f_N, g_N) for each blocklength N with (R, Δ_d, Δ_e) E-achievable triple. We must show that for some $Q_P \in \mathcal{Q}(P, \Delta_d, \Delta_e)$ the following inequalities hold for N large enough:

$$\frac{1}{N} \log L(N) + \epsilon \geq \max_{P \in \alpha(E,P^*)} I_{P,Q_P}(X, Y; \hat{X}), \tag{9}$$

$$\frac{1}{N} H(\mathbf{Y}|L(N)) - \epsilon \leq \min_{P \in \alpha(E,P^*)} H_{P,Q_P}(Y|\hat{X}). \tag{10}$$

Let $\mathcal{A}'$ be the complement of the set $\mathcal{A}$. The following statement is true:

$$\left|\mathcal{A} \bigcap \mathcal{T}_P^N(X,Y)\right| = \left|\mathcal{T}_P^N(X,Y)\right| - \left|\mathcal{A}' \bigcap \mathcal{T}_P^N(X,Y)\right|.$$

For $P \in \alpha(E - \epsilon, P^*)$

$$\begin{aligned} \left|\mathcal{A}' \bigcap \mathcal{T}_P^N(X,Y)\right| &= \frac{P^{*N}(\mathcal{A}' \cap \mathcal{T}_P^N(X,Y))}{P^{*N}(\mathbf{x},\mathbf{y})} \\ &\leq \exp\left\{N(H_P(X,Y) + D(P||P^*))\right\} \exp\left\{-N(E-\epsilon)\right\} \\ &\leq \exp\left\{N(H_P(X,Y) - \epsilon)\right\}. \end{aligned}$$

Hence,

$$\begin{aligned} \left|\mathcal{A} \bigcap \mathcal{T}_P^N(X,Y)\right| &\geq (N+1)^{-|\mathcal{X}||\mathcal{Y}|} \exp\left\{N H_P(X,Y)\right\} - \exp\left\{N(H_P(X,Y) - \epsilon)\right\} \\ &= \exp\left\{N(H_P(X,Y) - \epsilon)\right\} \left(\frac{\exp\{N\epsilon\}}{(N+1)^{|\mathcal{X}||\mathcal{Y}|}} - 1\right) \\ &\geq \exp\left\{N(H_P(X,Y) - \epsilon)\right\}. \end{aligned} \tag{11}$$

For each $\mathbf{x}, \mathbf{y} \in \mathcal{A} \bigcap \mathcal{T}_P^N(X,Y)$ corresponds a unique vector $\hat{\mathbf{x}}$ such that

$$\hat{\mathbf{x}} = g_N(f_N(\mathbf{x},\mathbf{y})) \ \text{ and } \ \hat{\mathbf{x}} \in \mathcal{T}_{P,Q}^N(\hat{X}|\mathbf{x},\mathbf{y}).$$

Let us divide the set of all vectors $\left|\mathcal{A} \bigcap \mathcal{T}_P^N(X,Y)\right|$ into subsets by conditional types Q_P. The class having maximum cardinality for given P, we denote by

$$\left(\left|\mathcal{A} \bigcap \mathcal{T}_P^N(X,Y)\right|\right)_{Q_P}.$$

According to the number of conditional types Q, for sufficiently large N, we have:

$$\begin{aligned} \left|\mathcal{A} \bigcap \mathcal{T}_P^N(X,Y)\right| &\leq (N+1)^{|\mathcal{X}||\mathcal{Y}|} \left(\left|\mathcal{A} \bigcap \mathcal{T}_P^N(X,Y)\right|\right)_{Q_P} \\ &\leq \exp\{N\epsilon/2\} \left(\left|\mathcal{A} \bigcap \mathcal{T}_P^N(X,Y)\right|\right)_{Q_P}. \end{aligned} \tag{12}$$

Let

$$\mathcal{D} = \left\{\hat{\mathbf{x}} : g_N(f_N(\mathbf{x},\mathbf{y})) = \hat{\mathbf{x}}, \text{for some} \, (\mathbf{x},\mathbf{y}) \in \mathcal{A} \bigcap \mathcal{T}_P^N(X,Y) \bigcap \mathcal{T}_{P,Q_P}^N(X,Y|\hat{\mathbf{x}})\right\}.$$

From definition of the code $|\mathcal{D}| \leq L(N)$, then

$$\begin{aligned} \left|\left(\mathcal{A} \bigcap \mathcal{T}_P^N(X,Y)\right)\right|_{Q_P} &\leq \sum_{\hat{\mathbf{x}} \in \mathcal{D}} \left|\mathcal{T}_{P,Q}^N(X,Y|\hat{\mathbf{x}})\right| \\ &\leq L(N)\exp\{NH_{P,Q_P}(X,Y|\hat{X})\}. \end{aligned} \tag{13}$$

From (11-13) follows

$$L(N) \geq \exp\{N(I_{P,Q_P}(X,Y;\hat{X}) - \epsilon)\}$$

for each $P \in \alpha(E-\epsilon, P*)$ and some Q_P for which $\mathbf{E}_{P,Q_P} d(X,\hat{X}) \leq \Delta_d$, because $\mathbf{x}, \mathbf{y} \in \mathcal{A}$. From achievability follows that

$$\Delta_e - \epsilon \leq \frac{1}{N} H(\mathbf{Y}|L(N)) \leq H_{P,Q_P}(Y|\hat{X}).$$

So $Q_P \in \mathcal{Q}(P, \Delta_d, \Delta_e)$ and inequalities (9) and (10) are valid. Theorem 1 is proved.

References

[1] C. E. Shannon, “Coding theorems for a discrete source with a fidelity criterion”, *IRE National Convention Record*, vol. 7, pp.142–163, 1959.

[2] H. Yamamoto, “A source coding problem for sources with additional outputs to keep secret from the receiver or wiretappers”, *IEEE Transactions on Information Theory*, vol. 29, no. 6, pp. 918–923, 1983.

[3] H. Yamamoto, ”Source coding theory for cascade and branching communication systems”, *IEEE Transactions on Information Theory*, vol. 27, no. 3, pp. 299–308, 1981.

[4] H. Yamamoto, ”A rate-distortion problem for a communication system with a secondarydecoder to be hindered”, *IEEE Transactions on Information Theory*, vol. 34, no. 4, pp. 835–842, 1988.

[5] H. Yamamoto, ”Rate-distortion theory for the Shannon cipher system”, *IEEE Transactions on Information Theory*, vol. 43, no. 3, pp. 827–835, 1997.

[6] E. Haroutunian, M. Haroutunian and A. Harutyunyan, “Reliability Criteria in Information Theory and in Statistical Hypothesis Testing”, *Foundations and Trends in Communications and Information Theory*, vol. 4, nos 2-3, pp. 97–263, 2007. doi: 10.1561/0100000008

[7] E. Haroutunian, A. Harutyunyan, A. Ghazaryan and E. van der Meulen, ”On branching communication system rates-reliability-distortions region with partial secrecy under distortion criterion”, *Mathematical Problems of Computer Science*, vol. 21, pp. 61–76, 2000.

[8] L. Sankar, S. R. Rajagopalan and H. V. Poor, “Utility-privacy tradeoffs in databases: an information-theoretic approach”, *IEEE Transactions on Information Theory*, vol. 8, no. 6, pp. 838–852, 2013.

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

[10] I. Csiszár, “Method of types”, *IEEE Transactions on Information Theory*, vol. 44, no. 6, pp. 2505-2523, 1998.

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

Հուսալիության չափանիշները գաղտնի բաղադրիչով աղբյուրի կոդավորման խնդրում

Մարիամ Ե. Հարությունյան[1], Ջեմմա Ս. Սանթրոսյան[2] և Փառանձեմ Մ. Հակոբյան[1]

[1]ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտ, Երևան, Հայաստան
[2]Վանաձորի պետական համալսարան, Վանաձոր, Հայաստան
e-mail: armar@sci.am, j.santrosian@gmail.com, par_h@iiap.sci.am

Ամփոփում

Այս աշխատանքում ուսումնասիրվում է կոռելացված ելքերով միակողմանի աղբյուրների կոդավորման խնդիրը: Այս մոդելի համար, ինչպես ավանդական աղբյուրի կոդավորման դեպքում, աղբյուրի մի ելքը փոխանցում է հասցեատիրոջը հաղորդագրությունը որոշակի շեղման մակարդակով: Միևնույն ժամանակ, աղբյուրի մյուս ելքը պետք է հնարավորինս գաղտնի պահվի ստացողից կամ հնարավոր գաղտնալսողից: Այս մոդելի համար սահմանվել և վերլուծվել են արագություն-հուսալիություն-շեղում-անորոշություն և անորոշություն-հուսալիություն-շեղում ֆունկցիաները:

Բանալի բառեր՝ արագություն-հուսալիություն-շեղում-անորոշություն ֆունկցիա, աղբյուրի կոդավորում:

Критерии надёжности в задаче кодирования источника с секретным компонентом

Мариам Е. Арутюнян[1], Джемма С. Сантросян[2] и Парандзем М. Акопян[1]

[1]Институт проблем информатики и автоматизации НАН РА, Ереван, Армения
[2]Ванадзорский государственный университет, Ванадзор, Армения
e-mail: armar@sci.am, j.santrosian@gmail.com, par_h@iiap.sci.am

Аннотация

В данной работе рассматривается задача кодирования источника для односторонних источников с коррелированными выходами. В этой модели один из выходов источника должен быть передан получателю с заданным уровнем искажения, аналогично традиционному кодированию источника. Одновременно с этим, другой выход источника должен быть максимально засекречен от получателя или потенциального перехватчика. Для данной модели определяются и анализируются функции скорость-надёжность-искажение-неопределённость и неопределённость-надёжность-искажение.

Ключевые слова: функция скорость-надёжность-искажение-неопределённость, кодирование источника.